

# Hitachi Content Platform Anywhere Enterprise

v7.6

---

## Edge Filer Administration Guide

This document describes how to use HCP Anywhere Enterprise Edge Filer as an Administrator.

© 2023 Hitachi Vantara LLC. 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, AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, GDPS, HyperSwap, IBM, Lotus, MVS, OS/390, PowerHA, PowerPC, RS/6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z14, 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> or [https://knowledge.hitachivantara.com/Documents/Open\\_Source\\_Software](https://knowledge.hitachivantara.com/Documents/Open_Source_Software).

---

# Contents

<b>Preface</b> .....	<b>8</b>
About this document.....	8
Document conventions.....	8
Intended audience.....	8
Accessing product downloads.....	9
Getting Help.....	9
<b>Chapter 1. Introduction to Hitachi Content Platform Anywhere Enterprise Edge Filers</b> .....	<b>10</b>
Accessing a HCP Anywhere Enterprise Edge Filer.....	10
Logging in.....	11
Connecting to a HCP Anywhere Enterprise Portal.....	12
Viewing the Status of the Connection to a HCP Anywhere Enterprise Portal.....	15
Navigating the HCP Anywhere Enterprise Edge Filer User Interface.....	16
Configuration View.....	17
Files View.....	18
Viewing Content in a File Manager.....	23
<b>Chapter 2. Setting Up the HCP Anywhere Enterprise Edge Filer</b> .....	<b>25</b>
Viewing HCP Anywhere Enterprise Edge Filer Details.....	25
Setting a Name and Location to Identify the Edge Filer.....	26
Setting the HCP Anywhere Enterprise Edge Filer Time and Date.....	27
Configuring the User Interface Language.....	29
Configuring Access to a Proxy Server.....	30
Enabling Remote Access to the HCP Anywhere Enterprise Edge Filer.....	31
Allowing Single Sign-on from HCP Anywhere Enterprise Portal.....	32
Exporting the Configuration.....	34
Importing the Configuration.....	35
<b>Chapter 3. Managing the HCP Anywhere Enterprise Edge Filer Storage</b> .....	<b>36</b>
Setting Up the Storage.....	36
Managing Arrays.....	38
Expanding an Array.....	38
Creating an Array.....	39
Renaming an Array.....	41
Deleting an Array.....	41

Managing Volumes.....	41
Deleting Volumes.....	44
Scanning and Repairing Volumes.....	44
Handling Volumes Close to Capacity.....	45
Managing Local Deduplication.....	46
Applying Local Deduplication to Existing Files.....	48
Disabling Local Deduplication.....	49
Logging Deduplication.....	50
Increasing Available HCP Anywhere Enterprise Edge Filer Storage.....	50
HCP Anywhere Enterprise Edge Filer in AWS.....	50
HCP Anywhere Enterprise Edge Filer in ESXi.....	51
HCP Anywhere Enterprise Edge Filer in Hyper-V.....	52
HCP Anywhere Enterprise Edge Filer in Other Platforms.....	53
<b>Chapter 4. Managing the HCP Anywhere Enterprise Edge Filer Users....</b>	<b>54</b>
Adding and Editing Users.....	54
Defining Users From an Active Directory Domain, Tree or Forest.....	54
Adding and Editing Local Users.....	58
Adding Users to User Groups.....	59
Viewing Users.....	59
Exporting the List of Users.....	60
Deleting Users.....	60
Managing User Groups.....	61
Deleting User Groups.....	63
<b>Chapter 5. Using HCP Anywhere Enterprise Edge Filer Cloud Services .</b>	<b>64</b>
Viewing the Connection to a HCP Anywhere Enterprise Portal Status.....	66
Managing the Connection to a HCP Anywhere Enterprise Portal.....	67
Reconnecting and Disconnecting to a HCP Anywhere Enterprise Portal.....	68
Managing Caching.....	68
Storage With a Caching Gateway.....	69
File Eviction from the HCP Anywhere Enterprise Edge Filer.....	71
What Happens to Simultaneous File Changes?.....	72
What Files are Not Synced From the HCP Anywhere Enterprise Portal?.....	72
Caching Operations.....	73
View the Cloud Sync Log.....	83
Accessing Previous File Versions.....	84
macOS: Enabling Using Finder to Search in the HCP Anywhere Enterprise Edge Filer.....	84
Searching Using Mac Finder.....	85



<b>Chapter 6. Managing Local Shares .....</b>	<b>86</b>
Configuring HCP Anywhere Enterprise Edge Filer Shares .....	86
Network Sharing Protocols .....	91
Configuring Windows File Sharing .....	91
Configuring FTP Access .....	95
Configuring NFS Access .....	96
Managing Network Shares .....	97
Blocking File Types from Network Shares .....	101
Copying Files From an External File Server to the HCP Anywhere Enterprise Edge Filer .....	102
Modifying Shares .....	102
Removing Shares .....	102
Accessing Network Shares .....	102
Viewing Network Shares Using Windows File Sharing .....	102
Accessing Network Shares Using FTP .....	103
Mounting Network Shares Using NFS .....	103
Accessing the Volumes Share .....	104
Enabling Non-administrators to Access Previous Versions .....	105
<b>Chapter 7. Protecting the Data .....</b>	<b>107</b>
Ransomware Protection .....	107
Requirements .....	107
Setting Up Ransom Protect .....	107
Coping with False Positive Detections .....	110
Blocking Malicious Users .....	113
Removing Users From the Blocked Users Group .....	117
Handling a Ransomware Incident .....	118
Investigating Ransomware Incidents .....	120
Antivirus File Scanning .....	120
Setting up Antivirus File Scanning .....	121
Managing Quarantined Files .....	122
Updating the Antivirus DAT File .....	124
Antivirus Logs .....	126
<b>Chapter 8. Managing Network Settings .....</b>	<b>127</b>
Configuring Network Settings .....	127
Configuring Proxy Server Settings .....	129
Configuring Ethernet Port Settings .....	129
Renewing the DHCP Lease .....	131
Network Diagnostics .....	131
Remotely Awakening Computers .....	135

<b>Chapter 9. Monitoring the HCP Anywhere Enterprise Edge Filer .....</b>	<b>137</b>
Viewing Session Activity.....	139
Using SNMP Monitoring .....	139
Setting Up SNMP Monitoring on the HCP Anywhere Enterprise Edge Filer....	140
<b>Chapter 10. HCP Anywhere Enterprise Edge Filer Logs .....</b>	<b>142</b>
Configuring Logging .....	143
Configuring Syslog Settings .....	144
Configuring Audit Log Settings.....	145
Viewing Different Types of Logs.....	146
System Log .....	146
Cloud Sync Log.....	147
Access Log.....	147
Audit Log .....	147
Filtering Logs .....	148
Exporting Logs.....	149
Understanding HCP Anywhere Enterprise Log File Entries .....	149
Auditing SMB File Access .....	150
Example Log Entries .....	152
<b>Chapter 11. Configuring Email Alerts.....</b>	<b>157</b>
<b>Chapter 12. Generating a Support Report .....</b>	<b>159</b>
Automatically Sending Crash Reports to Support .....	160
<b>Chapter 13. Maintaining a HCP Anywhere Enterprise Edge Filer .....</b>	<b>161</b>
Upgrading the Edge Filer.....	161
Configuring Automatic Firmware Updates .....	161
Manually Upgrading the Firmware .....	162
Restarting the HCP Anywhere Enterprise Edge Filer.....	163
Shutting Down the HCP Anywhere Enterprise Edge Filer.....	164
Resetting a HCP Anywhere Enterprise Edge Filer to its Default Settings .....	165
Changing the HCP Anywhere Enterprise Edge Filer License .....	166
<b>Chapter 14. macOS: Accessing a HCP Anywhere Enterprise Edge Filer</b>	<b>167</b>
Using HCP Anywhere Enterprise Cache Assist .....	167

---

# 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.

HCP Anywhere Enterprise Edge Filers are available as software-based virtual gateways in a virtual environment, such as AWS, Azure, ESXi. HCP Anywhere Enterprise Edge Filers enable you to do the following

- Share files across your network
- 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.

Using the HCP Anywhere Enterprise Edge Filers, connected to a HCP Anywhere Enterprise Portal, data is transparently synchronized and saved between the HCP Anywhere Enterprise Edge Filer and the HCP Anywhere Enterprise Portal Global File System.

This document describes how to manage the HCP Anywhere Enterprise Edge Filers.

## Document conventions

This document uses the following typographic convention:

Convention	Description
<b>Bold</b>	<ul style="list-style-type: none"><li>• Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click <b>OK</b>.</li><li>• Indicates emphasized words in list items.</li></ul>
<i>Italic</i>	Indicates a document title or emphasized words in text.
Monospace	Indicates text that is displayed on screen or entered by the user. Example: <code>pairdisplay -g oradb</code>

## Intended audience

This document is intended for HCP Anywhere Enterprise Edge Filer administrators.

## Accessing product downloads

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

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

## Getting Help

Hitachi Vantara Support Connect is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to Hitachi Vantara Support Connect for contact information: [https://support.hitachivantara.com/en\\_us/contact-us.html](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](https://community.hitachivantara.com), register, and complete your profile.

---

# Chapter 1. Introduction to Hitachi Content Platform Anywhere Enterprise Edge Filers

HCP 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.

HCP Anywhere Enterprise Edge Filers are available as software-based virtual gateways in a virtual environment. HCP Anywhere Enterprise Edge Filers enable you to do the following, depending on the license:

- Share files across your network
- 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 are saved locally, not the actual file content.
- Restore multiple file versions saved on the HCP Anywhere Enterprise Portal.
- Access file versions from anywhere, using a web browser.

Using the HCP Anywhere Enterprise Edge Filers, connected to a HCP Anywhere Enterprise Portal, data is transparently synchronized and saved between the HCP Anywhere Enterprise Edge Filer and the HCP Anywhere Enterprise Portal Global File System.

## Accessing a HCP Anywhere Enterprise Edge Filer

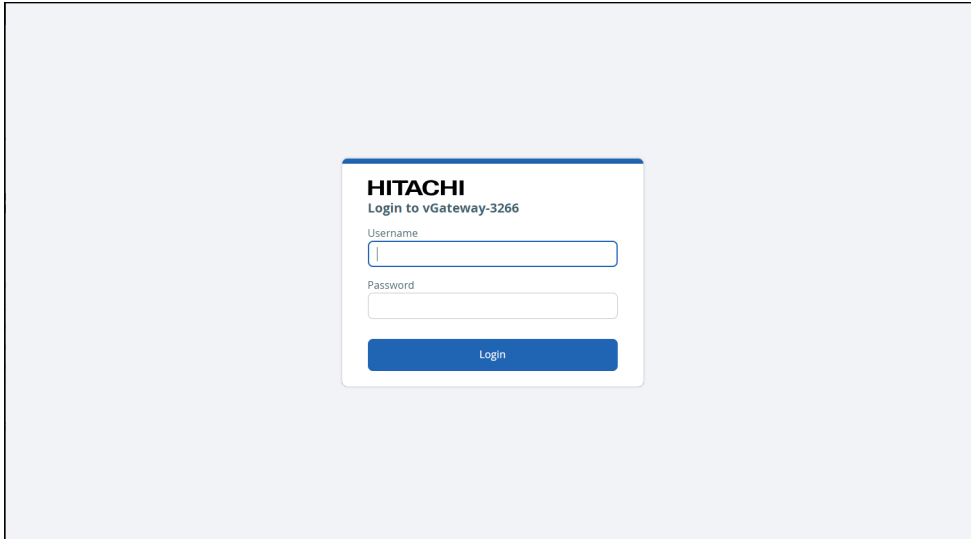
HCP Anywhere Enterprise Edge Filers are managed via a web-based user interface.

### To connect to a HCP Anywhere Enterprise Edge Filer:

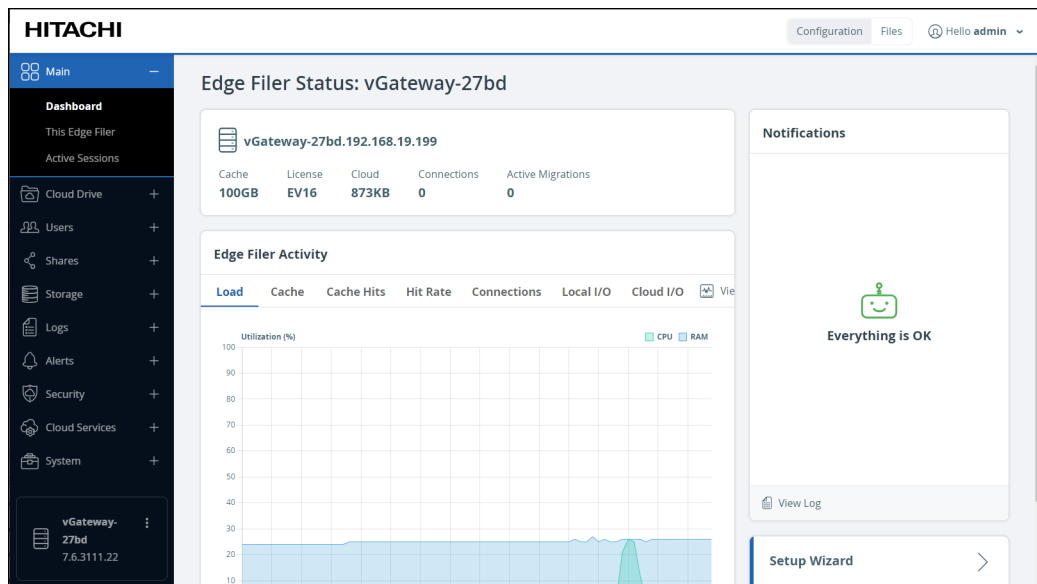
1. Open a web browser. You can use any of the latest two releases of Google Chrome, Apple Safari, Mozilla Firefox, and Microsoft Edge.
2. Enter the HCP Anywhere Enterprise Edge Filer's IP address to navigate to the HCP Anywhere Enterprise Edge Filer.

## Logging in

Each time you connect to the interface, your browser displays the Log In page:

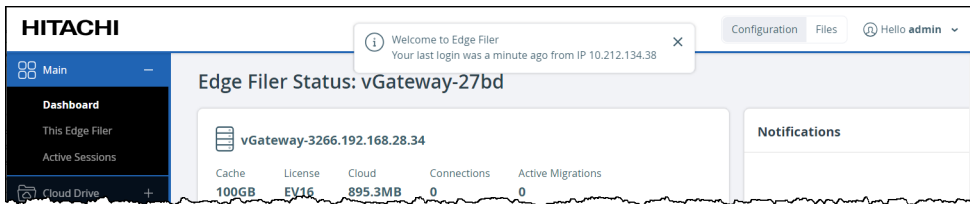


1. Enter your user name and password for accessing the HCP Anywhere Enterprise Edge Filer. The administrator user is defined as part of the initial setup immediately after installation. All other users are added by the administrator, as described in [Adding and Editing Users](#).  
**Note:** When the HCP Anywhere Enterprise Edge Filer is connected to Active Directory, the user name to log in can be the user name or the Active Directory UPN (User Principal Name).
2. Click **Login**.  
As a member of the Administrators or Read Only Administrators user groups, the **Configuration** view **Main > Dashboard** page is displayed.



**Note:** If the HCP Anywhere Enterprise Edge Filer is not connected to a HCP Anywhere Enterprise Portal, the HCP Anywhere Enterprise Edge Filer is unlicensed and the Cloud Drive is not available.

Details of logins and login attempts are displayed on each login.



To use the HCP Anywhere Enterprise Edge Filer, it must be connected to an HCP Anywhere Enterprise Portal. You connect the HCP Anywhere Enterprise Edge Filer to the HCP Anywhere Enterprise Portal using an administrator account. During the initial HCP Anywhere Enterprise Edge Filer setup you connect the HCP Anywhere Enterprise Edge Filer to the HCP Anywhere Enterprise Portal. If the connection between the HCP Anywhere Enterprise Edge Filer and Portal is down, reconnect using the procedure described in [Connecting to a HCP Anywhere Enterprise Portal](#).

Check the status of the connection, as described in [Viewing the Status of the Connection to a HCP Anywhere Enterprise Portal](#).

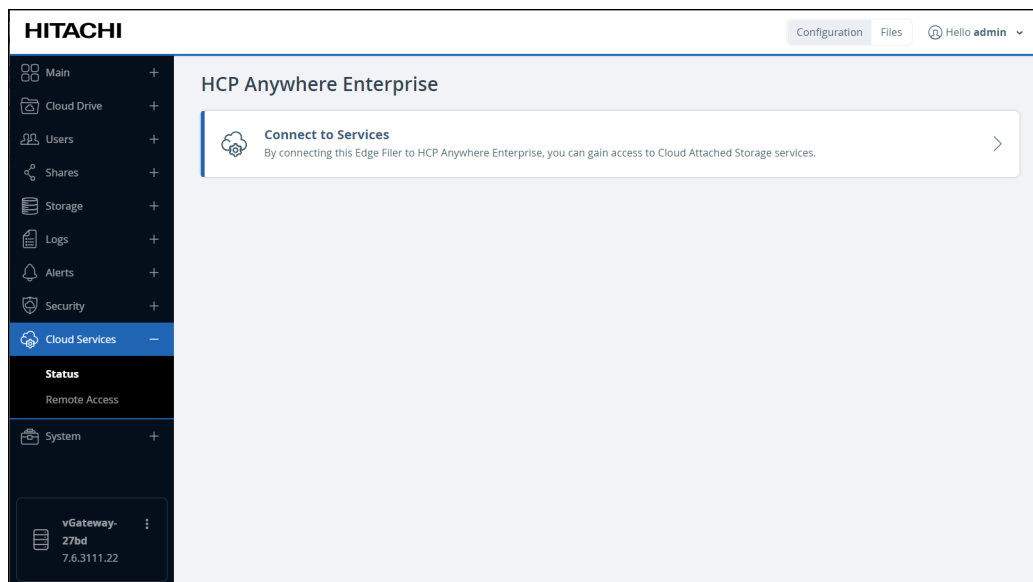
## Connecting to a HCP Anywhere Enterprise Portal

During the initial setup of the HCP Anywhere Enterprise Edge Filer, described in the installation guide, you connect to the HCP Anywhere Enterprise Portal. This section describes how to connect to the HCP Anywhere Enterprise Portal if it is not connected.

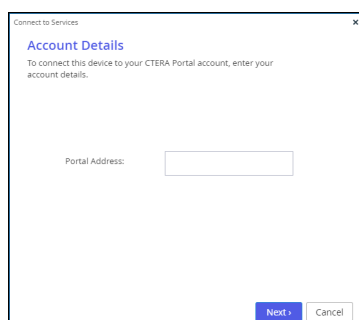
**Note:** If access using CAC, Common Access Card, has been enabled for the HCP Anywhere Enterprise Portal, the HCP Anywhere Enterprise Edge Filer connects to the HCP Anywhere Enterprise Portal using an activation code instead of the user and password credentials. For details, contact Hitachi Vantara support.

**To connect the HCP Anywhere Enterprise Edge Filer to a HCP Anywhere Enterprise Portal:**

1. In the **Configuration** view, select **Cloud Services > Status** in the navigation pane. The **HCP Anywhere Enterprise Portal** page is displayed.

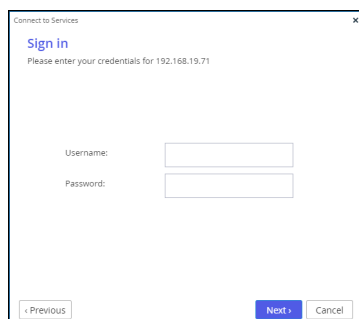


2. Click **Connect to Services**.  
The **Account Details** screen is displayed.



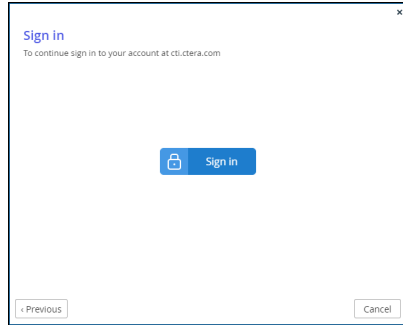
3. Enter the address of the HCP Anywhere Enterprise Portal, and then click **Next**.  
**Note:** If the HCP Anywhere Enterprise Portal does not have a valid certificate installed, a warning is displayed to the end user when logging a device into the portal, offering the option to proceed anyway. This warning is presented every time a user connects a device to the portal, until a valid certificate is installed.

The **Sign In** screen is displayed.



**Note:** If single sign-on has been set up to the portal, the following screen is displayed.





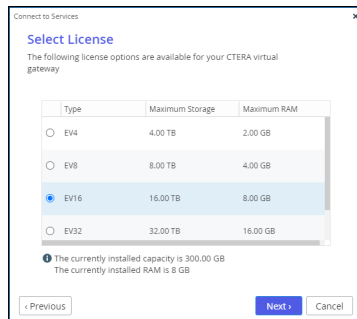
In this case, click **Sign In** and then **Allow** in a separate window when prompted, and then the **Select License** screen is displayed. For HCP Anywhere Enterprise Edge Filers except the HC100, skip the next step. For an HC100, skip the next 2 steps.

4. Enter the HCP Anywhere Enterprise Portal designated user username and password to access the HCP Anywhere Enterprise Portal.

**Note:** The designated user is the owner of the cloud folders and data to manage the HCP Anywhere Enterprise Edge Filer connection to the HCP Anywhere Enterprise Portal for all users and not just the current user. This designated user has HCP Anywhere Enterprise Portal read/write administrator permissions.

5. Click **Next**

The **Select License** screen is displayed.



You are prompted to select the license from those available on the HCP Anywhere Enterprise Portal.

**Note:** If only one license is available, this license is selected automatically.

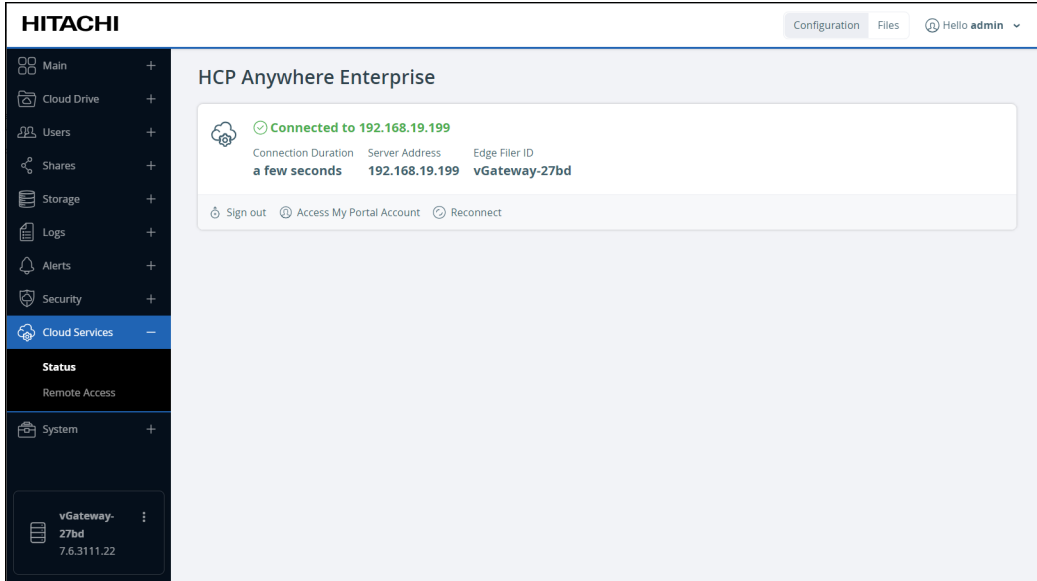
6. Select the license and click **Next**.

The HCP Anywhere Enterprise Edge Filer connects to the HCP Anywhere Enterprise Portal and is added to the HCP Anywhere Enterprise Portal account.

A success screen is displayed.

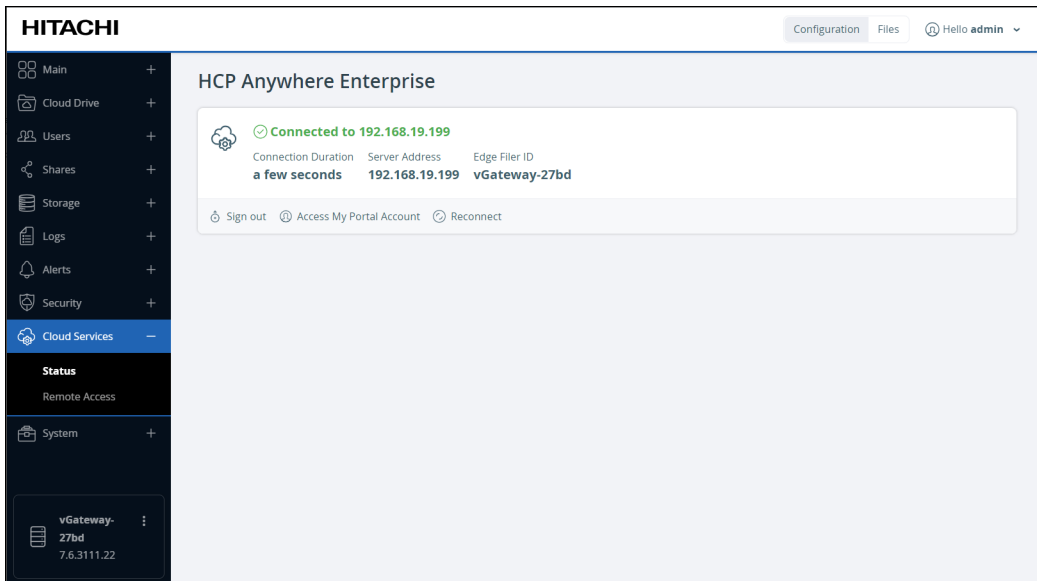
7. Click **Finish**.

The HCP Anywhere Enterprise Portal page is displayed, showing that the HCP Anywhere Enterprise Edge Filer is connected to the HCP Anywhere Enterprise Portal.



## Viewing the Status of the Connection to a HCP Anywhere Enterprise Portal

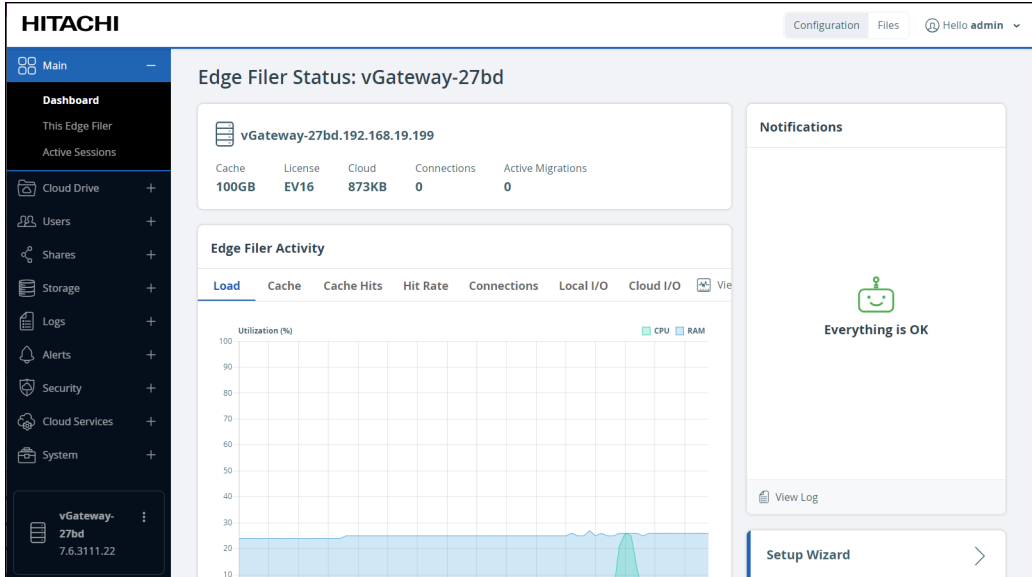
The **HCP Anywhere Enterprise Portal** page displays information about the HCP Anywhere Enterprise Edge Filer connection to a HCP Anywhere Enterprise Portal account.



After connecting to a HCP Anywhere Enterprise Portal the HCP Anywhere Enterprise Edge Filer status panel shows the following:

- The status of the connection to the HCP Anywhere Enterprise Portal can be one of the following:
  - **Resolving the portal address** – The HCP Anywhere Enterprise Edge Filer is resolving the HCP Anywhere Enterprise Portal address.
  - **Connected to portal** – The HCP Anywhere Enterprise Edge Filer is connected to the HCP Anywhere Enterprise Portal named *portal* or with the IP address *portal*, and the connection is currently in use.
  - **Connecting** – The HCP Anywhere Enterprise Edge Filer is connecting to the HCP Anywhere Enterprise Portal.
  - **Disconnected** – The HCP Anywhere Enterprise Edge Filer is disconnected from the HCP Anywhere Enterprise Portal. You can reconnect as described in Reconnecting and Disconnecting to a HCP Anywhere Enterprise Portal.
  - **Authenticating** – The HCP Anywhere Enterprise Edge Filer is authenticating to the HCP Anywhere Enterprise Portal.
  - **Connection Failed** – The connection to the HCP Anywhere Enterprise Portal failed.
- The amount of time that the HCP Anywhere Enterprise Edge Filer has been connected to the HCP Anywhere Enterprise Portal.
- The IP address of the HCP Anywhere Enterprise Portal.
- The edge filer identifier used by the portal.

## Navigating the HCP Anywhere Enterprise Edge Filer User Interface



The HCP Anywhere Enterprise Edge Filer user interface consists of the following elements:

- Across the top of the user interface the following is displayed:
  - **Configuration** view – Perform configuration tasks.
  - **Files** view – View and manage the files and folders on the HCP Anywhere Enterprise Edge

Filer.

- Your user name. Clicking the user name displays a drop-down menu with the following options:

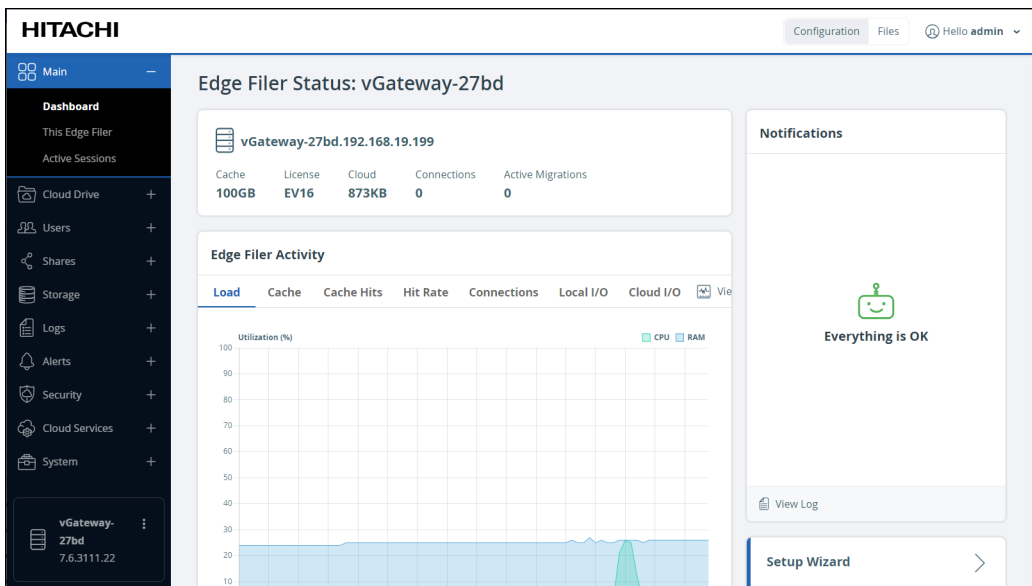
**Change Password** – Change the password to access the HCP Anywhere Enterprise Edge Filer with the current user. The password must be at least eight characters and must include at least a letter, digit and special character, such as ~, @, #, \$, %, ^, &, (.  
**Logout** – Log out of the HCP Anywhere Enterprise Edge Filer.

- The central portion of the user interface displays the content for the selected view.
- The navigation pane displays the menu to access the HCP Anywhere Enterprise Edge Filer configuration options.
- In the bottom left, under the navigation pane, the following information is displayed:
  - The name of the HCP Anywhere Enterprise Edge Filer.
  - The firmware version.
  - Three dots menu with options to restart and shut down the HCP Anywhere Enterprise Edge Filer.

**Note:** For details about the content of the **Dashboard**, see [Monitoring the HCP Anywhere Enterprise Edge Filer](#).

## Configuration View

Use the **Configuration** view to configure the HCP Anywhere Enterprise Edge Filer.

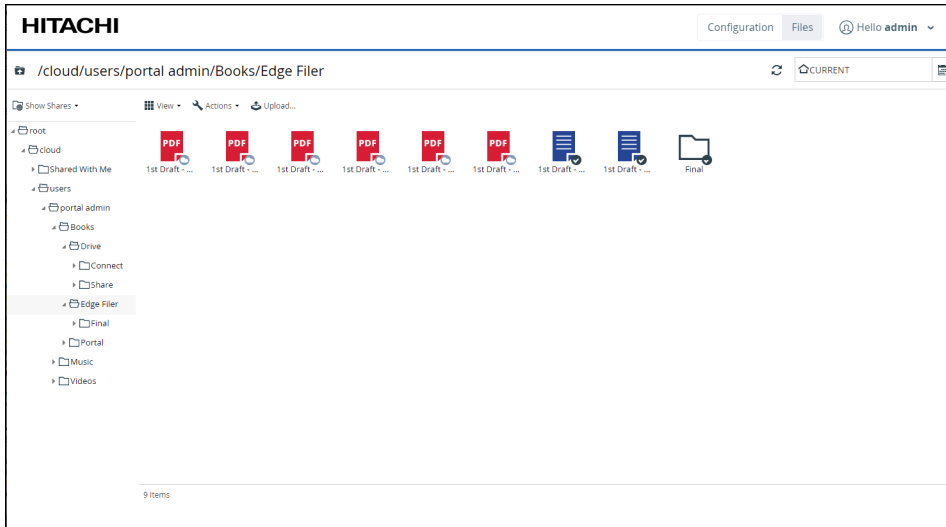


The view includes the following:

- The left side of the user interface is the navigation pane.
- The central portion of the user interface displays the content for the navigation pane item.

## Files View

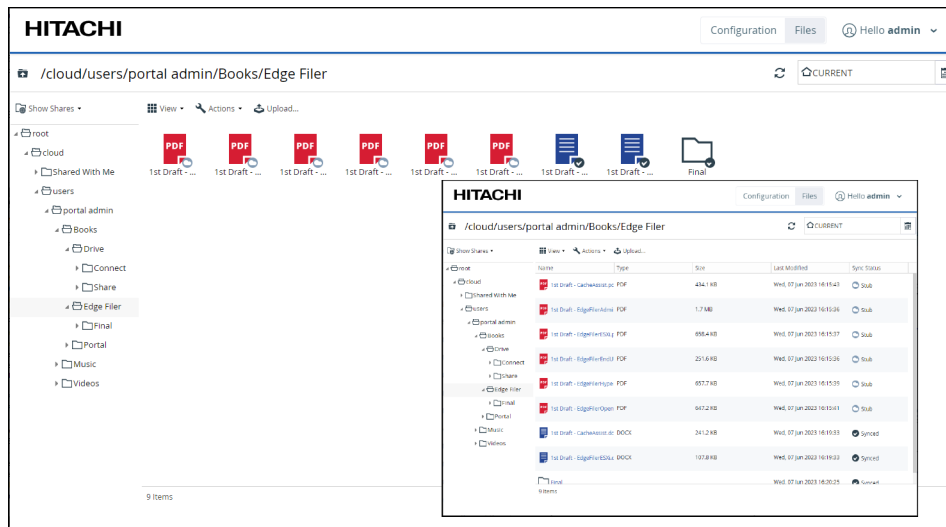
Use the **Files** view to manage folders and files on the HCP Anywhere Enterprise Edge Filer.






You can also map to the folders and files, including shared content, from a file manager, Windows File Explorer or macOS Finder, instead of using the **Files** view. For details, see [Viewing Content in a File Manager](#).

The view includes the following:

- **Show Shares** or **Show Volumes**. A tree of the **Shares** or **Volumes** content:
  - Show Shares** – Displays all network shares and the folders they contain.
  - Show Volumes** – Displays both volumes and network shares. In this view, you can see and manage folders that are not included in any network share.  
To change the tree pane view, click the **Show Shares/Show Volumes** option and then select the desired view.
- Note:** The **Show Volumes** view is available only to Administrators and Read Only Administrators groups.
- **View** – The way the folders are displayed:
  - Details** – The folders and files are displayed in a table with additional information such as the file type, size and last modification date.
  - Large Icons** – The folders and files are displayed as large icons. Selecting an icon displays the information about the file or folder.



When viewing the cloud drive content, each folder and file is marked with an icon indicating its current status:

-  – Folders or files that are in sync.
-  – Files that are currently synchronizing.
-  – Files that are stubs.

In **Details** view, the icon is displayed in the **Sync Status** column.

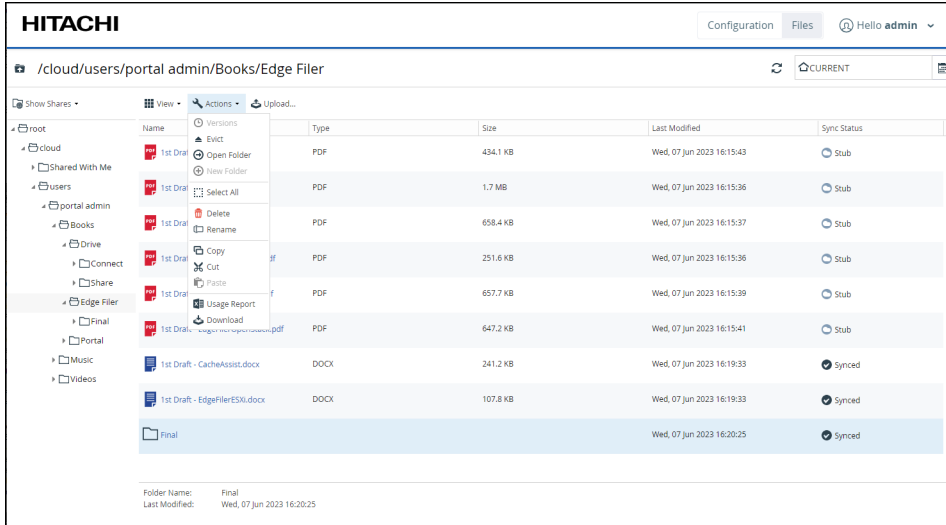
In **Large Icons** view, the icon is displayed over the file or folder.

Selected item details, such as the last modified date, are displayed at the bottom of the right pane.

- **Actions** – Actions you can perform on a selected folder or file, such as copying a folder and its contents or deleting content. For details, see [Actions](#).
- **Upload** – Upload a file to a folder.

## Actions

You can perform actions on a selected folder or file, such as copying a folder and its contents or deleting content. Actions are performed either by right-clicking the item or selecting the item and click **Actions** and then selecting the option in the drop-down menu. The list of options is dependent on the item.



## Accessing Previous Versions of a File

You can view and restore previous versions of the end-user files and folders residing in the cloud on the HCP Anywhere Enterprise Portal, or locally on the HCP Anywhere Enterprise Edge Filer.

For details, see [Accessing Previous File Versions](#).

## Evicting Folder Content From the Cache

You can evict folder contents to increase the free storage in the cache. The folder content is displayed as stubs after the eviction.

### To evict a folder:

1. In the **Files** view, in the **Show Shares** view, navigate to the parent folder.
2. Click the **Evict** action.

The folder content, including subfolder content, is evicted.

## Opening a Folder

### To open a folder:

1. In the **Files** view, in the **Show Shares** view, navigate to the parent folder.
2. Click the **Open Folder** action.

The folder content is displayed.

## Creating a Folder

### To create a folder:

1. In the **Files** view, in the **Show Shares** view, navigate to the parent folder.
2. Click the **New Folder** action.  
The Choose a name window is displayed.
3. Enter a name for the new folder.
4. Click **OK**.

The folder is created.

## Selecting All the Content

### To select all the content:

1. In the **Files** view, in the **Show Shares** view, navigate to the parent folder.
2. Click the **Select All** action.

All the content is selected.

## Deleting Folders and Files

### To delete a folder or file:

1. In the **Files** view, in the **Show Shares** view, navigate to the folder or file.
2. Click the **Delete** action.
3. Click **Yes** to confirm the delete.

## Renaming Folders and Files

### To rename a folder or file:

1. In the **Files** view, in the **Show Shares** view, navigate to the folder or file.
2. Click the **Rename** action.  
The **Choose a name** window is displayed.
3. Enter a new name.
4. Click **OK**.

## Copying and Moving Folders and Files

You can copy or move files and folders within the HCP Anywhere Enterprise Edge Filer to a different file location.

### To copy or move folder and file:

1. In the **Files** view, in the **Show Shares** view, navigate to the folder or file.
2. To copy a file or folder, right-click the folder or file and select **Copy** from the menu.
3. To move a file or folder, right-click the folder or file and select **Cut** from the menu.
4. Navigate to the target folder, right-click in the folder and select **Paste**.

**Note:** Standard Windows keyboard shortcuts, such as Ctrl-C to copy a file or folder and Ctrl-V to paste it, can also be used.



## Creating Folder Usage Reports

You can create a folder usage report that displays detailed information about the folder. The report is saved to your computer as a comma separated values (\*.csv) spreadsheet file.

### To create a folder usage report:

1. In the **Files** view, in the **Show Shares** view, navigate to the folder.
2. Click the **Usage Report** action.

The generated usage report includes the following columns:

- The size in kilobytes of the folder and subfolders.
- The path to the folder.

At the end of the report, the total size is displayed.

## Downloading Folders and Files

### To download an individual file:

1. In the **Files** view, in the **Show Shares** view, navigate to the item to download.
2. Click the **Download** action.

The item is downloaded to your computer.

**Note:** Double-clicking the file in **Large** view, or clicking the file in **Details** view either displays the file for viewing or downloads it.

### To download entire folders or multiple files:

1. In the **Files** view, in the **Show Shares** view, navigate to the folder.
2. In the right pane, select the content to download.
3. Click the **Download** action.

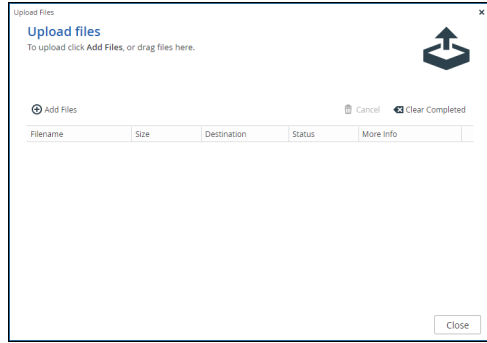
The selected content is downloaded to your computer as a .ZIP file.

## Uploading Files

### To upload files:

1. In the **Files** view, in the **Show Shares** view, navigate to the destination folder for the upload.
2. Click **Upload** in the menu bar.

The **Upload files** window is displayed.

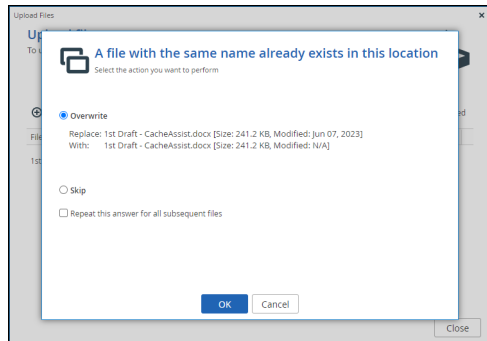


3. Click **Add files** and browse to the file.

**Note:** File names are case-sensitive. For example, *Getting Started.pdf* is treated as a separate file to *getting started.pdf*.

If you are using Chrome or FireFox as your browser, you can drag-and-drop a file from your computer to the **Upload files** window.

4. If the file already exists, the following window is displayed.



To overwrite the file with the file on your computer, select the Overwrite option and click OK.

5. Click Close.

#### To clear the list of completed uploads:

- In the **Upload files** window, click **Clear Completed**.

#### To cancel an upload:

- In the **Upload files** window, select the upload you want to cancel, and click **Cancel**.

## Viewing Content in a File Manager

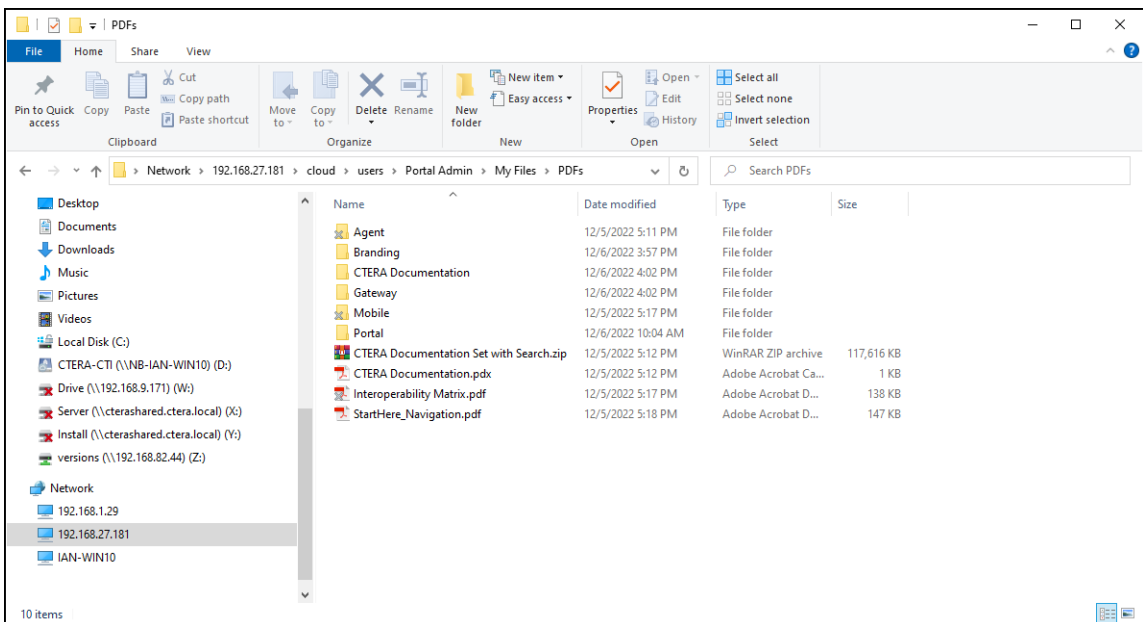
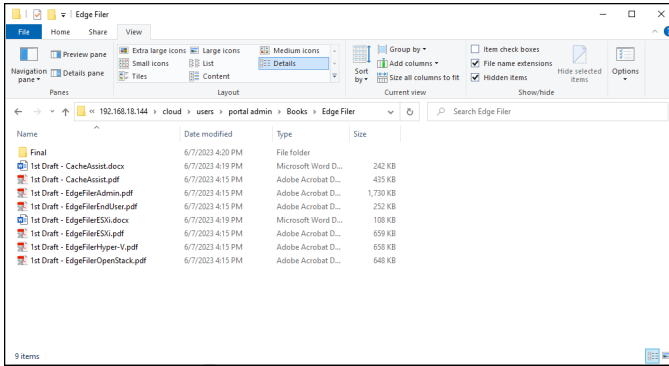
You can map the HCP Anywhere Enterprise Edge Filer. content in a file manager.

#### To view the HCP Anywhere Enterprise Edge Filer content from a file manager:

- Use the following address to access the folders and files from a file manager, for example, Windows File Explorer or macOS Finder: `\\edge_filer_ip\cloud` where *edge\_filer\_ip* is the IP address of the HCP Anywhere Enterprise Edge Filer.

When accessing the HCP Anywhere Enterprise Edge Filer from a macOS machine you need to follow the procedure described in [macOS: Accessing a HCP Anywhere Enterprise Edge Filer](#).

The following screenshot shows a HCP Anywhere Enterprise Edge Filer Caching Gateway accessed from Windows File Explorer.



Both Windows File Explorer and macOS Finder report that the total space and available free space for the mapped drive is a very high number to simulate the caching ability of infinite storage.

**Note:** The HCP Anywhere Enterprise Edge Filer user interface is case sensitive, so file and folder names with the same characters, but different cases, such as MYFOLDER, MyFolder, and myfolder are different folders. When connecting to the HCP Anywhere Enterprise Edge Filer using Windows File Sharing, SMB protocol, which is not case-sensitive, these folders or files are treated as having the same name.

# Chapter 2. Setting Up the HCP Anywhere Enterprise Edge Filer

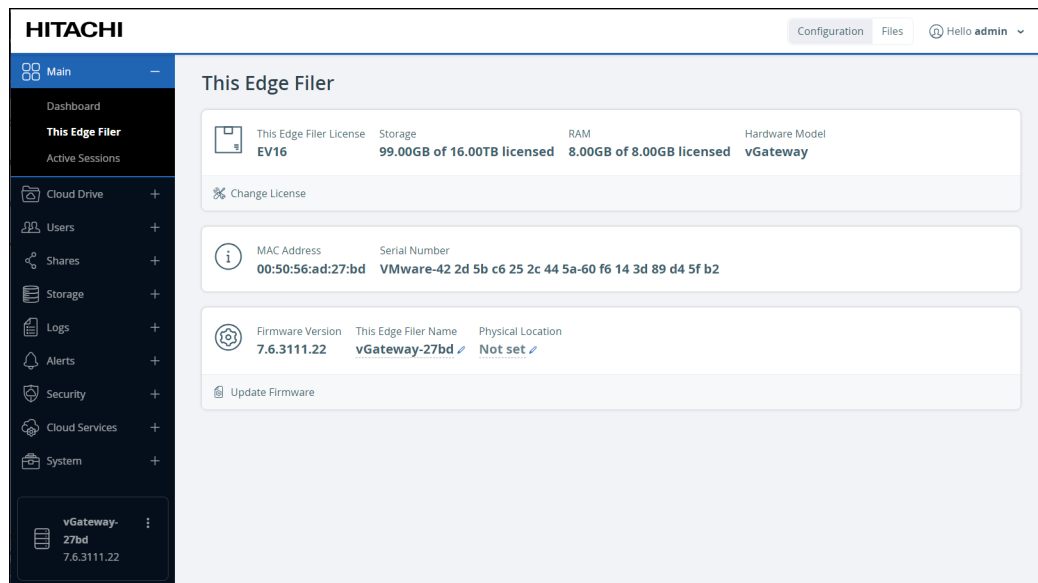
Setting the HCP Anywhere Enterprise Edge Filer time and language or enabling remote access from a HCP Anywhere Enterprise Portal is performed from within the HCP Anywhere Enterprise Edge Filer user interface.

Setting up the HCP Anywhere Enterprise Edge Filer storage and users is described in [Setting Up the Storage](#) and [Adding and Editing Users](#), if this was not done during the initial HCP Anywhere Enterprise Edge Filer set up. Configuring the HCP Anywhere Enterprise Edge Filer for caching is described in [Managing Caching](#).

## Viewing HCP Anywhere Enterprise Edge Filer Details

You can view general information about the HCP Anywhere Enterprise Edge Filer, such as the storage used, license details, and the firmware version.

- In the **Configuration** view, select **Main > This Edge Filer** in the navigation pane. The **This Edge Filer** page opens, displaying the product information.

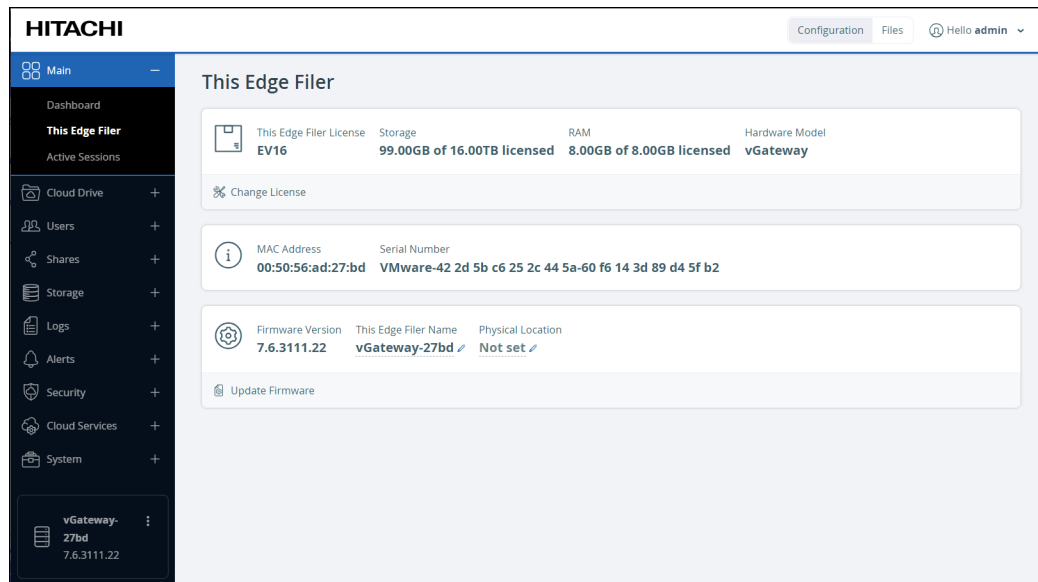


# Setting a Name and Location to Identify the Edge Filer

The HCP Anywhere Enterprise Edge Filer name is used as a unique identifier of this HCP Anywhere Enterprise Edge Filer on the network. The name must be different than any other HCP Anywhere Enterprise Edge Filer or PC on the network. The location field enables you to document the HCP Anywhere Enterprise Edge Filer physical location, and is optional.

## To configure the HCP Anywhere Enterprise Edge Filer name and location:

1. In the **Configuration** view, select **Main > This Edge Filer** in the navigation pane. The **This Edge Filer** page opens, displaying the product information.



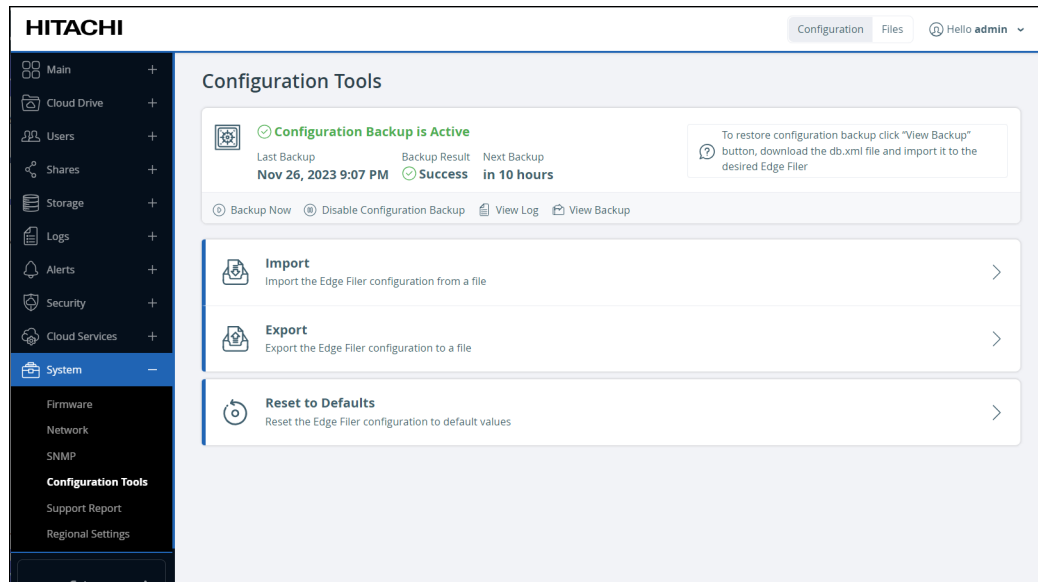
2. To configure the HCP Anywhere Enterprise Edge Filer's name:
  - a) Next to the Device Name field, click the *edit* icon.
  - b) Enter the name to represent the HCP Anywhere Enterprise Edge Filer in the network neighborhood.
  - c) Click the *tick* icon.
3. Configure the HCP Anywhere Enterprise Edge Filer's physical location.
  - a) Next to the Physical Location field, click the *edit* icon.
  - b) Enter the HCP Anywhere Enterprise Edge Filer's location. For example: "Delaware Branch Office".
  - c) Click the *tick* icon.

# Setting the HCP Anywhere Enterprise Edge Filer Time and Date

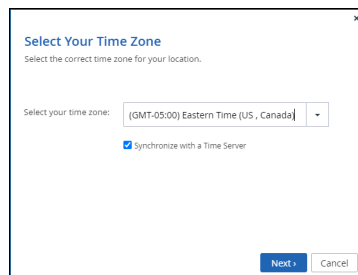
You can configure the HCP Anywhere Enterprise Edge Filer to obtain the time and date from an NTP server, or you configure the time and date manually.

## To configure the HCP Anywhere Enterprise Edge Filer time and date:

1. In the **Configuration** view, select **System > Regional Settings** in the navigation pane. The **Regional Settings** page opens, displaying the currently configured date, time, time zone, and language for the HCP Anywhere Enterprise Edge Filer.

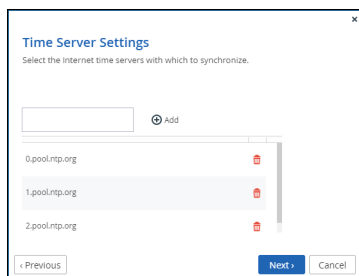


2. Click **Change date and time settings**. The **Select Your Time Zone** window is displayed.



3. Select the time zone.
4. To synchronize the HCP Anywhere Enterprise Edge Filer with an NTP server, select the **Synchronize with a Time Server** option.  
If you want to manually configure the date and time, clear the **Synchronize with a Time Server** check box.
5. Click **Next**.
  - If you chose to synchronize the HCP Anywhere Enterprise Edge Filer with an NTP server by checking **Synchronize with a Time Server**, the **Time Server Settings** window is

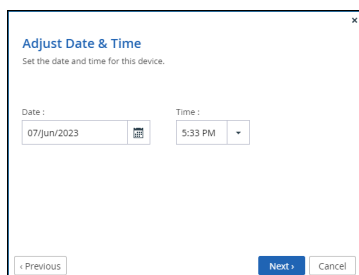
displayed with a list of time servers with which the HCP Anywhere Enterprise Edge Filer will synchronize time and date settings.



To add a time server to the list, enter the server's URL in the provided field, and then click **Add**.

To remove a time server from the list, click the  icon next to the server to be removed.

- If you chose to manually configure time and date settings on the HCP Anywhere Enterprise Edge Filer by unchecking **Synchronize with a Time Server**, the **Adjust Date & Time** window is displayed.



Do the following:

In the **Date** field, type the current date, or click to select the date from a calendar.

In the **Time** drop-down list, select the current time.

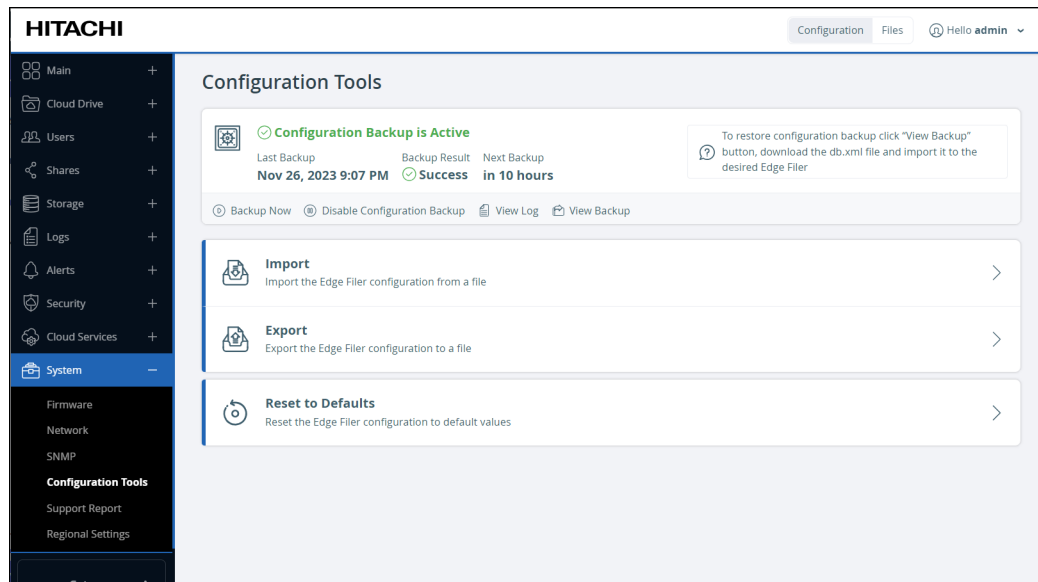
6. Click **Next** and then **Finish**.

# Configuring the User Interface Language

You can configure the language to be displayed in the HCP Anywhere Enterprise Edge Filer's user interface.

## To configure the user interface language:

1. In the **Configuration** view, select **System > Regional Settings** in the navigation pane. The **Regional Settings** page opens, displaying the currently configured date, time, time zone, and language for the HCP Anywhere Enterprise Edge Filer.



2. Click **Change Language**.  
The **Change Language** window is displayed.
3. Select the language from the drop-down list.
4. Click **Save**.

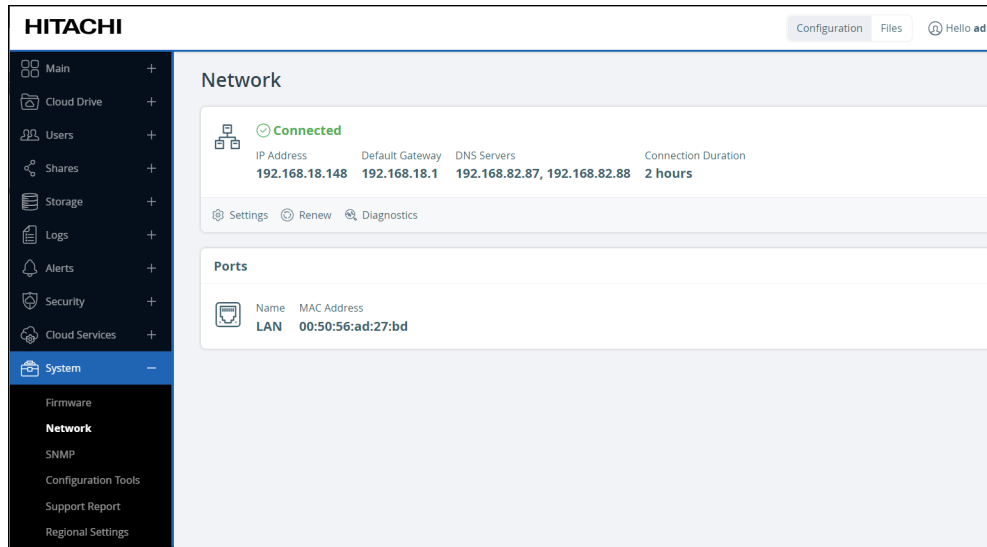


# Configuring Access to a Proxy Server

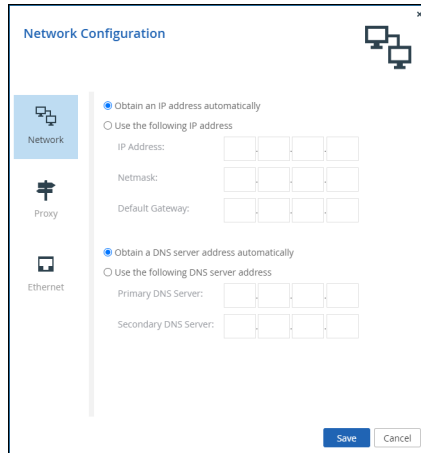
The HCP Anywhere Enterprise Edge Filer can be configured to connect to a HCP Anywhere Enterprise Portal via a proxy server. HTTPS proxies that support the CONNECT method may be used.

## To configure proxy settings:

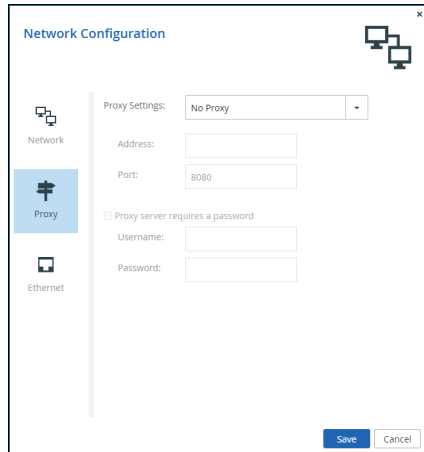
1. In the **Configuration** view, select **System > Network** in the navigation pane. The **Network** page is displayed.



2. Click **Settings**. The **Network Configuration** window is displayed.



3. Select the **Proxy** option.



4. Specify the proxy settings.
  - Proxy Settings** – Select Use HTTP Proxy and configure the appropriate settings:
    - **Address** – The address of the proxy server.
    - **Port** – The proxy server port number.
  - Proxy server requires a password** – 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.
5. Click **Save**.

## Enabling Remote Access to the HCP Anywhere Enterprise Edge Filer

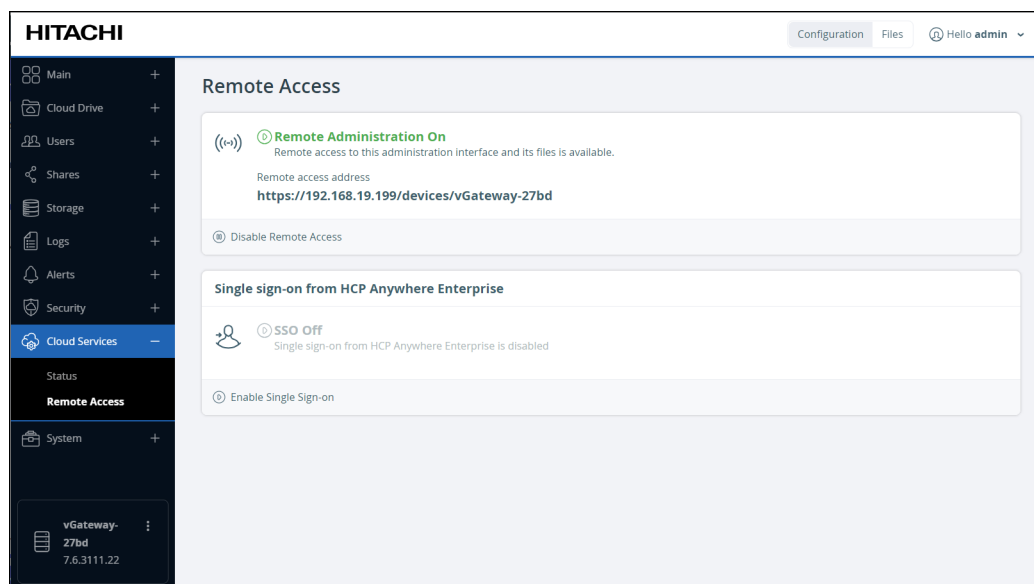
When the HCP Anywhere Enterprise Edge Filer is connected to a HCP Anywhere Enterprise Portal, you can access the HCP Anywhere Enterprise Edge Filer over the Internet by enabling **Remote Access**. **Remote Access** is a cloud service and when it is enabled, the HCP Anywhere Enterprise Edge Filer is assigned a unique DNS name. You can then use this DNS name to access the HCP Anywhere Enterprise Edge Filer anywhere over the Internet.

You can always access the HCP Anywhere Enterprise Edge Filer from within the local network, regardless of the **Remote Access** setting.

**Note:** You do not need to open any ports on the firewall in order to access the HCP Anywhere Enterprise Edge Filer using the DNS name from a remote location.

### To enable and disable remote access:

1. Make sure that the HCP Anywhere Enterprise Edge Filer is connected to a HCP Anywhere Enterprise Portal. For details, see [Managing the Connection to a HCP Anywhere Enterprise Portal](#).
2. In the **Configuration** view, select **Cloud Services > Remote Access** in the navigation pane. The Remote Access page is displayed.



3. Click **Disable Remote Access** to disable remote access, or **Enable Remote Access** to enable remote access.

When enabled, a link to the administration interface is displayed. Use this URL link for remote access to the HCP Anywhere Enterprise Edge Filer.

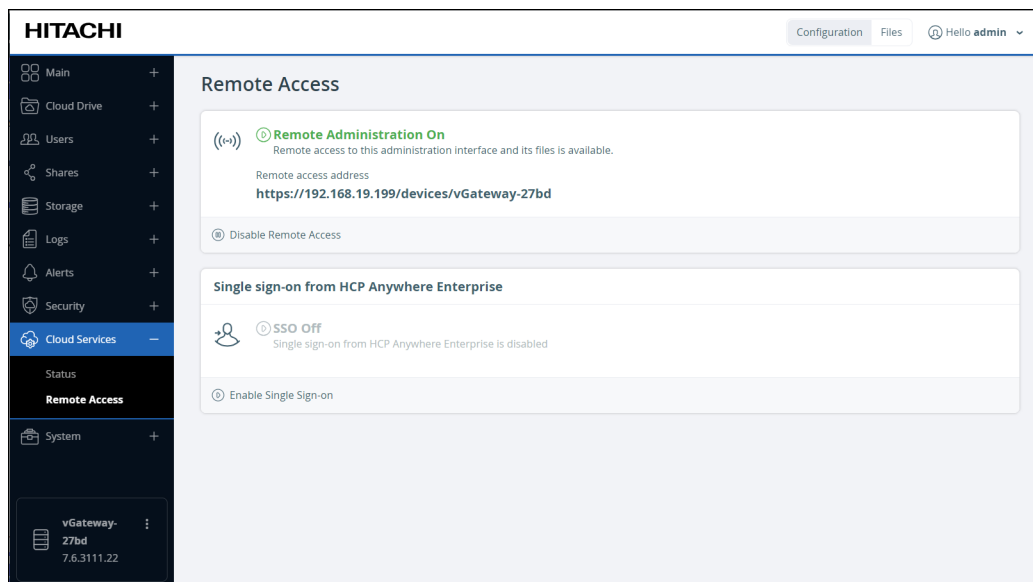
## Allowing Single Sign-on from HCP Anywhere Enterprise Portal

The HCP Anywhere Enterprise Edge Filer user interface can be accessed by a logged in user from within the HCP Anywhere Enterprise Portal user interface, without the user entering HCP Anywhere Enterprise Edge Filer credentials. The user signed in to the HCP Anywhere Enterprise Portal must be the same user as the HCP Anywhere Enterprise Edge Filer user.

**Note:** If single sign-on using CAC (Common Access Card) has been enabled for the HCP Anywhere Enterprise Portal, the HCP Anywhere Enterprise Edge Filer must connect to the HCP Anywhere Enterprise Portal using an activation code instead of the user and password credentials. For details, contact Hitachi Vantara Support Connect support.

### To enable single sign-on to the HCP Anywhere Enterprise Edge Filer:

1. In the **Configuration** view, select **Cloud Services > Remote Access** in the navigation pane. The **Remote Access** page is displayed.



2. Make sure **Enable Remote Access** is set.
3. Click **Enable Single Sign-on** to enable SSO from the HCP Anywhere Enterprise Portal, or **Disable Single Sign-on** to disable SSO from the HCP Anywhere Enterprise Portal.

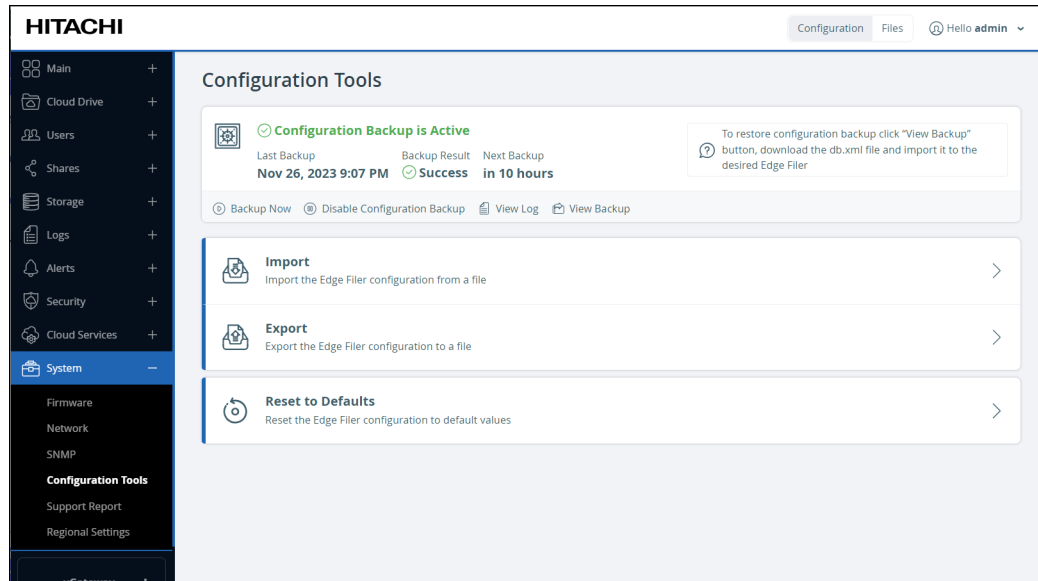
#### Saving HCP Anywhere Enterprise Edge Filer Settings

You can manually export the HCP Anywhere Enterprise Edge Filer configuration to an XML file on your computer, and use this file to restore the HCP Anywhere Enterprise Edge Filer settings as needed.

# Exporting the Configuration

**To export the HCP Anywhere Enterprise Edge Filer configuration to an XML file:**

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



2. Click **Export**.

The HCP Anywhere Enterprise Edge Filer configuration is exported to an XML file in your computer's download folder.

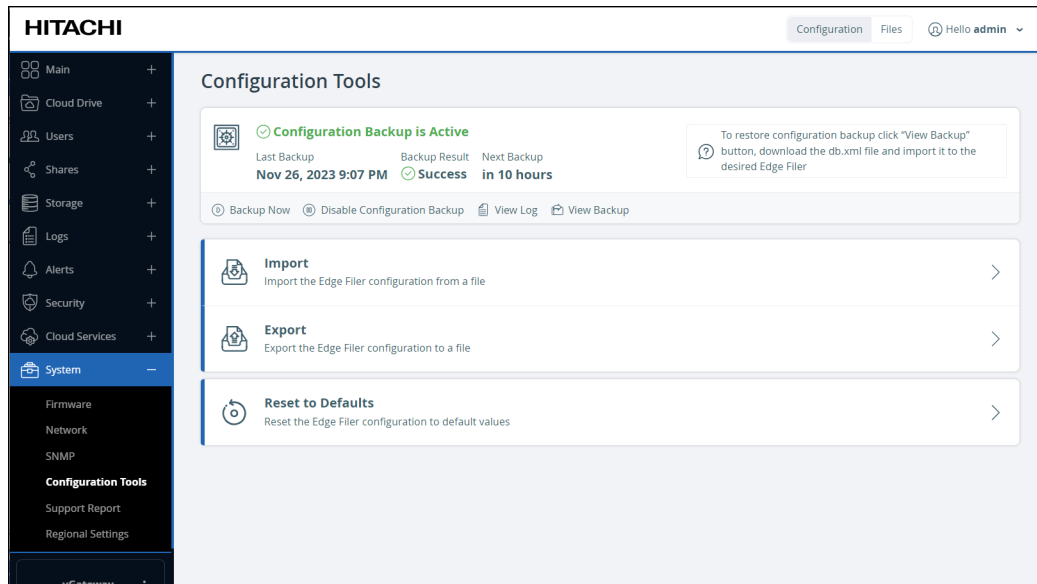
**Note:** For security reasons, all passwords are stored in an encrypted format. However, the export file information is sensitive, and it is therefore recommended that you keep it in a safe place.

# Importing the Configuration

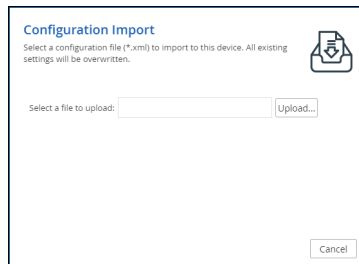
**Note:** Before importing a configuration to a HCP Anywhere Enterprise Edge Filer, a volume must be configured on the edge filer.

**To import a HCP Anywhere Enterprise Edge Filer configuration from an XML configuration file:**

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



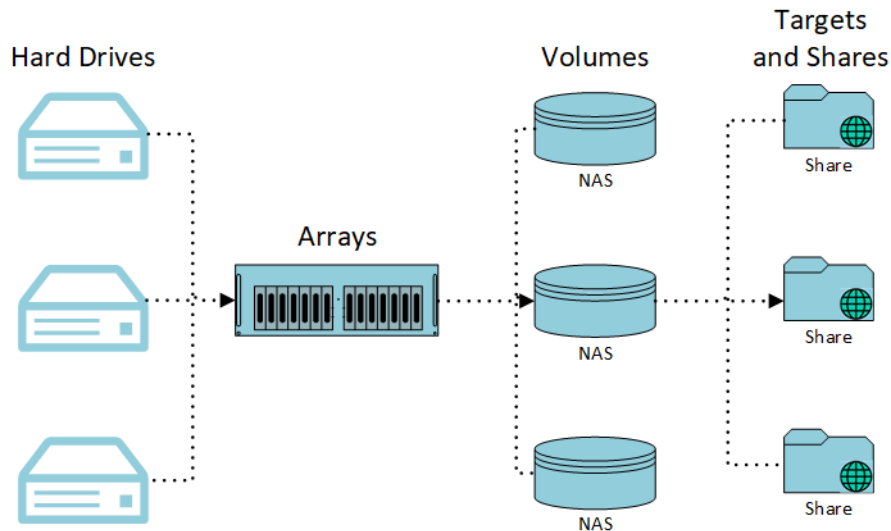
2. Click **Import**. The **Configuration Import** window is displayed.



3. Click **Upload** and browse to the desired configuration file and click **Open**. The configuration file is imported. When the upload is complete, the **Configuration Import Completed** window is displayed. If any errors occurred during the import, they are displayed.
4. Click **Finish**.

## Chapter 3. Managing the HCP Anywhere Enterprise Edge Filer Storage

HCP Anywhere Enterprise Edge Filers support NAS volumes. NAS volumes are accessible through file access protocols. You can create folders on NAS volumes and store files in the folders. You can also define folders as network shares and share them across the network, via several protocols.



You can create an array to combine the drives into a larger pool of storage, set up redundancy between drives, and/or increase performance. Once you've set up an array, you can create volumes, which are logical units of storage.

You can define additional virtual disks for a HCP Anywhere Enterprise Edge Filer and create RAID configurations for these disks. The HCP Anywhere Enterprise Edge Filer supports the definition of up to 16 virtual disks. Depending on the license, it is possible to enlarge the virtual disks. HCP Anywhere Enterprise recommends that the maximum storage is defined as a single disk.

### Setting Up the Storage

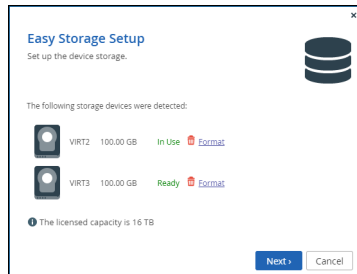
You store the HCP Anywhere Enterprise Edge Filer data on a volume, which is defined on a virtual array. Hitachi Vantara recommends that the maximum storage is defined as a single disk when the HCP Anywhere Enterprise Edge Filer is created.

During the initial setup of the HCP Anywhere Enterprise Edge Filer an LVM array, *array1*, is created with a volume, *vol1*.

If required, you can extend an existing virtual disk, and then enlarge the volume. If you do require multiple disks, for example, when running the HCP Anywhere Enterprise Edge Filer in ESXi, where the maximum disk size is 62TB, the additional disks can be added to the LVM-based array.

### To set up storage:

1. In the **Configuration** view, select **Storage > Arrays** or **Storage > Volumes** in the navigation pane and click **Storage Setup Wizard**.  
The **Easy Storage Setup** window is displayed.



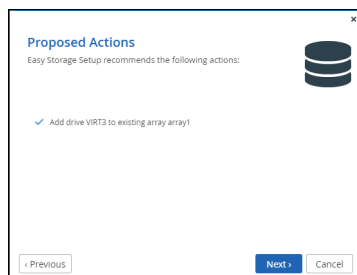
In this example, the HCP Anywhere Enterprise Edge Filer has 2 disks: VIRT2 and VIRT3. In this example, VIRT2 was the original disk and VIRT3 was added.

**Note:** Normally, a HCP Anywhere Enterprise Edge Filer requires one disk. After clicking **Format** and then **Yes** to confirm, the drive is formatted and all the data on the drive is erased.

**Warning:** Formatting erases all data on the drive.

2. Click **Next**.

If there are proposed actions, they are displayed.



3. To continue with the proposed action, click **Next**.
4. Click **Finish** in the **Wizard Completed** window.

If an action was proposed, the action is implemented.



# Managing Arrays

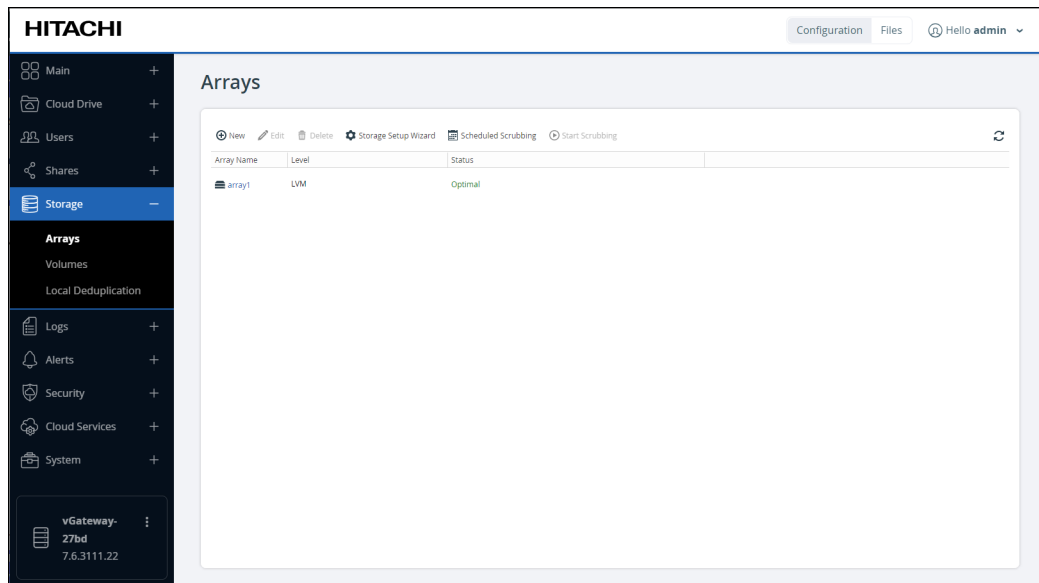
The array and volume are created during the initial setup of the HCP Anywhere Enterprise Edge Filer.

## Expanding an Array

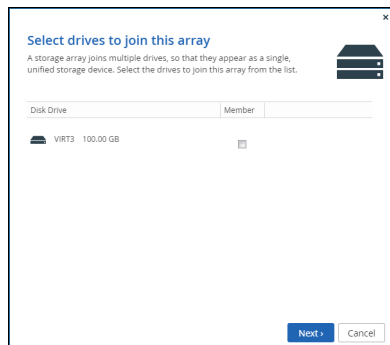
To expand an array after adding new disks, you add the disks to the existing array.

**To expand an array:**

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



2. Click the array to expand or select the array row and click **Edit**. The **Select drives to join this array** wizard is displayed, which shows you all drives available to join the array.



3. Check the **Member** box for each drive to include in the array.
4. Click Next to the end of the wizard and then click **Finish**.

After expanding an array, the added disk space can be used to increase volume sizes. For details, see [Managing Volumes](#).

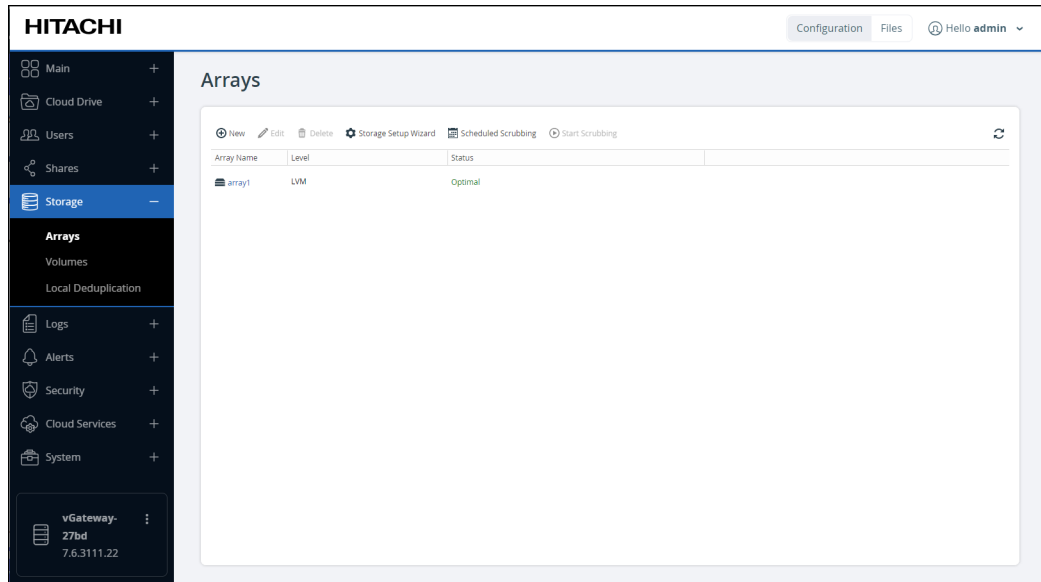
## Creating an Array

This procedure is only required in the following circumstances:

- You did not set up storage during the initial setup of the HCP Anywhere Enterprise Edge Filer.
- You did not set up storage using the storage setup wizard, described in [Setting Up the Storage](#).
- You have additional disks that you want to use in a new array, separate from the existing array.

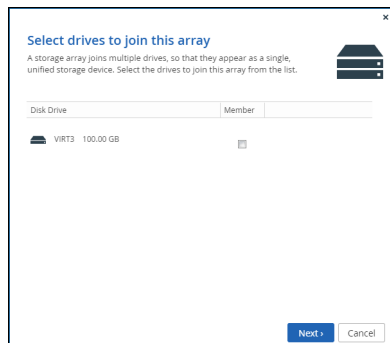
### To create an array:

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

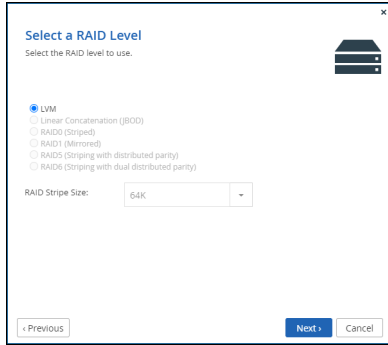


2. Click **New**.

The **Select drives to join this array** wizard is displayed, which shows you all drives available and asks you to select drives to join the new array.



3. Check the **Member** box for each drive you want to include in the array.
4. Click **Next** and then select the type of array you want to create.



**Note:** Only array types that can be selected are enabled.

**LVM** – A Logical Volume Manager-based array. This is the default array type.

**RAID0 (Striped)** – When more than one drive is specified for the array, RAID0 combines the capacity of the drives and increases the read and write speed using striping. You must have at least two drives to create a RAID0 array.

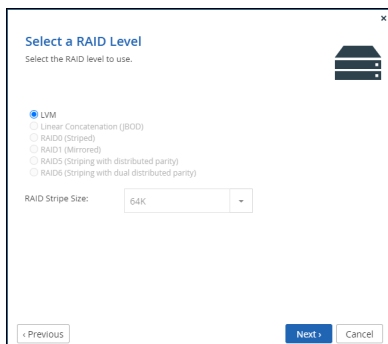
- Specify the **RAID Stripe Size**. This is the size of blocks that data is divided into when it is written to the array and distributed across the drives. Reading and writing large data files sequentially generally benefits from a large stripe size. Small random reads and writes generally benefit from a smaller stripe size. The default value is 64K.

5. Click **Next** and enter a name for the array.



6. Click **Next**.

7. To immediately create a volume on the array, select the **I want to create a logical volume on this storage array** check box.



8. Click **Finish**.

If you checked the **I want to create a logical volume on this storage array** check box, you proceed to create a volume. For details, see [Managing Volumes](#).

## Renaming an Array

### To rename an array:

1. In the **Configuration** view, select **Storage > Arrays** in the navigation pane. The **Arrays** page is displayed.
2. Click the array to rename or select the array row and click **Edit**. The **Select drives to join this array wizard** is displayed.
3. Click **Next** until the **Name this Array** window is displayed.



4. Change the **Array name** value.
5. Click **Next**.
6. Click **Finish** in the **Wizard Completed** window.

## Deleting an Array

**Note:** You cannot delete an array that has a volume defined on it.

### To delete an array:

1. Select the array row, and click **Delete**.
2. Click **Yes** to confirm.

The array is deleted.

## Managing Volumes

Volumes are logical partitions on the HCP Anywhere Enterprise Edge Filer that users can access. You create a NAS volume, and the HCP Anywhere Enterprise Edge Filer acts as a files server for NAS volumes, which can be accessed using any of the supported file sharing protocols.

The HCP Anywhere Enterprise Edge Filer supports the XFS file system. XFS volumes cannot be shrunk. HCP Anywhere Enterprise recommends starting with the required storage and then increasing the storage when using XFS rather than starting with a large storage which cannot be decreased.

When the volume defined in the HCP Anywhere Enterprise Edge Filer does **not** use all the available storage, you can edit the volume to enlarge the volume size.

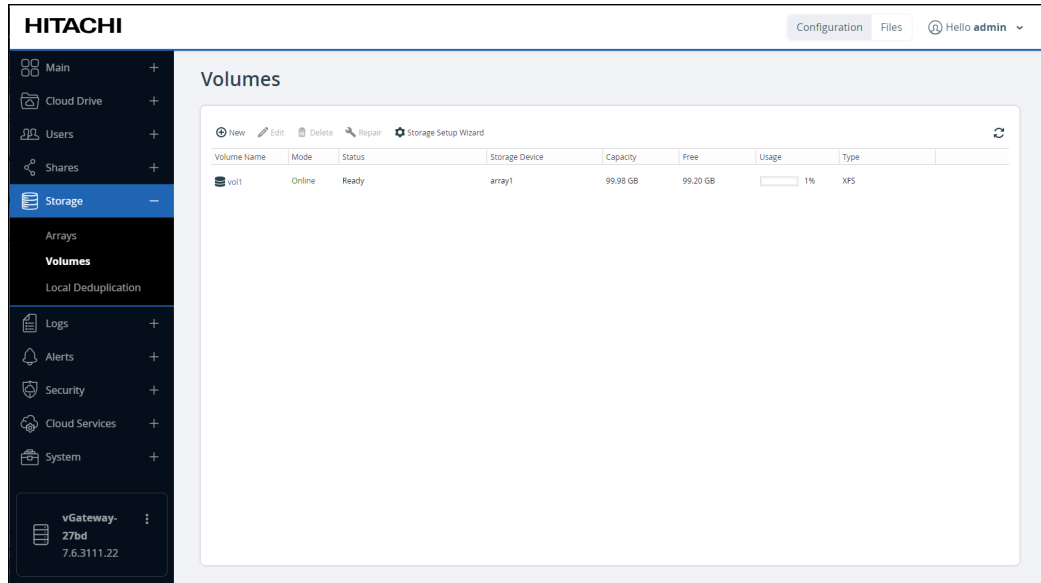
**Note:** When the volume defined in the HCP Anywhere Enterprise Edge Filer uses all the available storage, see [Increasing Available HCP Anywhere Enterprise Edge Filer Storage](#).

To create a volume, you **must** have an array defined. An array is automatically defined as part of the initial setup, described in the installation guide.

A volume is created during the initial setup, described in the installation guide.

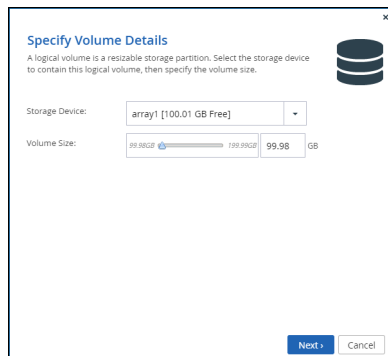
**To create or edit a volume:**

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

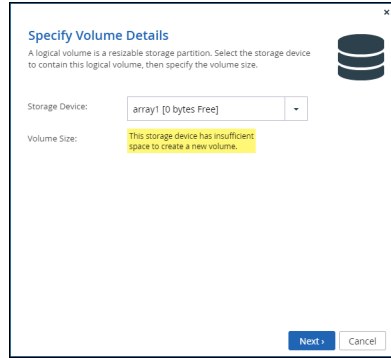


If a volume was not created when the HCP Anywhere Enterprise Edge Filer was installed, the page is empty.

2. Click **New** or select the volume to edit and click **Edit**. The **Specify Volume Details** window is displayed.



**Note:** If the selected disk storage is fully used, the following window is displayed:



3. Set the volume details:

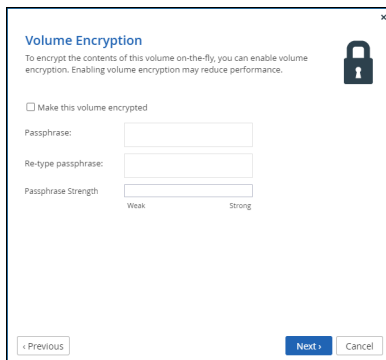
**Storage Device** – The array on which to create the volume. The size of each array is shown in brackets.

**Volume Size** – You can either drag the slider or enter a number of GB. Hitachi Vantara recommends that the volume size is set to the maximum available.

When adding to an existing array, the minimum size displayed is the size of the current volume. The volume size cannot be decreased.

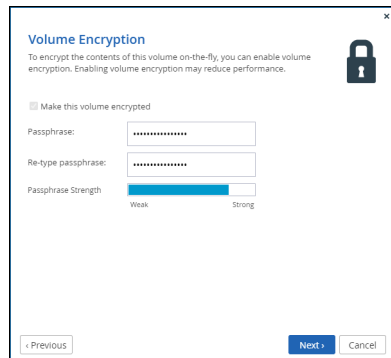
4. Click **Next**.

When defining a new volume you can choose to encrypt the volume.



**Make this volume encrypted** – Encrypt the contents of this volume using a passphrase. This option is disabled when editing a volume.

**Note:** After encrypting a volume, you can edit the volume to change the password, but not remove the encryption.



**Passphrase** – The passphrase to use to access the volume. The passphrase must be a

minimum 7 characters.

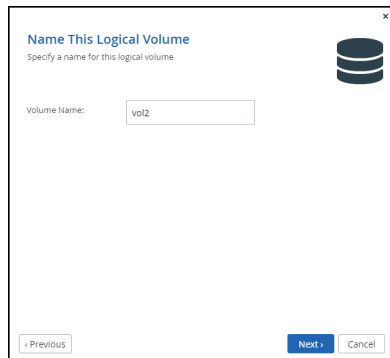
**Retype Passphrase** – Enter the same passphrase again to confirm it.

The encryption method employed is the Advanced Encryption Standard (AES-256 CBC ESSIV). Enabling volume encryption may reduce performance.

**Note:** It is important to keep the passphrase in a safe place as there is no way of retrieving it if you lose it. If you reset the HCP Anywhere Enterprise Edge Filer to its default settings, you cannot access the volume without this passphrase.

5. Click **Next**.

The **Name This Logical Volume** window is displayed.



6. If the volume is a new volume, enter a name for the volume.

**Note:** You cannot change the name of an existing volume.

7. Click **Next** and then click **Finish**.

The volume is displayed in the **Volumes** page.

## Deleting Volumes

To delete a volume, select the volume and click **Delete** and then **Yes** to confirm.

**Note:** You cannot delete a volume if it has data stored on it.

## Scanning and Repairing Volumes

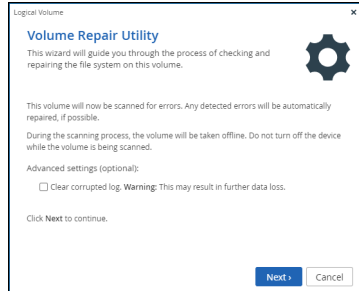
You can scan the file system on a volume for errors. Any detected errors are automatically repaired, if possible.

**Warning:** During the scanning process, the volume is taken off line. Do not turn off the HCP Anywhere Enterprise Edge Filer while the volume is being scanned.

**To scan and repair a volume:**

1. In the **Configuration** view, select **Storage > Volumes** in the navigation pane.
2. Select the volume and click **Repair**.

The **Volume Repair Utility** wizard is displayed.



3. Optionally, configure the settings for the repair operation.

4. Click **Next**.

While the files system on the volume is scanned for errors, the **Scanning & Repairing** window displays a progress bar, including what is being checked, such as inodes, blocks and sizes and group summary information.

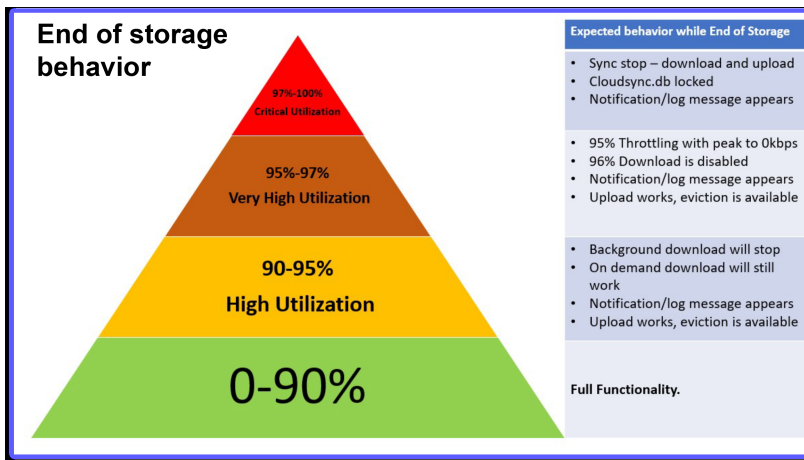
When the process is complete, the **Repair Complete** window displays a list of files system errors that were corrected.

5. Click **Finish**.

## Handling Volumes Close to Capacity

Handling situations when the storage volume is almost full is performed as follows:

- Background downloads are disabled when the disk is 90% full, and syncing is disabled when the disk is 97% full.
- When the storage volume is 1% less than the critically full value, the default being 97%, all downloads to the HCP Anywhere Enterprise Edge Filer are canceled.
- When the storage volume is 2% less than the critically full value, the default being 97%, throttling starts to slow down the writes to the volume.





# Managing Local Deduplication

HCP Anywhere Enterprise Edge Filers support file-level deduplication that reduces physical cache storage and improves performance when accessing stub files that already exists as another file on the HCP Anywhere Enterprise Edge Filer.

Files with the same content are linked to the same on-disk data, instead of taking twice the disk space. A deduped file, upon being modified, is populated with the underlying data.

Files are deduped:

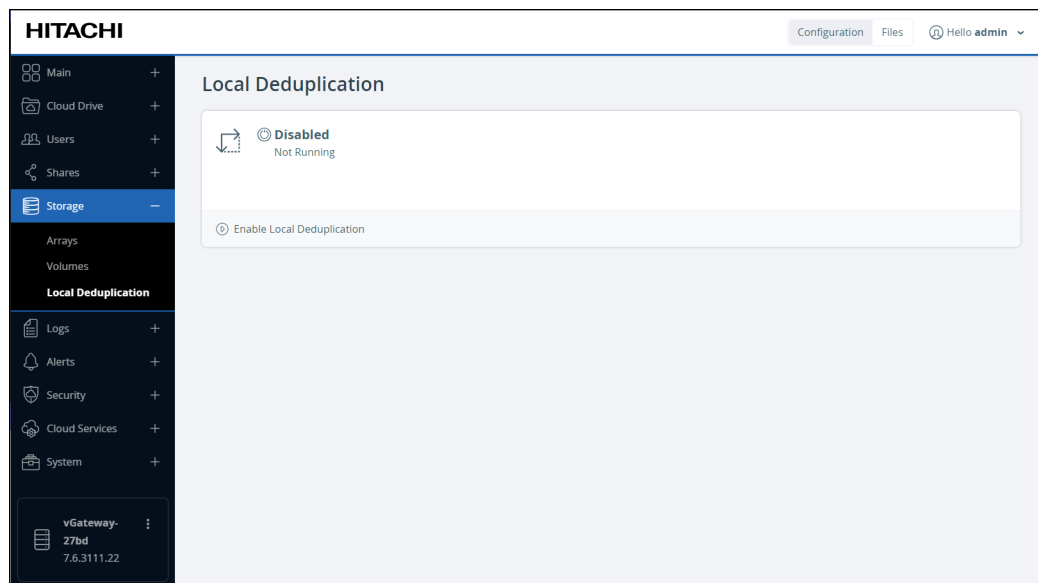
- During a copy and paste operation in Windows File Explorer or Mac Finder.
- After a file is modified locally, during the upload to the HCP Anywhere Enterprise Portal, the file will be deduplicated with a local copy of the data, if one exists.
- If a local copy exists before a download starts, deduplication is immediate and the file is not downloaded, saving the network traffic.

**Note:** If you enable deduplication and then run a migration, the file system is automatically reindexed. You must **not** restart the edge filer while the reindexing is being performed. If the edge filer is restarted while reindexing is being performed, any file that was not reindexed when the edge filer was restarted, is never evicted from the HCP Anywhere Enterprise Edge Filer.

**To enable local deduplication:**

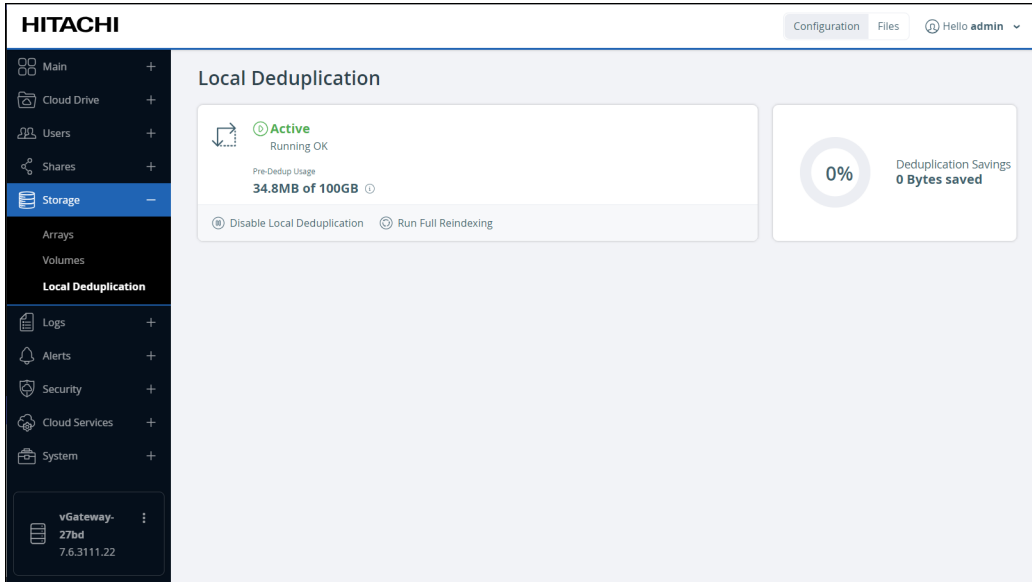
**Warning:** A restart is required when enabling deduplication.

1. In the **Configuration** view, select **Storage > Local Deduplication** in the navigation pane. The **Local Deduplication** page is displayed.



2. Click **Enable Local Deduplication**.
3. Click **OK** to confirm restarting the edge filer.

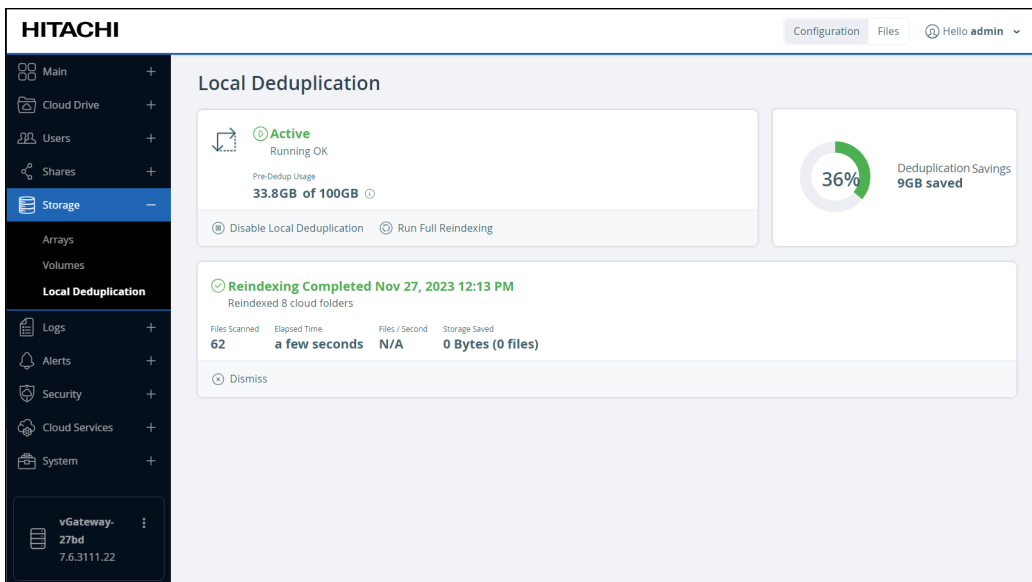
The HCP Anywhere Enterprise Edge Filer reboots. When logging back in to the HCP Anywhere Enterprise Edge Filer, local deduplication is enabled.



The **Local Deduplication** page shows storage usage prior to applying deduplication and the storage saved after applying deduplication as a percentage of the storage and as an amount of storage actually saved.

Existing files are not deduped, unless you reindex the HCP Anywhere Enterprise Edge Filer, described in [Applying Local Deduplication to Existing Files](#).

After reindexing the HCP Anywhere Enterprise Edge Filer, or after adding new files that can be deduped, the page shows the amount of storage saved by deduplication.

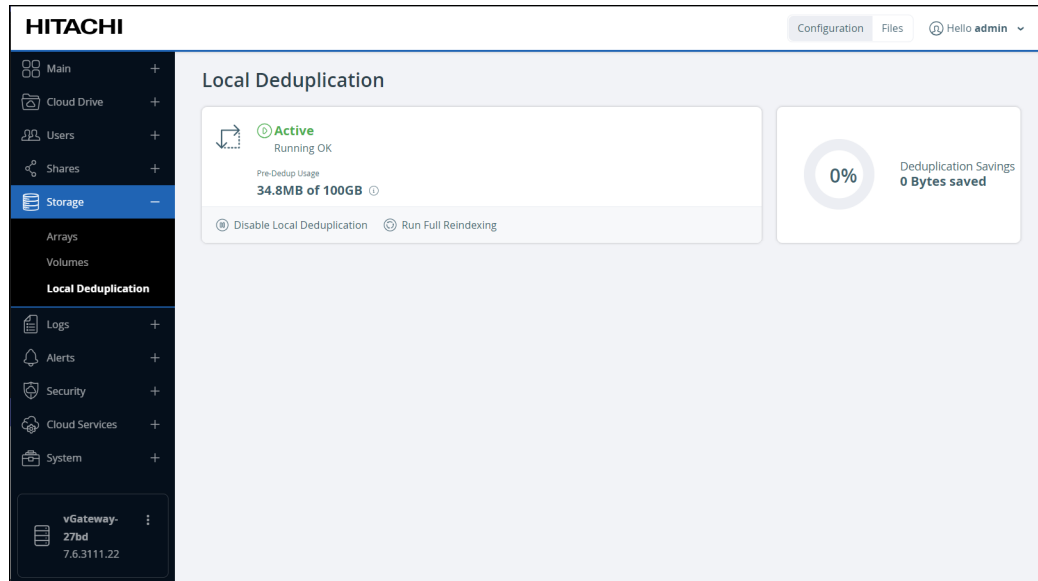


## Applying Local Deduplication to Existing Files

Deduplication is only applied to files added after deduplication is enabled unless reindexing is performed.

### To reindex the HCP Anywhere Enterprise Edge Filer:

1. In the **Configuration** view, select **Storage > Local Deduplication** in the navigation pane.
2. The **Local Deduplication** page is displayed.



3. Click **Run Full Reindexing**.

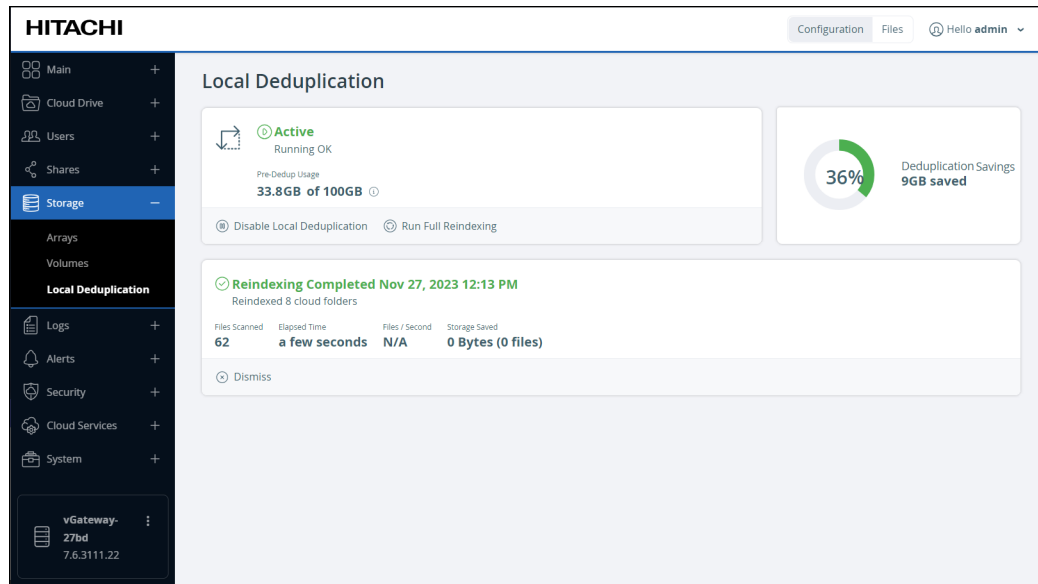
The progress of the reindexing is displayed.

## Disabling Local Deduplication

To disable local deduplication:

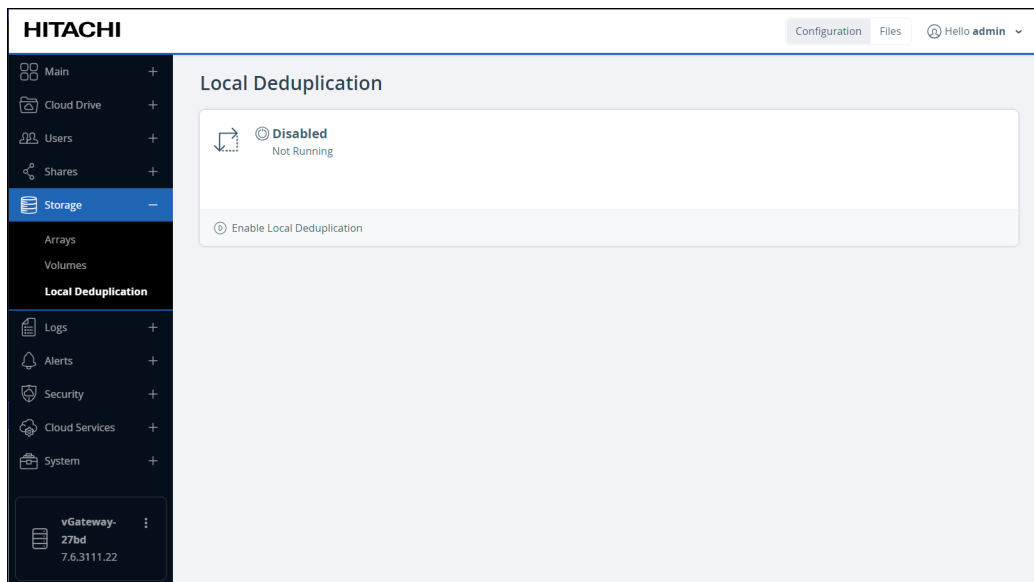
**Warning:** A restart is required when enabling deduplication.

1. In the **Configuration** view, select **Storage > Local Deduplication** in the navigation pane. The **Local Deduplication** page is displayed.



2. Click **Disable Local Deduplication**.
3. Click **OK** to confirm restarting the edge filer.

The HCP Anywhere Enterprise Edge Filer reboots. When logging back in to the HCP Anywhere Enterprise Edge Filer, local deduplication is disabled.



## Logging Deduplication

The percentage of deduplication for each deduped file is reported in the [Cloud Sync Log](#).

## Increasing Available HCP Anywhere Enterprise Edge Filer Storage

You can increase the volume size when the volume defined in the HCP Anywhere Enterprise Edge Filer does not use all the available storage, as described in [Managing Volumes](#).

When the volume defined in the HCP Anywhere Enterprise Edge Filer **does** use all the available storage and the initial storage allocated was not the maximum allowed by the license, you can increase the storage by either increasing the size of the disk or adding another existing disk.

**Note:** Hitachi Vantara recommends, whenever possible, increasing the size of the disk rather than adding a new disk, except for HCP Anywhere Enterprise Edge Filers running on an ESXi platform.

The amount of storage that can be used by a HCP Anywhere Enterprise Edge Filer 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 128TB.
- For an EV256 license the maximum 256TB.

## HCP Anywhere Enterprise Edge Filer in AWS

The following procedure includes creating a snapshot of the existing volume as a backup.

### To increase storage:

1. Log in to your Amazon Web Services account.  
Perform the following steps to take a snapshot of the HCP Anywhere Enterprise Edge Filer database EBS volume as a backup.
  - a) In the **Amazon Web Services > Compute** area, click **EC2**.  
The **EC2 Dashboard** screen is displayed.
  - b) In the navigation pane, click **ELASTIC BLOCK STORE > Volumes**.  
The **ELASTIC BLOCK STORE > Volumes** screen is displayed.
  - c) Locate the EBS volume to enlarge, right-click it and click **Create Snapshot**.  
The **Create Snapshot** pane is displayed.
  - d) Optionally, enter a description for the snapshot.
  - e) Click **Create Snapshot**.
2. In the Amazon Web Services EC2 Dashboard under **ELASTIC BLOCK STORE > Volumes**, locate the currently attached database EBS volume to enlarge, right-click it and click **Modify Volume**.  
The **Modify Volume** window is displayed.
3. Specify a disk size greater than the current size. When configured as a Caching Gateway,

Hitachi Vantara recommends storage at least 20% of the HCP Anywhere Enterprise Portal Global Name Space. The maximum usable 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 128TB.
- For an EV256 license the maximum 256TB.

4. Click **Modify**.
5. Follow the instructions in the procedure *To create or edit a volume in Managing Volumes*.

## HCP Anywhere Enterprise Edge Filer in ESXi

**Note:** Hitachi Vantara recommends adding a new disk rather than increasing the size of the disk. ESXi limits disks to a maximum of 62TB. If more than 62TB is required you **must** use more than one virtual disk. Storage greater than 62TB is only applicable to HCP Anywhere Enterprise Edge Filers with an EV64, EV128, or EV256 license.

### To increase available HCP Anywhere Enterprise Edge Filer storage:

1. In the vSphere Client, right-click the HCP Anywhere Enterprise Edge Filer VM and select **Edit Settings**.  
The configuration is displayed for the HCP Anywhere Enterprise Edge Filer.
2. Click **ADD NEW DEVICE** and select **Hard Disk** from the drop-down menu.
3. Specify the disk size. Hitachi Vantara recommends that the storage is at least 20% of the HCP Anywhere Enterprise Portal Global Name Space. The maximum usable 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 128TB.
  - For an EV256 license the maximum 256TB.

**Note:** A VMware ESXi host limits disks to a maximum of 62TB. To support storage greater than 62TB, you need to create multiple disks, each less than 62TB and then add the new disk to the storage array.
4. Click **OK**.
5. Restart the HCP Anywhere Enterprise Edge Filer. For details, see [Restarting the HCP Anywhere Enterprise Edge Filer](#).
6. In the **Configuration** view, select **Storage > Arrays** in the navigation pane.
7. Select the array and click **Edit**.  
The **Select drives to join this array** wizard is displayed, which shows you all drives available and asks you to select drives to join the array.
8. Check the **Member** box for each drive to include in the array.
9. Click **Next** to the end of the wizard and then click **Finish**.
10. Follow the instructions in the procedure *To create or edit a volume in Managing Volumes*.

## HCP Anywhere Enterprise Edge Filer in Hyper-V

### To increase available HCP Anywhere Enterprise Edge Filer storage when the current disk is Dynamically expanding:

**Note:** You can only expand a disk in Hyper-V if it was initially defined as **Dynamically expanding**. If it was defined as **Fixed size**, you can add another disk but you cannot expand the existing disk. For details of adding another disk, see the procedure *To increase available HCP Anywhere Enterprise Edge Filer storage when the current disk is Fixed size*.

1. In the Hyper-V Manager, shut down the virtual machine.
2. Right-click the HCP Anywhere Enterprise Edge Filer VM and select **Settings**.  
The configuration is displayed for the HCP Anywhere Enterprise Edge Filer.
3. Choose the hard disk and click **Edit**.  
The **Edit Virtual Hard Disk Wizard** is displayed.
4. In the **Choose Action** page, select **Expand** and click **Next**.
5. Enter a new size greater than the current size. The maximum disk size is dependent on the HCP Anywhere Enterprise Edge Filer 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 128TB.
  - For an EV256 license the maximum 256TB.
6. Click **Finish**.
7. Start the virtual machine and follow the instructions in the procedure *To create or edit a volume* in Managing Volumes.

### To increase available HCP Anywhere Enterprise Edge Filer storage when the current disk is Fixed size:

**Note:** When the current disk is Fixed size and not Dynamically expanding, you must add additional virtual disks.

1. In the Hyper-V Manager, shut down the virtual machine.
2. Right-click the HCP Anywhere Enterprise Edge Filer VM and select **Settings**.  
The configuration is displayed for the HCP Anywhere Enterprise Edge Filer.
3. Select **SCSI Controller** and click **Add** to add a hard drive.
4. Click **New**.  
The **New Virtual Hard Disk Wizard** opens, displaying the **Choose Disk Format** window.
5. Choose the **VHDX** format and click **Next**.  
The **Choose Disk Type** window is displayed.
6. If you are not likely to increase the disk size, choose **Fixed size** otherwise, choose **Dynamically expanding**.  
**Note:** Using a dynamically expanding, thin provisioned, disk is initially very slow to format the disk in the HCP Anywhere Enterprise Edge Filer user interface.
7. Click **Next**.  
The **Specify Name and Location** window is displayed.
8. Specify a name and location for the disk and click **Next**.  
The **Configure Disk** window is displayed.
9. Specify the disk size. Hitachi Vantara recommends that the storage is at least 20% of the 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 128TB.
  - For an EV256 license the maximum 256TB.
10. Click **Next** to review the disk details and then click and **Finish**.
  11. Click **Apply**.

The disk is created.
  12. Click **OK**.
  13. Start the virtual machine.
  14. Log in to the HCP Anywhere Enterprise Edge Filer as an administrator.
  15. In the **Configuration** view, select **Storage > Arrays** in the navigation pane.
  16. Select the array and click **Edit**.

The **Select drives to join this array** wizard is displayed, which shows you all drives available and asks you to select drives to join the array.
  17. Check the Member box for each drive to include in the array.
  18. Click Next to the end of the wizard and then click Finish.
  19. Follow the instructions in the procedure To create or edit a volume in Managing Volumes.

## HCP Anywhere Enterprise Edge Filer in Other Platforms

For all other platforms, either increase the size of the virtual disk and then follow the instructions in [Managing Volumes](#), or add another disk to the virtual machine and then add the disk to an array, as described in [Managing Arrays](#).



---

## Chapter 4. Managing the HCP Anywhere Enterprise Edge Filer Users

In order to enable users to access shared folders, you must define the users in the HCP Anywhere Enterprise Edge Filer. You can:

- Grant the user access rights to network shares.
- Add a custom user group. The entire user group can then be granted access rights to network shares, and the access rights will apply to all members of the user group.
- Users can be grouped, as described in [Managing User Groups](#).
- Add the user to the built-in **Read Only Administrators** user group, which includes read-only access rights to view the settings in the **Configuration** view.
- Add the user to the built-in **Administrators** user group, which includes read-write access rights to view and modify settings in the **Configuration** view.

**Note:** Users and user groups are granted access rights to network shares during share configuration. See [Managing Local Shares](#).  
Users that are not members of the Administrators or Read Only Administrators user groups do not see the **Configuration** view.

To enable sharing files when the HCP Anywhere Enterprise Edge Filer is a Caching Gateway, as described in [Managing Caching](#), both HCP Anywhere Enterprise Portal users and HCP Anywhere Enterprise Edge Filer users must have matching names.

### Adding and Editing Users

You can add users to the HCP Anywhere Enterprise Edge Filer by connecting to Active Directory, or add local users.

When connecting to Active Directory, you can add users from a domain or from an Active Directory tree or forest: [Defining Users From an Active Directory Domain, Tree or Forest](#).

When adding local users to the HCP Anywhere Enterprise Edge Filer: [Adding and Editing Local Users](#).

**Note:** The Active Directory domain controller must be read/write and not read-only.

### Defining Users From an Active Directory Domain, Tree or Forest

When an Active Directory structure includes domains such that the HCP Anywhere Enterprise Edge Filer is joined to one domain, which is set up to trust a second domain, you set up ID mapping for the second domain on the HCP Anywhere Enterprise Edge Filer. The HCP Anywhere Enterprise Edge Filer can list users and groups, and users can access the resources on the HCP Anywhere Enterprise Edge Filer based on the permissions.

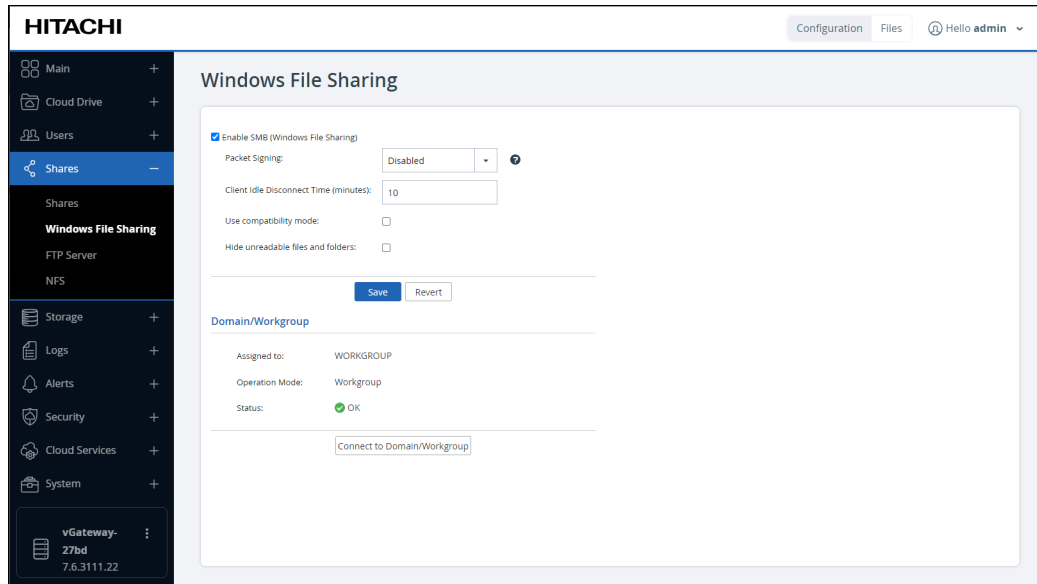
When the trust between domains is one way, for example, domain A is set up to trust domain B, but domain B is not set up to trust domain A, you can set up ID mapping for domain B on the HCP Anywhere Enterprise Edge Filer connected to domain A and users and groups from domain B can

access the HCP Anywhere Enterprise Edge Filer. But, if you connect the HCP Anywhere Enterprise Edge Filer to domain B, users and groups from domain A will not be able to access the HCP Anywhere Enterprise Edge Filer.

**Note:** The ID mapping range 1 to 199999 is reserved and must not be manually overwritten.

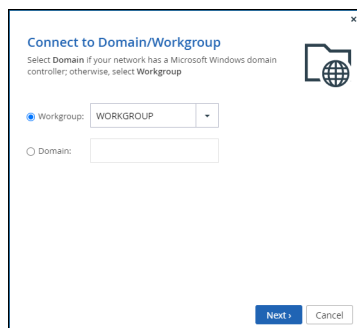
**To define users from an Active Directory domain:**

1. In the **Configuration** view, select **Shares > Windows File Sharing** in the navigation pane. The **Windows File Sharing** page is displayed.



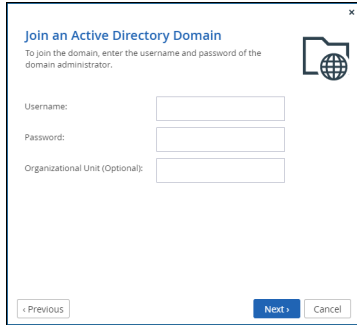
2. Click **Connect to Domain/Workgroup**.

The **Windows File Sharing** wizard opens, displaying the **Connect to Domain/Workgroup** window.



3. Choose **Domain** and type the domain name.
4. Click **Next**.

The **Join an Active Directory domain** window is displayed.



5. In the **Username** and **Password** fields, type the domain administrator's username and password.
6. 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.portal/Suffix*

**L**=Locality Name, for example, *London*

**ST**=State or Province Name, for example, *London*

**O**=Organization Name, for example, *HCP Anywhere Enterprise*

**OU**=Organizational Unit Name, for example, *Sales*

**C**=Country Name, for example, *GB*

**STREET**=Street Address

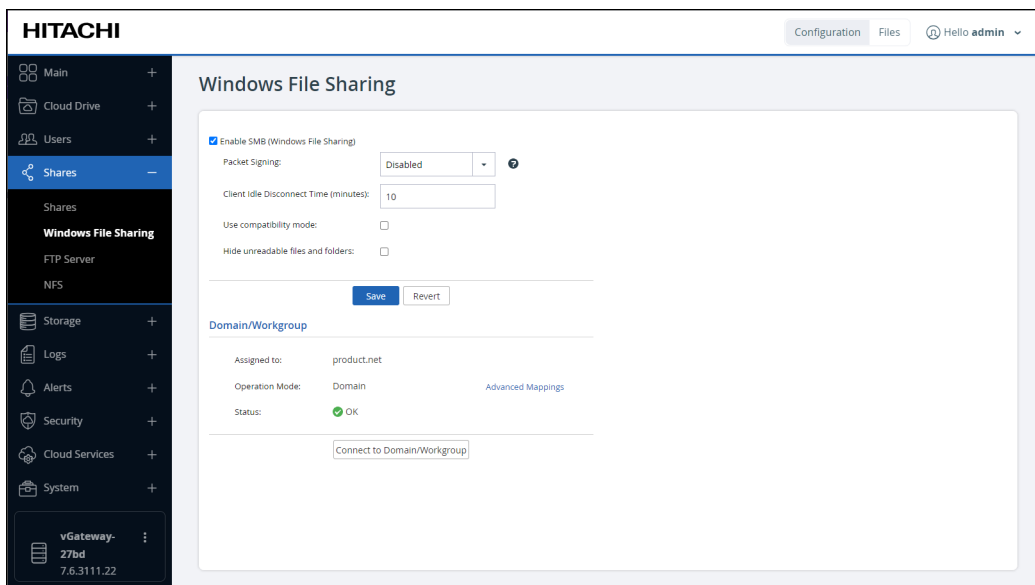
**DC**=Domain Component, for example, *com*

**UID**=Userid

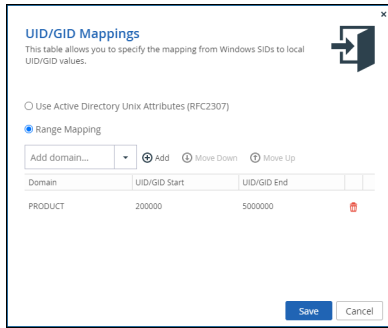
7. Click **Next** and then **Finish**.

**To define HCP Anywhere Enterprise Edge Filer users from for an Active Directory tree or forest:**

1. After setting up the Active Directory domain, in the Windows File Sharing page, in the Domain/Workgroup area, click the **Advanced Mappings** link.



The UID/GID Mapping window is displayed.



2. For each domain in the tree/forest displayed in the list of domains, specify the UID/GID range allocated on HCP Anywhere Enterprise for users and groups from Active Directory. The UID/GID range is defined by **UID/GID Start** value and **UID/GID End** value. This is set for each domain that is trusted in the Active Directory environment. The UID/GID range has a default minimum value of 200,000 in order to reserve a range for local accounts and system accounts to run on the system and should not be changed.

**Note:** The ID mapping range 1 to 199999 is reserved and must not be manually overwritten.

a) In the **Add domain** field, either type the desired domain's name, or select it from the drop-down list.

b) Click **Add**.

The domain is displayed in the table.

c) Leave the **UID/GID Start** field with the default value.

d) Click in the **UID/GID End** field and type the ending number in the range of HCP Anywhere Enterprise Edge Filer user and group IDs (UID/GID) that should be assigned to users and user groups from this domain. The end number is calculated as follows:

The RID, Relative ID, value, added to the UID/GID Start number.

The SID is the identity of a user in Active Directory. SIDs are represented in the following way: S-1-5-21-1180699209-877415012-3182924384-4850000, where the last part of the SID is the RID value, 4850000 in this SID example.


For example, if the RID is 4850000 and **UID/GID Start** is 200000, **UID/GID End** is  $4850000 + 200000 = 5050000$ .

3. To re-order the domains, do any of the following:

- To move a domain up in the table, click on the desired domain, then click **Move Up**.

- To move a domain down in the table, click on the desired domain, then click **Move Down**.

The order in which domains appear in the table represents the order in which the domains will appear in drop-down lists throughout the HCP Anywhere Enterprise Edge Filer user interface, for example, when managing access rights to projects.

4. To remove a domain, in the domain row, click the  icon.

The domain is not displayed in the table.

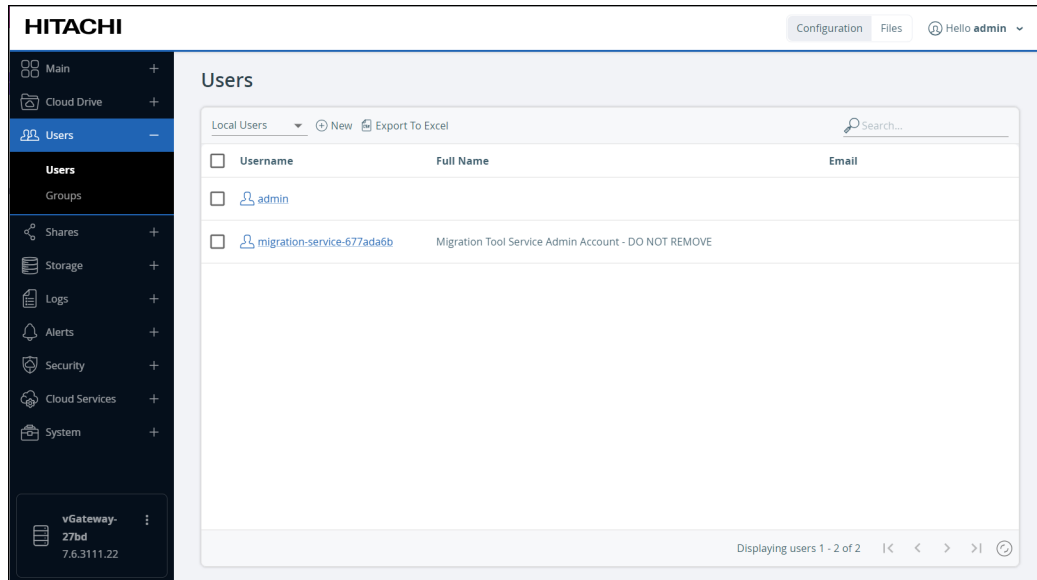
5. Click **Save**.

## Adding and Editing Local Users

You specify the local users who have access to the HCP Anywhere Enterprise Edge Filer.

### To add or edit a user:

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



**Note:** A **Migration Tool Service Admin Account** administrator is automatically added: `migration-service-n`, where `n` is a unique identifier. You must not delete this administrator.

2. To add a user, click **New**.

Or,

To edit a user, either click the user name or select the user row and click **Edit**.

The **Specify User Details** window is displayed. If you are editing an existing user, the window is displayed with the user details.

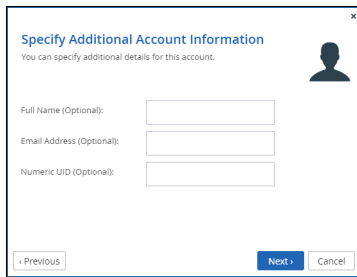
3. Specify the user details.

**Username** – A name for the user.

**Password** – A password for the user. The password must be at least eight characters and must include at least a letter, digit and special character, such as `~`, `@`, `#`, `$`, `%`, `^`, `&`, `(`. The password cannot contain the **Username** as part or all of the password.

**Retype password** – The same password you entered in the Password field.

4. Click **Next** and optionally specify additional account information:



The dialog box titled "Specify Additional Account Information" contains the following fields and buttons:

- Full Name (Optional):
- Email Address (Optional):
- Numeric UID (Optional):
- Buttons: Previous, Next, Cancel

**Full Name** – The full name of the user.

**Email Address** – The email address of the user.

**Numeric UID** – A numeric user ID (UID) to assign the user.

5. Click **Next** and then **Finish**.

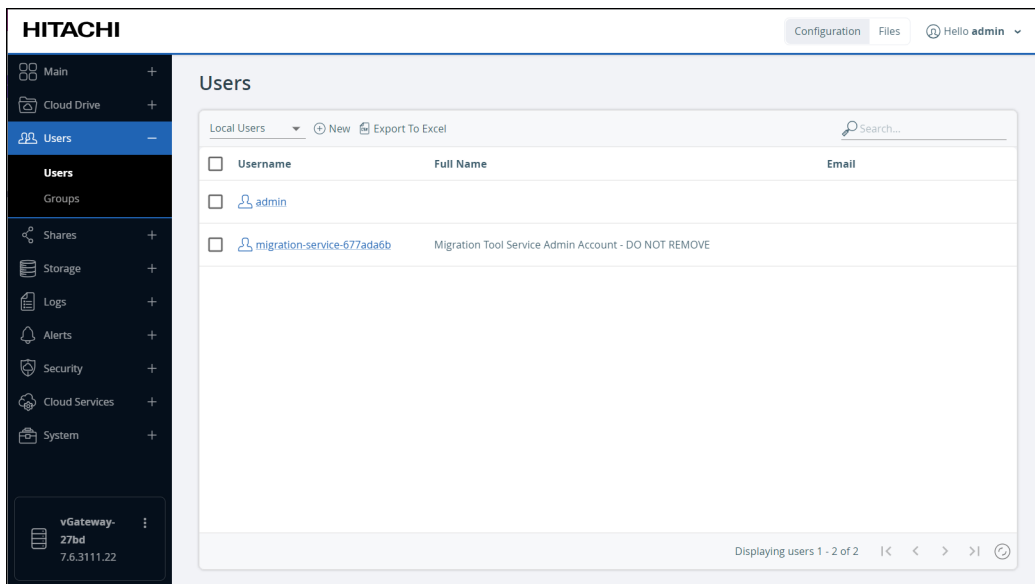
The new user is displayed on the **Users** page.

## Adding Users to User Groups

Users are added to user groups during user group configuration. See [Managing User Groups](#).

## Viewing Users

1. In the **Configuration** view, select **Users > Users** in the navigation pane. The **Users** page opens, displaying all local users.



The screenshot shows the HITACHI web interface. The left navigation pane is expanded to show the **Users** section. The main content area displays the **Users** page with the following elements:

- Header: HITACHI, Configuration, Files, Hello admin
- Navigation: Main, Cloud Drive, Users (selected), Groups, Shares, Storage, Logs, Alerts, Security, Cloud Services, System
- Users Page: Local Users, New, Export To Excel, Search...
- Table of Users:

<input type="checkbox"/>	Username	Full Name	Email
<input type="checkbox"/>	admin		
<input type="checkbox"/>	migration-service-677ada6b	Migration Tool Service Admin Account - DO NOT REMOVE	

Displaying users 1 - 2 of 2

2. To display domain users, in the **Local Users** drop-down list, select **Domain *domain* Users**, where *domain* is the name of the domain.

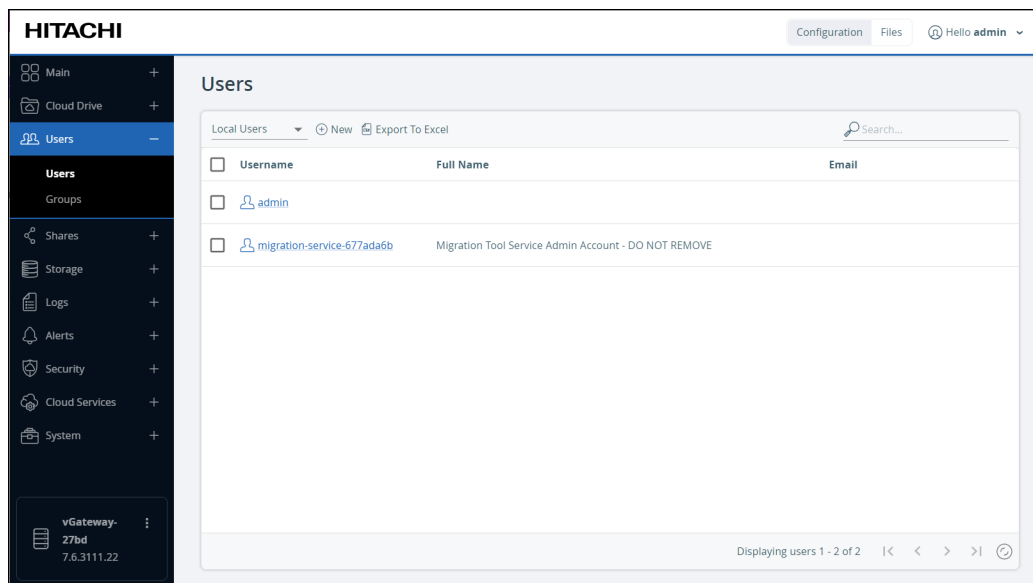
All domain users are displayed.

## Exporting the List of Users

You can export a list of users and their details to a Comma-Separated Values (CSV) file on your computer. You can then view the file as a worksheet in Microsoft Excel.

### To export a list of users:

1. In the **Configuration** view, select **Users > Users** in the navigation pane. The **Users** page opens, displaying all local users.



2. Click **Export to Excel**.

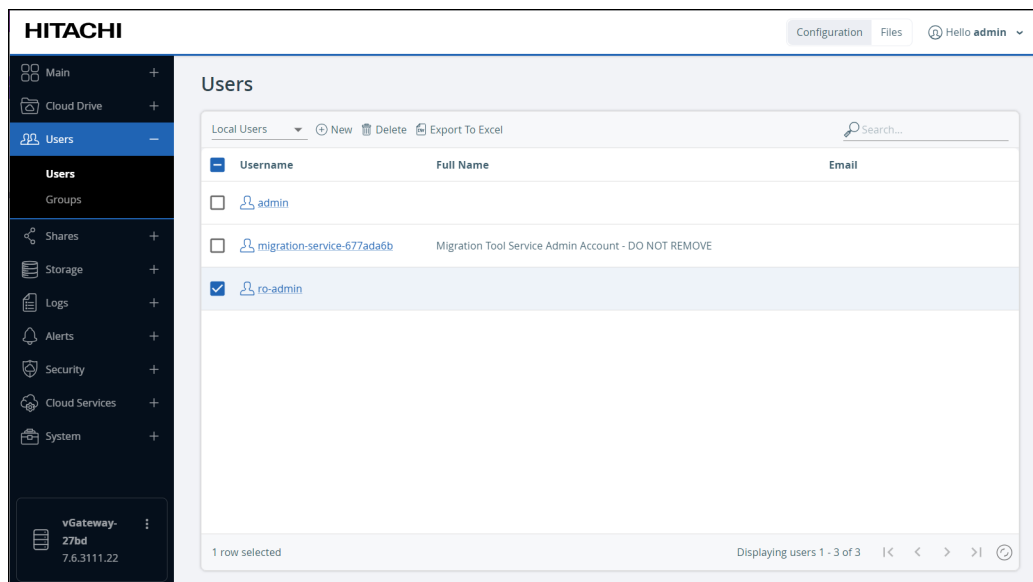
The users list is exported.

## Deleting Users

**Note:** You cannot delete the main administrator account.

### To delete a user:

1. In the **Configuration** view, select **Users > Users** in the navigation pane. The **Users** page opens, displaying all local users.
2. Select the user row and click **Delete**.



**Note:** The **Delete** option is displayed after selecting the row of the user to delete.

3. Click **Delete** to confirm.

The user is deleted.

## Managing User Groups

The HCP Anywhere Enterprise Edge Filer includes built-in user groups. You can create additional user groups to meet your organization's requirements. It is possible to add each user to more than one group.

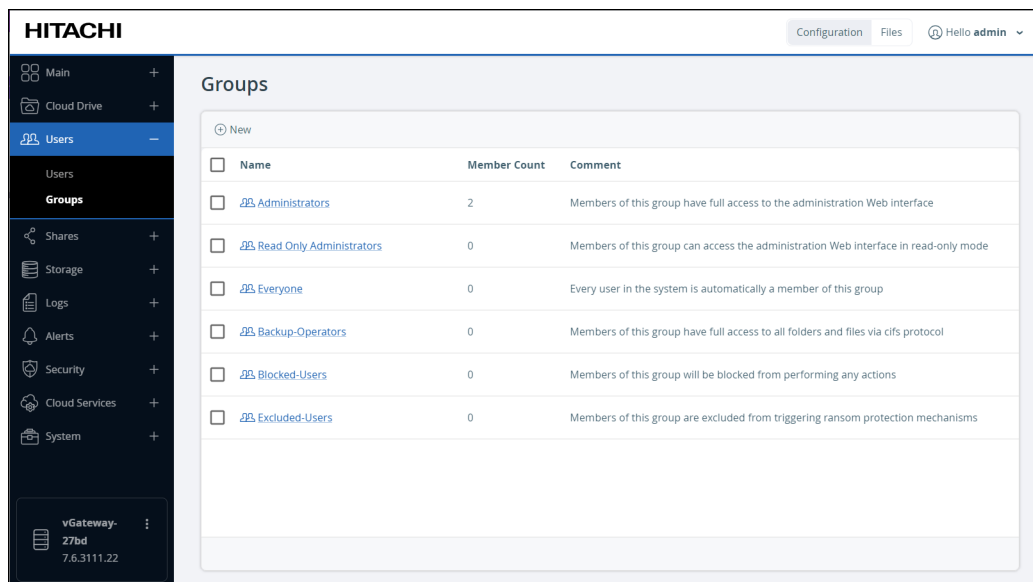
**Warning:** The built-in user groups must not be deleted.

HCP Anywhere Enterprise Edge Filer administrators can create local groups with nested Active Directory groups. Nesting Active Directory groups within local groups is useful when addressing frequent changes in branch user hierarchies. The **Backup-Operators** group initially has no members and is for users who require access to backup files and folders, even if they do not have the correct ACL permissions.

**To add or edit a user group:**

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



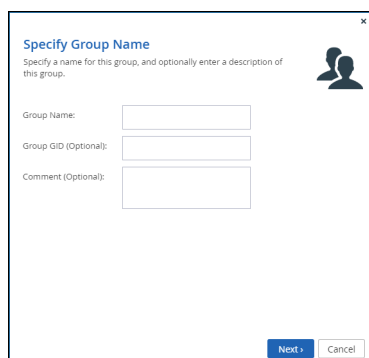


2. To add a group, click **New**.

Or,

To edit a group, either click the group name or select the group row and click **Edit**.

The **Specify Group Name** window is displayed. If you are editing an existing group, the window is displayed with the group details.



**Note:** You cannot edit the **Group Name** of the built-in groups, such as **Administrators** and **Read Only Administrators**.

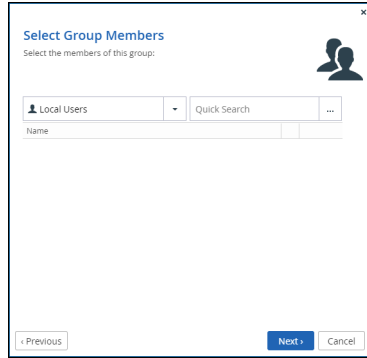
3. Specify the group name and, optionally, other details.

The following reserved names cannot be used:

Administrator, Backup Operators, Domain Admins, Domain Computers, Domain Controllers, Domain Guests, Domain Users, Guest, Guests, Network, Self, Service, Users

**Note:** Upgrading from a version that has one of these names as a group name causes a warning to be written to the log.

4. Click **Next** and select the group members, either from **Local Users**, or from **Domain domainName Users**, or from **Domain domainName Groups**.



- a) Select the group whose member you want to include.
  - b) Either start to enter a user name in the **Quick Search** text box or, click and select the user from the list.
5. When you are done adding users, click **Next** and then **Finish**.

## Deleting User Groups

To delete a user group, select the group row, click **Delete**, and then click **Yes** to confirm.

**Note:** Deleting a user group does not delete the group members.  
Built-in groups, such as *Administrators* and *Read Only Administrators*, cannot be deleted.

If the deleted user group had been granted access rights to network shares, the group members will no longer have access rights to those network shares. To assign individual users access rights to network shares, see [Managing Local Shares](#).

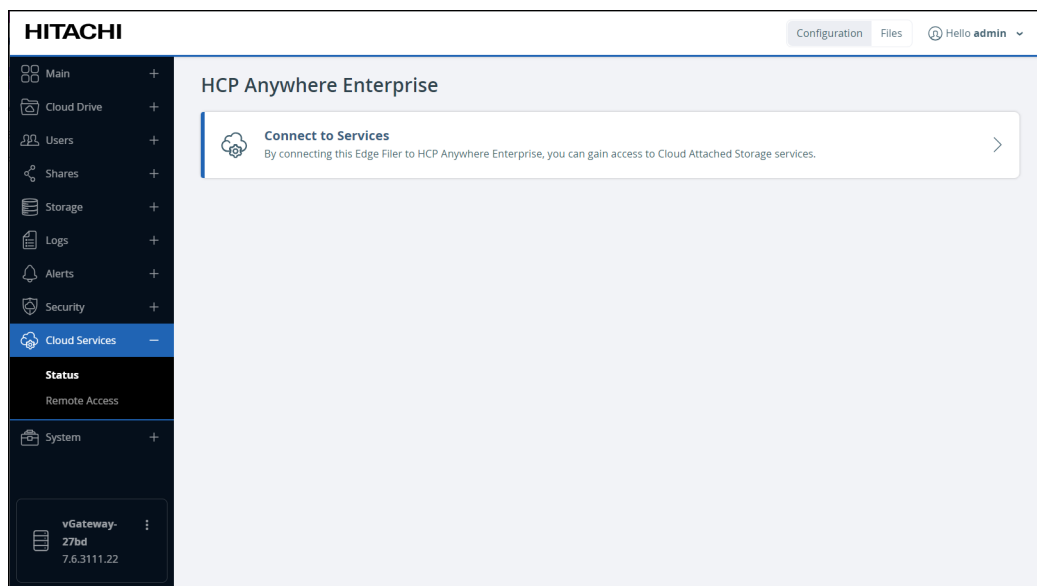
# Chapter 5. Using HCP Anywhere Enterprise Edge Filer Cloud Services

You connect the HCP Anywhere Enterprise Edge Filer to the HCP Anywhere Enterprise Portal using an administrator account. During the initial HCP Anywhere Enterprise Edge Filer setup, described in the installation guide, you connect the HCP Anywhere Enterprise Edge Filer to the HCP Anywhere Enterprise Portal.

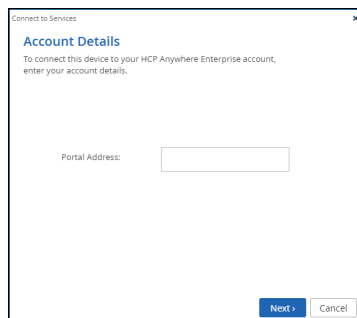
**Note:** If access using CAC, Common Access Card, has been enabled for the HCP Anywhere Enterprise Portal, the HCP Anywhere Enterprise Edge Filer connects to the HCP Anywhere Enterprise Portal using an activation code instead of the user and password credentials. For details, contact Hitachi Vantara support.

## To connect the HCP Anywhere Enterprise Edge Filer to a HCP Anywhere Enterprise Portal:

1. In the **Configuration** view, select **Cloud Services > Status** in the navigation pane. The **HCP Anywhere Enterprise** page is displayed.



2. Click **Connect to Services**.

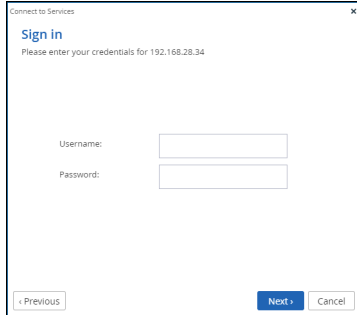


The **Account Details** window is displayed.

3. Enter the address of the HCP Anywhere Enterprise Portal, and then 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 device into the portal, offering the option to proceed anyway. This warning is presented every time a user connects a device to the portal, until a valid certificate is installed.

The **Sign In** window is displayed.



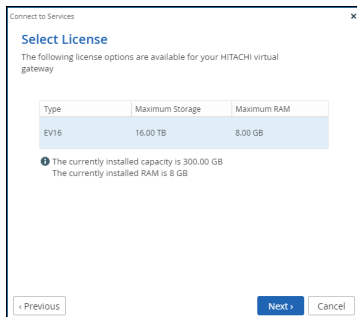
**Note:** If single sign-on has been set up to the HCP Anywhere Enterprise Portal, click **Sign In** and then **Allow** in a separate window when prompted, and then the **Select License** window is displayed, skipping the next step.

4. Enter the HCP Anywhere Enterprise Portal designated user username and password to access the HCP Anywhere Enterprise Portal.

**Note:** The designated user is the owner of the cloud folders and data to manage the HCP Anywhere Enterprise Edge Filer connection to the HCP Anywhere Enterprise Portal for all users and not just the current user. This designated user has HCP Anywhere Enterprise Portal read/write administrator permissions.

5. Click **Next**.

The **Select License** window is displayed.



Type	Maximum Storage	Maximum RAM
EV16	16.00 TB	8.00 GB

You are prompted to select the license from those available on the HCP Anywhere Enterprise Portal.

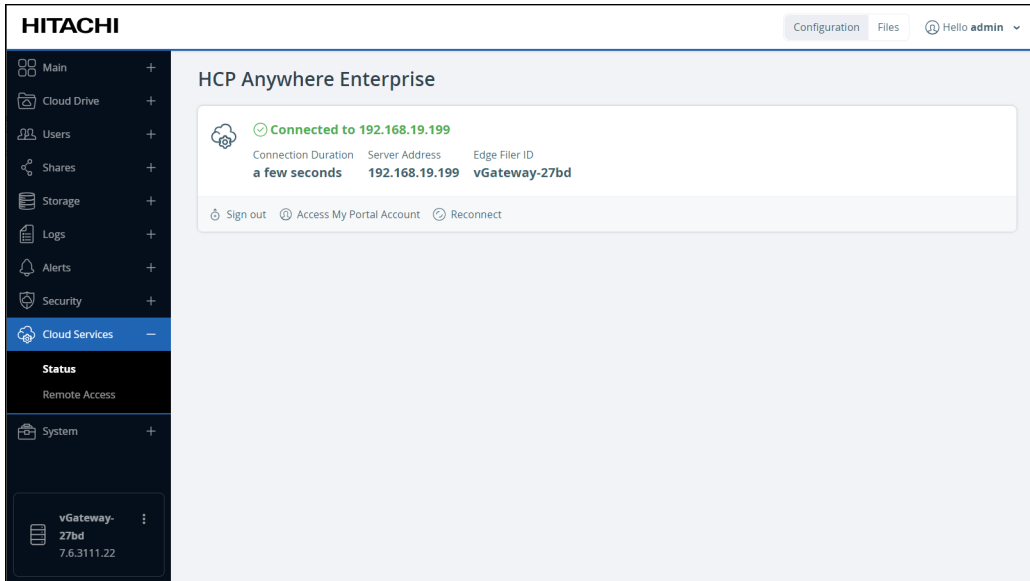
**Note:** If only one license is available, this license is selected automatically.

6. Select the license and click **Next**.

The HCP Anywhere Enterprise Edge Filer connects to the HCP Anywhere Enterprise Portal and is added to the HCP Anywhere Enterprise Portal account. A success window is displayed.

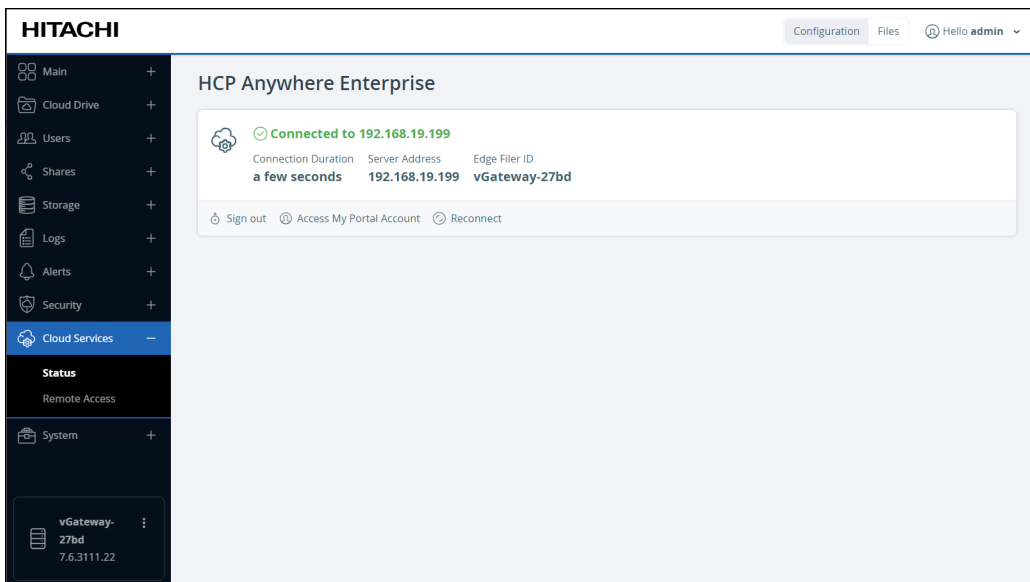
7. Click **Finish**.

The HCP Anywhere Enterprise Portal page is displayed, showing that the HCP Anywhere Enterprise Edge Filer is connected to the HCP Anywhere Enterprise Portal.



## Viewing the Connection to a HCP Anywhere Enterprise Portal Status

The **HCP Anywhere Enterprise** page displays information about the HCP Anywhere Enterprise Edge Filer connection to a HCP Anywhere Enterprise Portal account.



After connecting to a HCP Anywhere Enterprise Portal the HCP Anywhere Enterprise Edge Filer status panel shows the following:

- The status of the connection to the HCP Anywhere Enterprise Portal can be one of the following:

**Resolving the portal address** – The HCP Anywhere Enterprise Edge Filer is resolving the HCP Anywhere Enterprise Portal address.

**Connected to *portal*** – The HCP Anywhere Enterprise Edge Filer is connected to the HCP Anywhere Enterprise Portal named *portal* or with the IP address *portal*, and the connection is currently in use.

**Connecting** – The HCP Anywhere Enterprise Edge Filer is connecting to the HCP Anywhere Enterprise Portal.

**Disconnected** – The HCP Anywhere Enterprise Edge Filer is disconnected from the HCP Anywhere Enterprise Portal. You can reconnect as described in [Reconnecting and Disconnecting to a HCP Anywhere Enterprise Portal](#).

**Authenticating** – The HCP Anywhere Enterprise Edge Filer is authenticating to the HCP Anywhere Enterprise Portal.

**Connection Failed** – The connection to the HCP Anywhere Enterprise Portal failed.

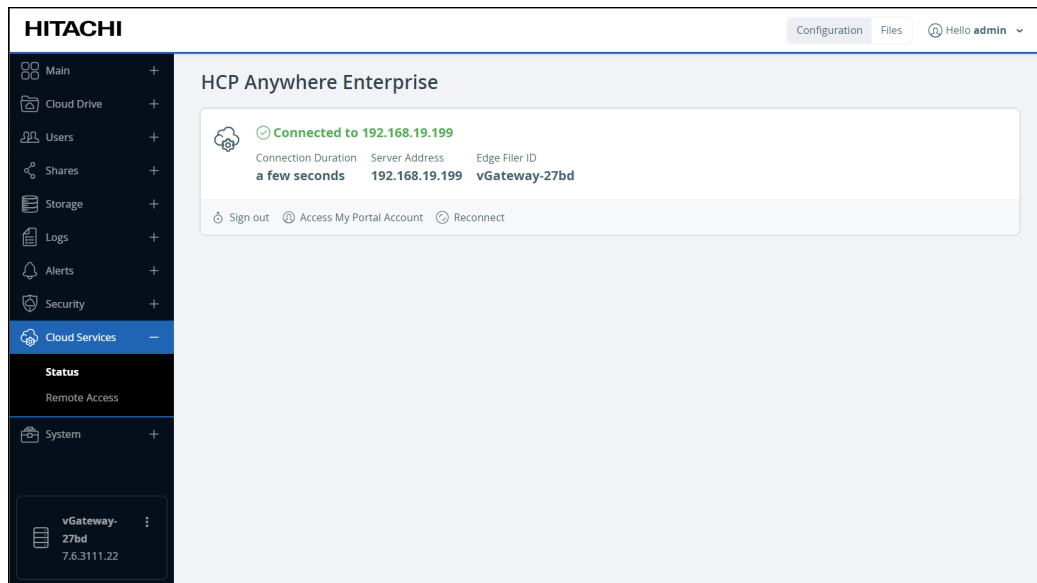
- The amount of time that the HCP Anywhere Enterprise Edge Filer has been connected to the HCP Anywhere Enterprise Portal.
- The IP address of the HCP Anywhere Enterprise Portal.
- The HCP Anywhere Enterprise Edge Filer identifier used by the HCP Anywhere Enterprise Portal.

## Managing the Connection to a HCP Anywhere Enterprise Portal

After connecting a HCP Anywhere Enterprise Edge Filer to a HCP Anywhere Enterprise Portal, you can access the HCP Anywhere Enterprise Portal account.

### To access the HCP Anywhere Enterprise Portal account:

1. In the **Configuration** view, select **Cloud Services > Status** in the navigation pane. The **HCP Anywhere Enterprise** page is displayed.



2. Click **Access My Portal Account**.

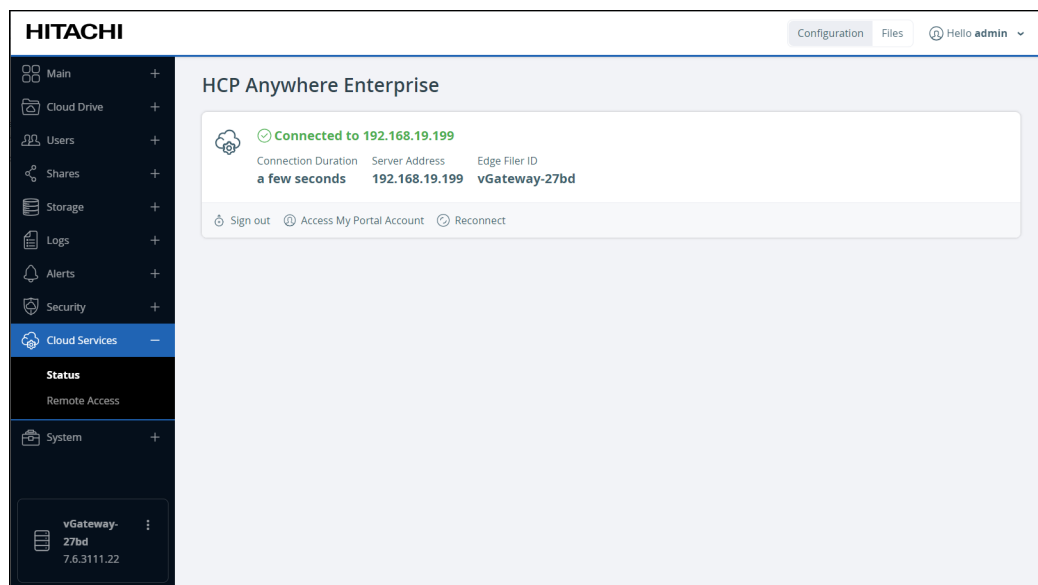
The HCP Anywhere Enterprise Portal sign in page is displayed in a new window, and you can sign in and access the account. For details about using the HCP Anywhere Enterprise Portal account, refer to HCP Anywhere Enterprise Portal documentation.

## Reconnecting and Disconnecting to a HCP Anywhere Enterprise Portal

If the connection to the HCP Anywhere Enterprise Portal is lost due to a connectivity failure, the HCP Anywhere Enterprise Edge Filer automatically reconnects when it detects that the HCP Anywhere Enterprise Portal is available. To force the HCP Anywhere Enterprise Edge Filer to immediately try to reconnect, click Reconnect. The connection status displays whether the reconnection attempt is successful or not.

### To disconnect from a HCP Anywhere Enterprise Portal:

1. In the **Configuration** view, select **Cloud Services > Status** in the navigation pane. The **HCP Anywhere Enterprise** page is displayed.



2. Click **Sign out** and **Yes** when the confirmation message is displayed.

## Managing Caching

Content is synced between the HCP Anywhere Enterprise Portal global file system and the HCP Anywhere Enterprise Edge Filers connected to the HCP Anywhere Enterprise Portal. Folder content is identical across all the HCP Anywhere Enterprise Edge Filers connected to the HCP Anywhere Enterprise Portal. Whenever any change of any kind is made to any file in any of the synced folders, the same change is made immediately in the other synced folders. For example, if a file is deleted from one of the folders, the same file is deleted from the other synced folders. It makes no difference which user made the change or in which of the synced folders the change was made.

**Note:** Every 7 days a task runs in the background to verify that all the files on the HCP Anywhere Enterprise Edge Filer are synced with the HCP Anywhere Enterprise Portal global file

system. Any files on the HCP Anywhere Enterprise Edge Filer that are not synced with the HCP Anywhere Enterprise Portal global file system are automatically synced. Each HCP Anywhere Enterprise Portal user accesses the content that was synced to the HCP Anywhere Enterprise Edge Filer according to the permission set defined for their access on the HCP Anywhere Enterprise Portal.

When the HCP Anywhere Enterprise Portal is connected to the HCP Anywhere Enterprise Edge Filer, the folder structure defined in the HCP Anywhere Enterprise Portal global file system is created automatically on the HCP Anywhere Enterprise Edge Filer when the HCP Anywhere Enterprise Edge Filer syncs with the HCP Anywhere Enterprise Portal. Setting up the HCP Anywhere Enterprise Edge Filer to enable syncing is dependent on a number of considerations:

- Do you need to maintain the file structure and ACLs after migrating the data to a HCP Anywhere Enterprise Edge Filer?  
In this case, the setup should be done using nested shares.  
Even if a folder is shared with a user but the folder has no ACL access permissions, when the user attempts to access the folder a message similar to the following is displayed: `You have no permission to view this folder.`
- Do you need to maintain the file structure, but not the ACLs, after migrating the data to a HCP Anywhere Enterprise Edge Filer?  
In this case, the setup should be done using nested shares.  
Access to files is determined by the authorization levels set in the HCP Anywhere Enterprise Portal, such as *Read/Write* or *Preview Only*.

HCP Anywhere Enterprise recommends whenever possible to set up the HCP Anywhere Enterprise Edge Filer using nested shares.

Setting up the HCP Anywhere Enterprise Edge Filer for caching offers the following advantages:

- Content can be synced between different branch HCP Anywhere Enterprise Edge Filers and with the HCP Anywhere Enterprise Portal global file system. This means that the data is available for users to access at the branch at LAN speed, as well as when they are roaming outside the office.
- Users can sync files across their own devices. Syncing files allows users with multiple personal devices, such as a desktop computer, laptop, and smartphone, to take their files with them effortlessly wherever they go, with the confidence that the files they are working on are always current. Users do not even need to remember which device they were working on when they last modified a file. For example, you can create a file on your laptop and later open and modify it from your desktop.
- Users can collaborate easily with others. You can sync any number of shared folders and everyone who syncs the shared folder can view, update, and delete the files in the shared folder.

## Storage With a Caching Gateway

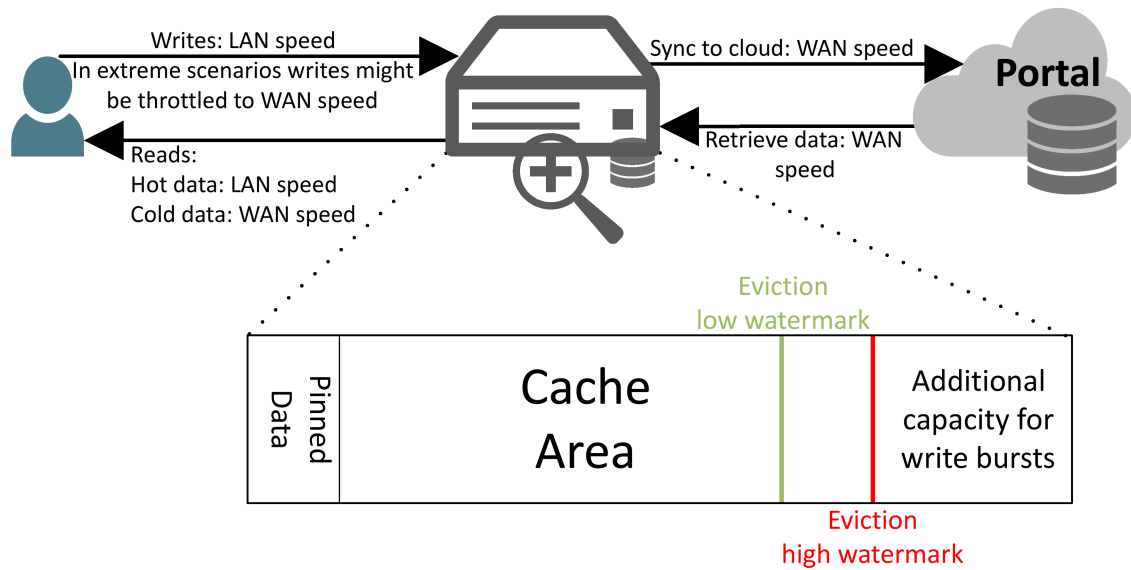
With a Caching Gateway, files are stored in cloud storage and only stored on the HCP Anywhere Enterprise Edge Filer when required. However, all the metadata is downloaded to the HCP Anywhere Enterprise Edge Filer so users have access to everything that they have permission to access on the HCP Anywhere Enterprise Portal. Changes to the metadata in the HCP Anywhere Enterprise Portal are reflected in the HCP Anywhere Enterprise Edge Filer, but the content itself is not stored on the HCP Anywhere Enterprise Edge Filer. Only what is being worked on at the



moment or what is wanted to be permanently available is stored on the HCP Anywhere Enterprise Edge Filer. The files that have not been downloaded to the HCP Anywhere Enterprise Edge Filer are displayed in the HCP Anywhere Enterprise Edge Filer as stubs, which take up very little storage.

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. Streamed files are added to a background download queue. After the download has completed, the file is unstubbed. Any changes to the file are synced back to the HCP Anywhere Enterprise Portal. Folders with files that are always required can be marked in the HCP Anywhere Enterprise Edge Filer user interface as pinned, in which case the files, and not the stubs, are stored on the HCP Anywhere Enterprise Edge Filer. For more details about pinned files, see [Pinning Folders so that Files are Always Available Locally](#).

Files on the HCP Anywhere Enterprise Edge Filer are referred to as hot files. Less frequently accessed files, that remain in the cloud managed by HCP Anywhere Enterprise Portal, are referred to as cold files. Files that have not been accessed recently are evicted when the amount of storage used reaches a high watermark. The HCP Anywhere Enterprise Edge Filer also has spare capacity to absorb common write bursts at LAN speed. This means that users do not require access to the cloud and the additional slowness that is implied with this access is avoided during these bursts. For more details about evicting files, see [File Eviction from the HCP Anywhere Enterprise Edge Filer](#).



Any file in either the pinned data area or cache area is available at LAN speed.

Accessing a file from the HCP Anywhere Enterprise Portal global file system causes the file to be downloaded and opened without delay, and where possible, large files are streamed from the cloud so that the user can access the file before it has been completely downloaded. Where possible, random access within the file is also supported, so the user does not have to wait for a sequential stream to complete to access parts of the file.

Files that were updated in the HCP Anywhere Enterprise Portal global file system and are defined as hot files, are downloaded automatically to the HCP Anywhere Enterprise Edge Filer in

background, so that when they are required, the user will have access to the up-to-date version of the file at LAN speed.

## File Eviction from the HCP Anywhere Enterprise Edge Filer

As the HCP Anywhere Enterprise Edge Filer storage space gets used up, the HCP Anywhere Enterprise Edge Filer starts to remove, evict, files leaving stubs on the HCP Anywhere Enterprise Edge Filer. Files start to be evicted only when the amount of storage used reaches the high watermark, 75% of the total HCP Anywhere Enterprise Edge Filer storage. At this point, files are evicted until the amount of storage used is equal to, or less than, the low water mark, 65% of the total HCP Anywhere Enterprise Edge Filer storage.

The following hot files are never evicted, so they are always available at LAN speed:

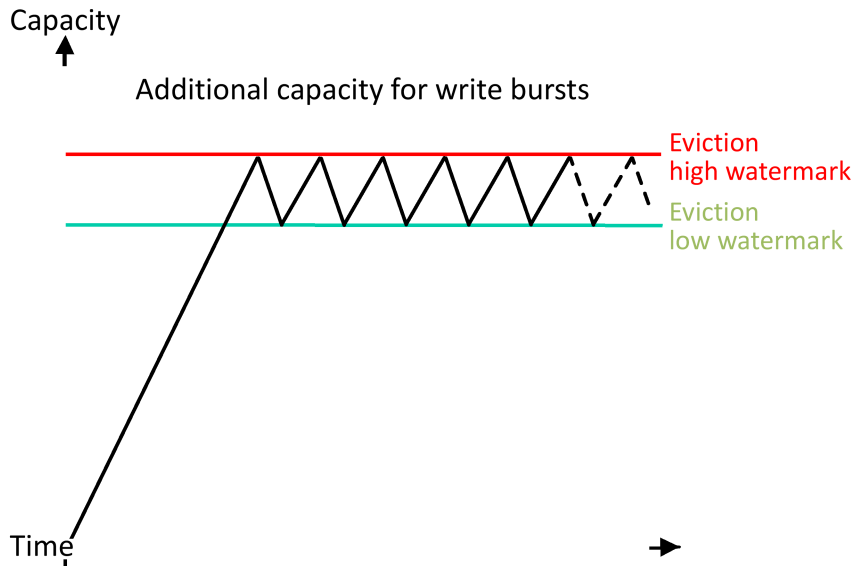
- Files in a folder marked in the HCP Anywhere Enterprise Edge Filer as pinned. These files are downloaded to the HCP Anywhere Enterprise Edge Filer and never evicted.
- Files that are currently open.
- Files that have not yet been synced to the HCP Anywhere Enterprise Portal. For example, a new file on the HCP Anywhere Enterprise Edge Filer or a file that was edited but not yet synced.

Other hot files can be evicted. These files are grouped according to the time since they were last accessed. The files are evicted within these groups, the files in the oldest group first, followed by the files in the next oldest group.

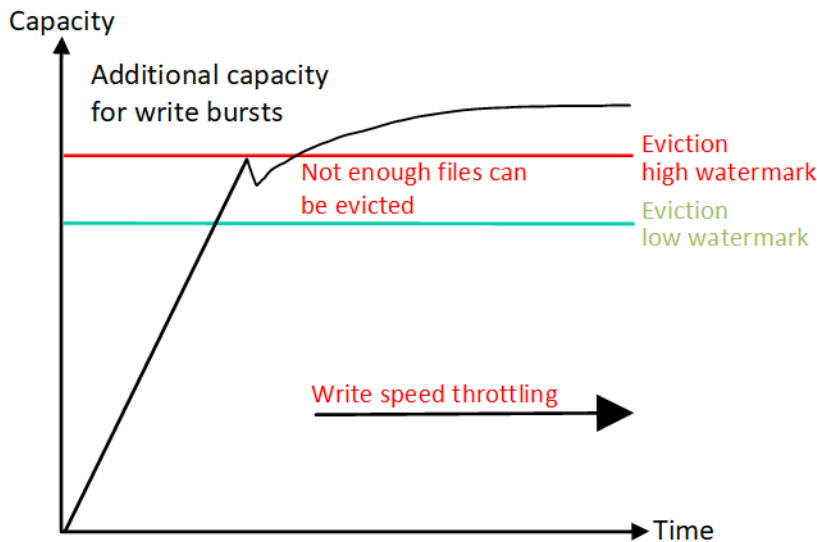
**Note:** Eviction is based on days and not file size. Also, there is no differentiation within a group of the length of time since a file was accessed.

For details on how to manage eviction, see [Manage File Eviction From the Cache](#).

The following graph shows expected disk space usage in a normal scenario.



If the available free space does become too small, throttling is implemented so that users can continue to write to their files, but the client's write speed is reduced to WAN speed so that the data being written is not faster than the data that is evicted to the cloud.



This type of scenario is not usual, except during a migration of a large amount of data, or a very heavy write burst, using all the 25% storage space reserved for write bursts.

## What Happens to Simultaneous File Changes?

Different people can work on the same files at the same time, which means that conflicts can occur. HCP Anywhere Enterprise Edge Filer keeps track of who makes updates and detects and resolves file conflicts when updates occur simultaneously. A file with the conflicts is written in the HCP Anywhere Enterprise Portal global file system so that users can verify that the conflicts were resolved correctly.

HCP Anywhere Enterprise Edge Filer records the history of file events. The changes made in the most recent update are always saved to the original file. Changes that are lost due to conflict are retained in a renamed version of the file.

**Note:** In order for conflict resolution to be performed correctly, the HCP Anywhere Enterprise Edge Filer clock must be synchronized with the HCP Anywhere Enterprise Portal clock. If there is more than one hour difference between the two clocks (after taking into account time zone differences), the HCP Anywhere Enterprise Edge Filer will not synchronize the cloud drive folder.

## What Files are Not Synced From the HCP Anywhere Enterprise Portal?

Temporary files on the HCP Anywhere Enterprise Portal are not synced to the HCP Anywhere Enterprise Edge Filer. The following are not synced:

- Files that begin with \$, .HCP Anywhere Enterprise.tmp or .\_  
\_
- Files of type tmp, temp, swp, dwl, or dwl2

- Files named `desktop.ini`, `Thumbs.db`, `.DS_Store`, `._.DS_Store`, `CredDB.cef`, `.AppleDouble`, `.AppleSingle` or `.Parent`
- Files that end with `Zone.Identifier`

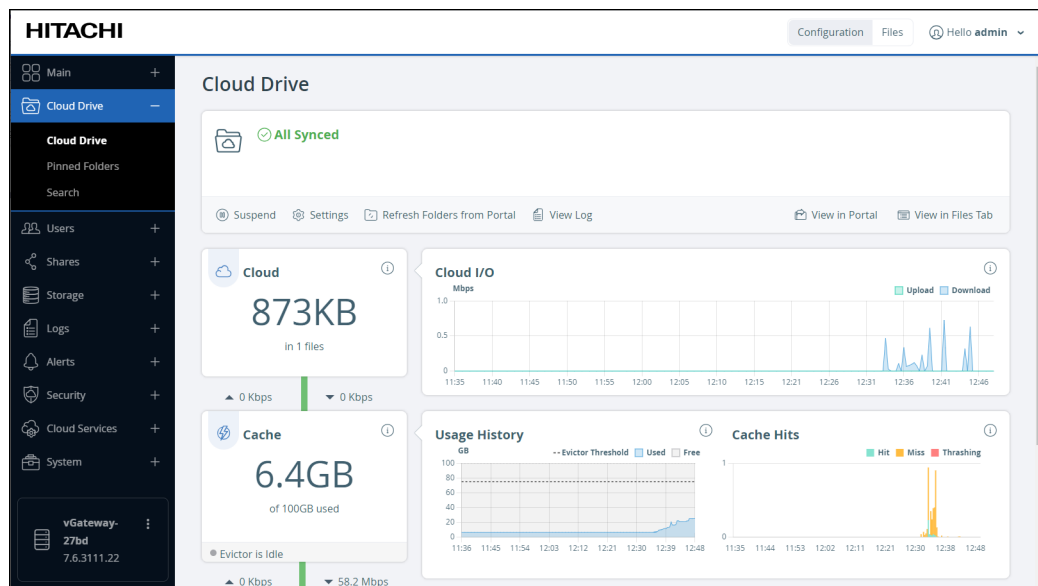
## Caching Operations

When the HCP Anywhere Enterprise Edge Filer is connected to a HCP Anywhere Enterprise Portal, you can:

- [Pinning Folders so that Files are Always Available Locally](#)
- [Suspend and Unsuspend Cloud Sync](#)
- [Refresh the Folder List From the HCP Anywhere Enterprise Portal](#)
- [Control Cloud Sync Upload and Download Speeds](#)
- [Manage File Eviction From the Cache](#)
- [Monitor HCP Anywhere Enterprise Edge Filer Caching](#)
- [Enable Fast Disaster Recovery](#)
- [View the Cloud Sync Log](#)

These operations, except for [Pinning Folders so that Files are Always Available Locally](#) are performed from the **Cloud Drive** page in the user interface.

- In the **Configuration** view, select **Cloud Drive > Cloud Drive** in the navigation pane. The **Cloud Drive** page is displayed.



**Note:** [Pinning Folders so that Files are Always Available Locally](#) is performed in the **Configuration** view, by selecting **Cloud Drive > Pinned Folders** in the navigation pane.

## Pinning Folders so that Files are Always Available Locally

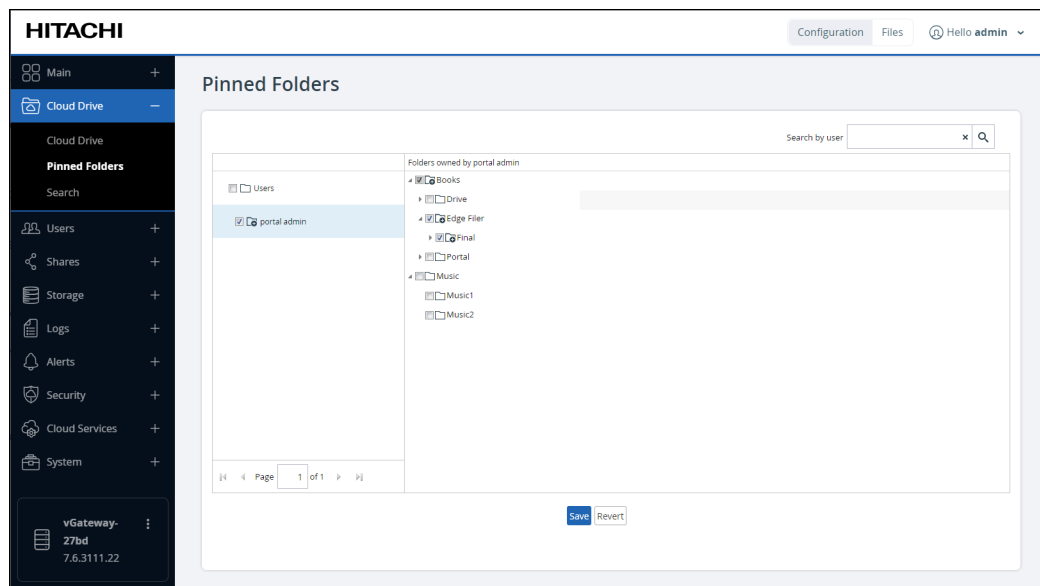
Files in pinned folders stay on the HCP Anywhere Enterprise Edge Filer and are never evicted. This is useful for files that you always want to be available, with immediate access, avoiding downloading these files over the Internet. This ensures that the folder is always accessible even when the HCP Anywhere Enterprise Edge Filer is offline or if there is downtime of the cloud provider or HCP Anywhere Enterprise Portal.

The HCP Anywhere Enterprise Edge Filer supports many thousands of pinned folders.

**Note:** If the amount of data that you need to access locally can easily fit in a local appliance, it is recommended to pin all the data to provide the same levels of predictable performance and accessibility as a regular file server.

### To pin files to be available locally in CACHING mode:

1. 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.

2. Select a user to display the folders owned by the user and then select the folders that you want pinned for this user. In addition, you can use the search field to jump to a specific user.

**Note:** You can select 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.

3. Click **Save**.

The checked folders are pinned to the cloud share. The files in the pinned folders are downloaded from the HCP Anywhere Enterprise Portal. For example, after pinning a folder called **Photos**, the files in **Photos** are downloaded from the HCP Anywhere Enterprise Portal but the files in unpinned folders **My Files** and **Music** remain as stubs.

**Note:** When accessing the HCP Anywhere Enterprise Edge Filer from a Mac machine, you need to follow the procedure in [macOS: Accessing a HCP Anywhere Enterprise Edge Filer](#).

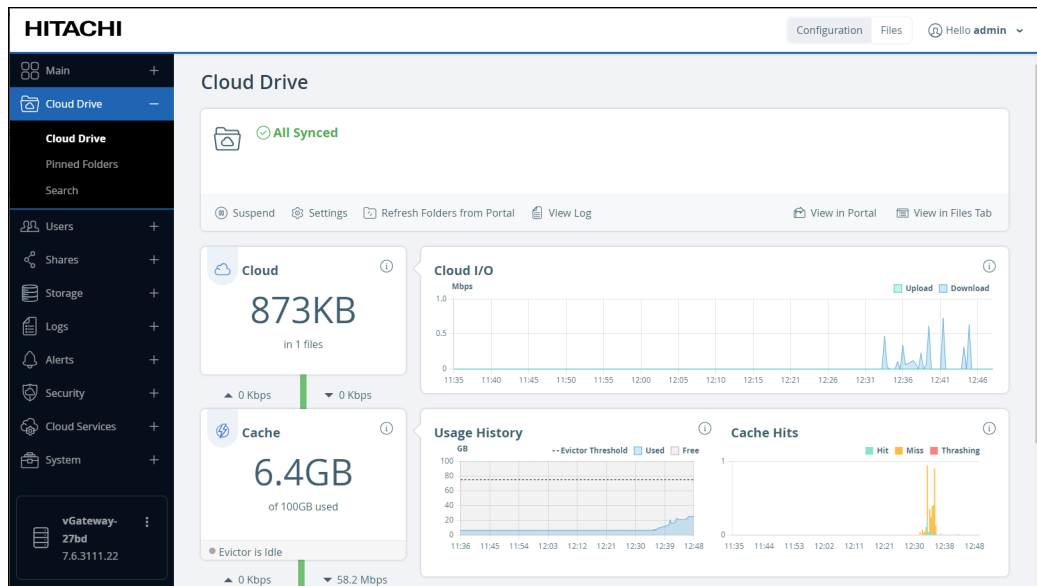
### What Happens to Files that are Not Pinned?

Files that are not pinned, are displayed in the HCP Anywhere Enterprise Edge Filer as stubs. When a user accesses a file stub, a small file is downloaded and opened without delay. When a user accesses a large file, the file is opened by streaming from the cloud and in parallel, the file is added to a background download queue. As the HCP Anywhere Enterprise Edge Filer storage space gets used up, the HCP Anywhere Enterprise Edge Filer starts to remove, evict, files leaving only a stub on the HCP Anywhere Enterprise Edge Filer.

### Suspend and Unsuspend Cloud Sync

You can suspend or unsuspend cloud syncing at any time.

- To suspend syncing, in the **Configuration** view, select **Cloud Drive > Cloud Drive** in the navigation pane, and then click **Suspend**.

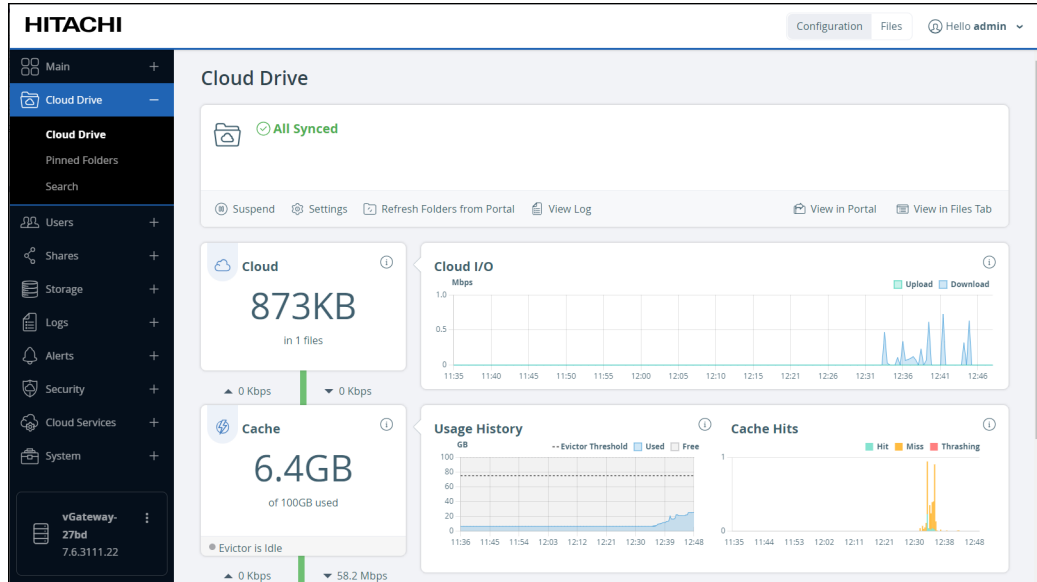


To resume syncing, in the **Cloud Drive** page click **Unsuspend**.

## Refresh the Folder List From the HCP Anywhere Enterprise Portal

You can refresh the folder list from the HCP Anywhere Enterprise Portal.

- To refresh the folder list, in the **Configuration** view, select **Cloud Drive > Cloud Drive** in the navigation pane, and then click **Refresh Folders from Portal**.

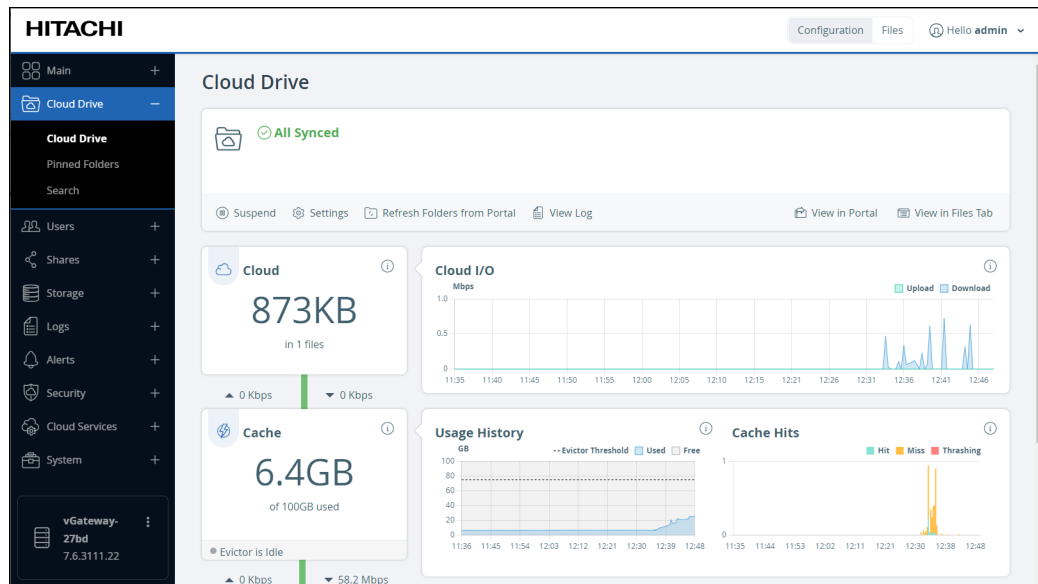


## Control Cloud Sync Upload and Download Speeds

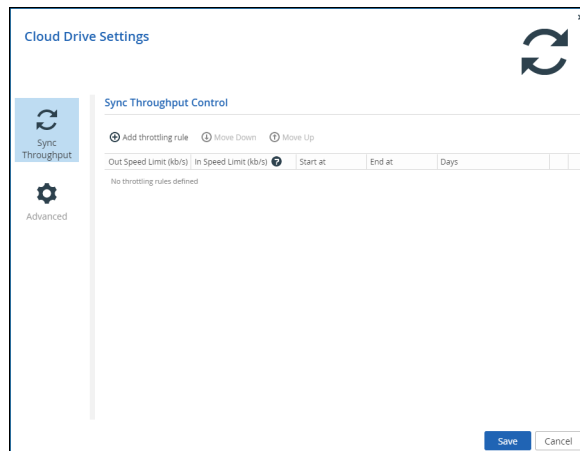
You can limit the cloud sync upload and download speeds using throttling rules to define multiple times and bandwidths for bandwidth throttling.

### To control sync throughput:

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



2. Click **Settings**. The **Cloud Drive Settings** window is displayed.



When no throttling rules are defined, there is no speed restriction for uploading or downloading files to the Cloud Drive.


3. Click **Add throttling rule**.
4. Define the following for the throttling rule:  
**Out Speed Limit (kb/s)** – The maximum speed to use for cloud drive sync upload in Kbits per



second. The minimum value for the speed is 8kb/s. If a value is not set, there is no speed limit.  
**In Speed Limit (kb/s)** – The maximum speed to use for cloud drive sync download in Kbits per second. The minimum value for the speed is 8kb/s. If a value is not set, there is no speed limit.  
**Start at** – Specify the time when the bandwidth limit used for cloud drive sync throttling starts.  
**End at** – Specify the time when the bandwidth limit used for cloud drive sync throttling ends. When the end time is before the start time, the end time is the next day.  
**Days** – Specify that the bandwidth used for cloud drive sync throttling should be restricted every day (the default) or only on specified days.

**Note:** A maximum of 50 rules can be defined.

When the start and end times for more than one rule overlap, the order of the rules in the list determines how they are implemented with the rule at the top of the list implemented first. Use **Move Down** and **Move Up** to change the order the rules are listed.

5. To remove a rule, select the rule row and click the  icon.  
The rule is removed.
6. Click **Save**.

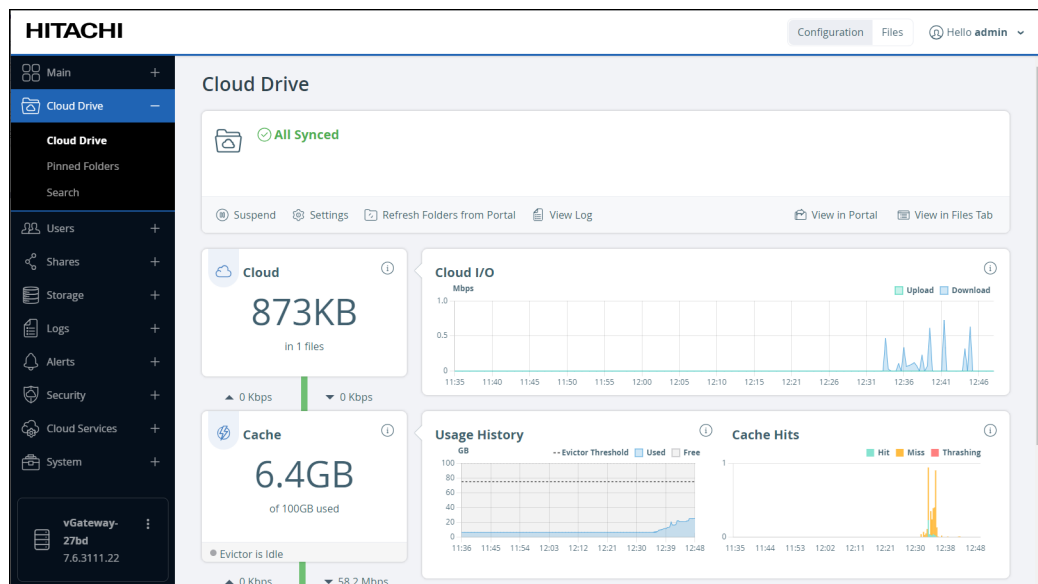
## Manage File Eviction From the Cache

Files that are evicted leave only the stubs in the cache.

When there are many files to be checked for eviction, the whole file system needs scanning. To improve the time required to determine which files need evicting, enable local deduplication on the HCP Anywhere Enterprise Edge Filer and run full reindexing, described in [Applying Local Deduplication to Existing Files](#).

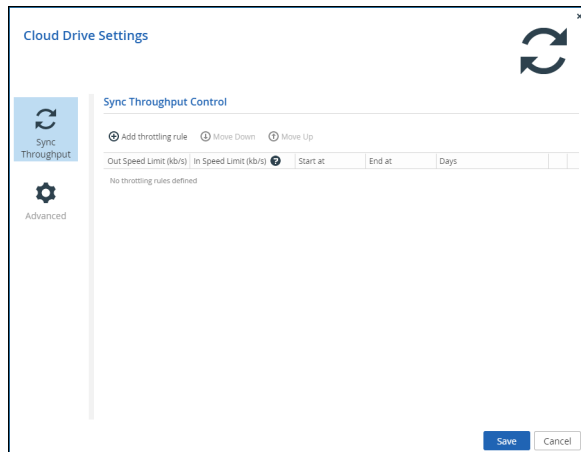
### To manage eviction from the cache:

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

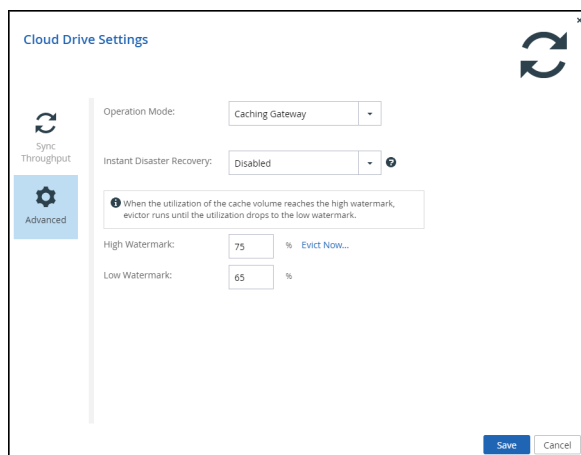


2. Click **Settings**.

The **Cloud Drive Settings** window is displayed.



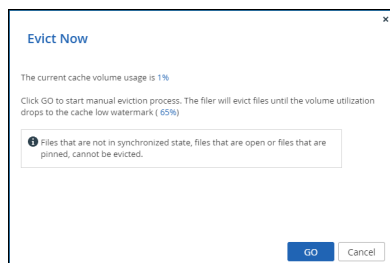
3. Select the **Advanced** option.



4. Change either the **High Watermark** or **Low Watermark** or both as required.

5. Optionally, click **Evict Now** to start evicting files based on the eviction policy.

The **Evict Now** window is displayed.



- Click **GO** to start evicting content from the cache. When **Evict Now** is run by the user, the process is the same as when a scheduled eviction is performed. Eviction will not start if the amount of data in the cache is less than the low watermark. If required, throttling is also implemented.

Additional changes to the eviction policy can be configured. For details, contact Hitachi Vantara support.

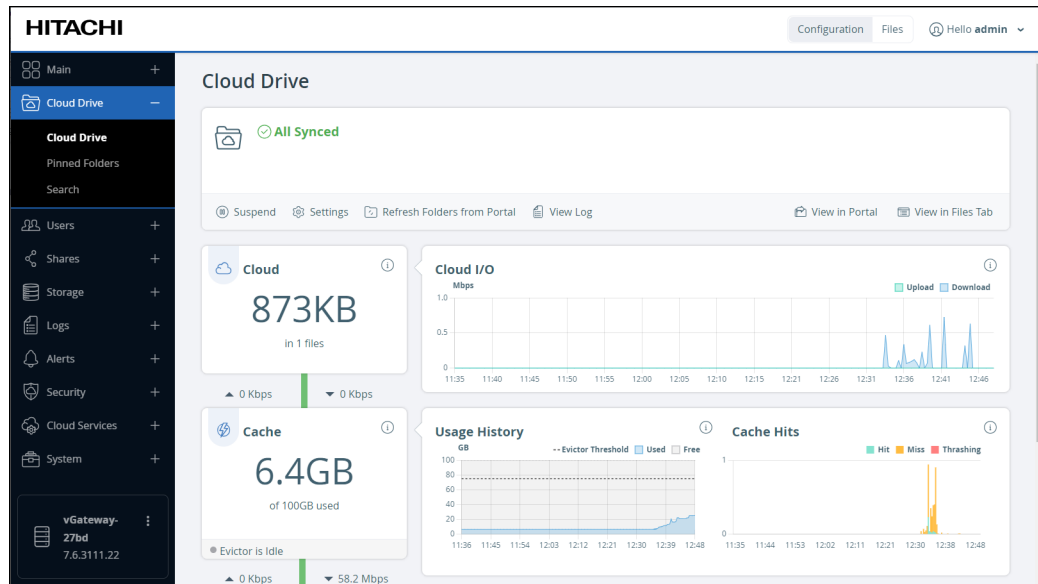
## Evicting Individual Folder Content From the Cache

You can evict individual folder content, including all the subfolder content, from the HCP Anywhere Enterprise Edge Filer cache. See [Evicting Folder Content From the Cache](#).

## Monitor HCP Anywhere Enterprise Edge Filer Caching

### To monitor HCP Anywhere Enterprise Edge Filer caching:

- In the **Configuration** view, select **Cloud Drive > Cloud Drive** in the navigation pane. The **Cloud Drive** page is displayed.



The following information is available on the top and left side of the page:

- The scanning status between the edge filer and the portal, such as **All Synced**, **Scanning**.
- The amount of storage transferred between the HCP Anywhere Enterprise Edge Filer and the HCP Anywhere Enterprise Portal and the number of files involved.
- The rate of transfer of data in both directions between the HCP Anywhere Enterprise Edge Filer and the HCP Anywhere Enterprise Portal.
- The amount of data currently in the cache and the total amount of storage available.
- The status of the evictor, either idle or running.
- The number of currently active local connections to the HCP Anywhere Enterprise Edge Filer and the rate of transfer of data in both directions between the HCP Anywhere Enterprise Edge Filer and the local connection.
- The throttling status for the connection, either idle or running.

**Note:** The current throttling is displayed and not the aggregated value of all the connections.

The graphs show the following:

**Cloud I/O** – The rate of transfer of data over time from the HCP Anywhere Enterprise Edge Filer to the HCP Anywhere Enterprise Portal (**Upload**) and from the HCP Anywhere Enterprise Portal to the HCP Anywhere Enterprise Edge Filer over time (**Download**).

**Usage History** – The evictor threshold, the amount of data in the cache, and the amount of free space in the cache over time.

**Cache Hits** – The hits, misses and thrashing when accessing files and performing operations, such as write, on the files.

- **Hit** – The file was accessed from the cache: it was not a stub file.
- **Miss** – The file was a stub file that was downloaded from the HCP Anywhere Enterprise Portal. However, the file had not been accessed within the last 24 hours.
- **Thrashing** – The file was a stub file that was downloaded from the HCP Anywhere Enterprise Portal. The file was not in the cache for less than 24 hours. Thrashing means that files that were recently evicted are needed.

**Local Activity** – The write throttling, the write rate from the local connections to the HCP Anywhere Enterprise Edge Filer, and the read rate from the HCP Anywhere Enterprise Edge Filer to the local connections over time.

## Enable Fast Disaster Recovery

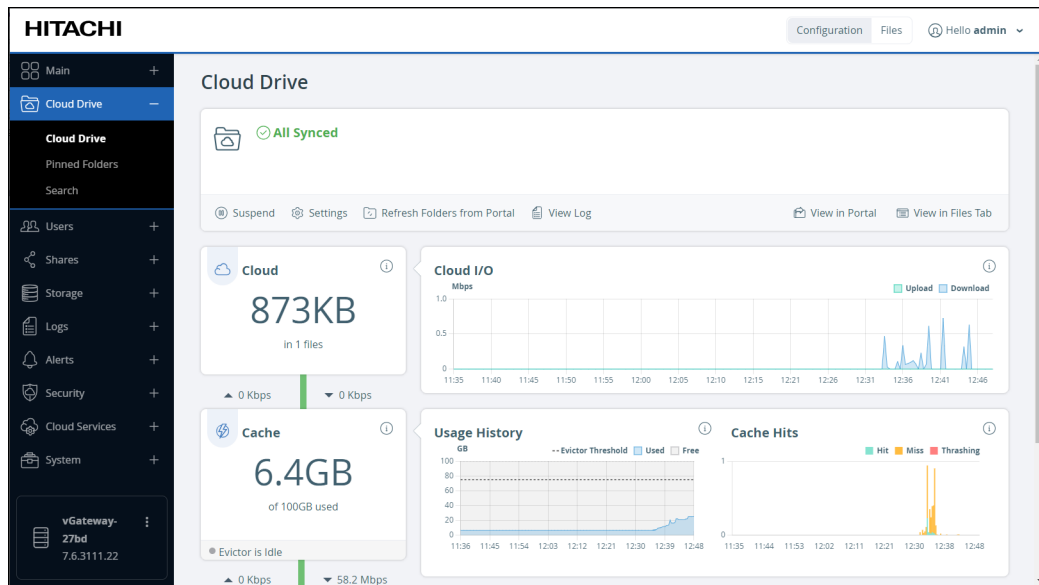
Business continuity is an organization's ability to ensure operations, and core business functions are not severely impacted by a disaster or unplanned incident that take critical systems offline. Being able to recover from a disaster is categorized by two factors: Recovery Time Objective (RTO) and Recovery Point Objective (RPO). RTO is the maximum time allowed to get the systems back online, and RPO is the maximum amount of data loss that can be suffered.

If an HCP Anywhere Enterprise Edge Filer fails, after setting up a replacement, the metadata from the HCP Anywhere Enterprise Portal can be downloaded quickly so that the stub files are almost immediately available on the replacement HCP Anywhere Enterprise Edge Filer.

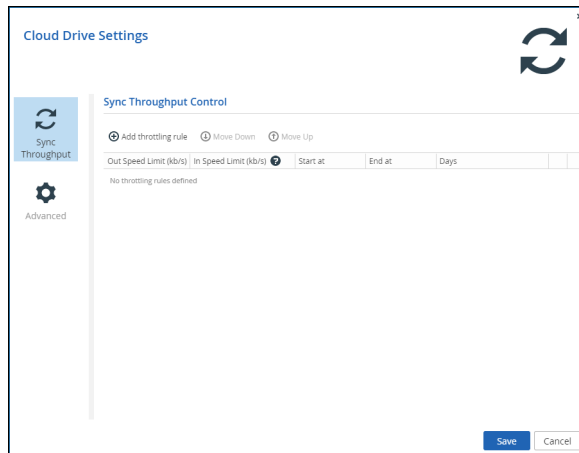
Both metadata and data are populated to the replacement HCP Anywhere Enterprise Edge Filer based on priority: When a path is entered to access content, that content receives download priority, so it becomes available even when all the metadata has not been downloaded.

**To initiate disaster recovery:**

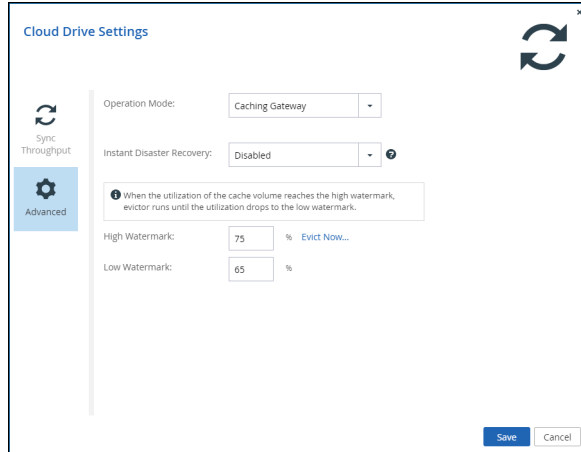
1. In the **Configuration** view, select **Cloud Drive > Cloud Drive** in the navigation pane. The **Cloud Drive** page is displayed.



2. Click **Settings**. The **Cloud Drive Settings** window is displayed.



3. Select the **Advanced** option.



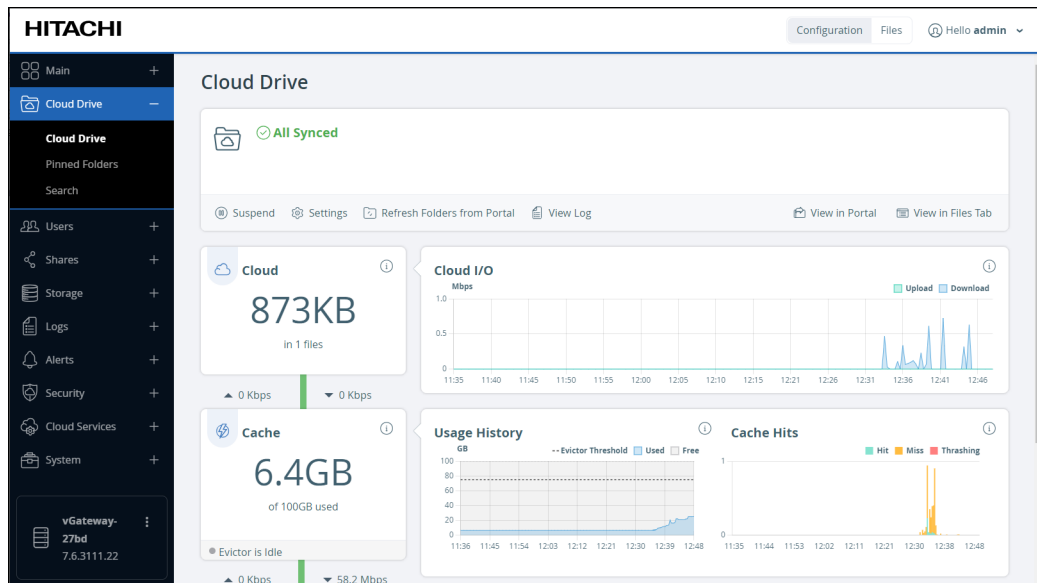
**4. Change the Instant Disaster Recovery to Enabled.**

**Note:** Since enabling **Instant Disaster Recovery** can have a negative impact on ongoing use of the HCP Anywhere Enterprise Edge Filer, Hitachi Vantara recommends only enabling it when populating an HCP Anywhere Enterprise Edge Filer from the HCP Anywhere Enterprise Portal for the first time, after a disaster, and disabling it once the HCP Anywhere Enterprise Edge Filer is populated.

## View the Cloud Sync Log

You can access the cloud sync log directly from the **Cloud Drive** page.

1. To access the cloud sync log, in the **Configuration** view, select **Cloud Drive > Cloud Drive** in the navigation pane.



2. Click **View Log**.

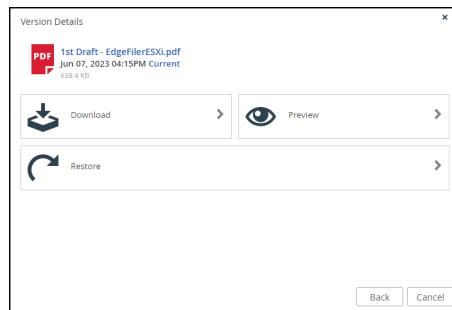
The **Log Viewer** page is displayed showing the Cloud Sync Log.

## Accessing Previous File Versions

You can view and restore previous versions of the end-user files and folders residing in the cloud on the HCP Anywhere Enterprise Portal, or locally on the HCP Anywhere Enterprise Edge Filer.

### To view and restore previous versions:

1. In the **Files** view, navigate to the file.
2. Right-click the file and select **Versions**.
3. Click the desired version of the file.



4. Select the action for the file version. The options include:
  - Download** – Download the file to your local machine.
  - Preview** – If a preview of the file is possible, this option is displayed.
  - Restore** – Restore the version. If a version of the file exists, a window is displayed where you can either replace the existing file with the version or rename it.
    - a) Select the option you want.  
A window is displayed when the restore has completed.
    - b) Click **OK**.

## macOS: Enabling Using Finder to Search in the HCP Anywhere Enterprise Edge Filer

When using a Mac computer to search for files in a share on the HCP Anywhere Enterprise Edge Filer, you can search for these files using Mac Finder. Enabling file searches requires a file index. After indexing completes, you can search for files even when the HCP Anywhere Enterprise Edge Filer syncing is suspended.

**Note:** Building and maintaining this index can impact performance and the search mechanism is disabled by default. Searching in Finder will only return the list of files for which the user has permission to see.

### To enable searching for files in HCP Anywhere Enterprise Edge Filer shares using Mac Finder:

**Note:** Do not enable file searching on a Mac if you also configure NFS access, described in [Configuring FTP Access](#).

1. In the **Configuration** view, select **Cloud Drive > Search** in the navigation pane. The **File Indexing** page is displayed.
2. Click **Enable file indexing**.

3. Restart the HCP Anywhere Enterprise Edge Filer. For details, see [Resetting a HCP Anywhere Enterprise Edge Filer to its Default Settings](#).

**To disable file search:**

1. In the **Configuration** view, select **Cloud Drive > Search** in the navigation pane. The **File Indexing** page is displayed.
2. Click **Disable file indexing**.
3. Restart the HCP Anywhere Enterprise Edge Filer. For details, see [Resetting a HCP Anywhere Enterprise Edge Filer to its Default Settings](#).

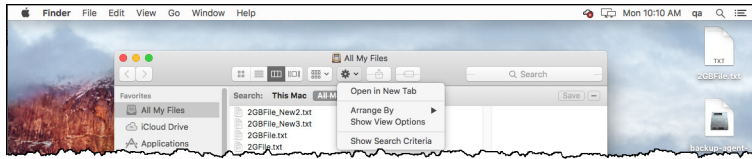
## Searching Using Mac Finder

You must have at least three characters in the search string. When searching for strings with spaces, use double quotes around the search string.

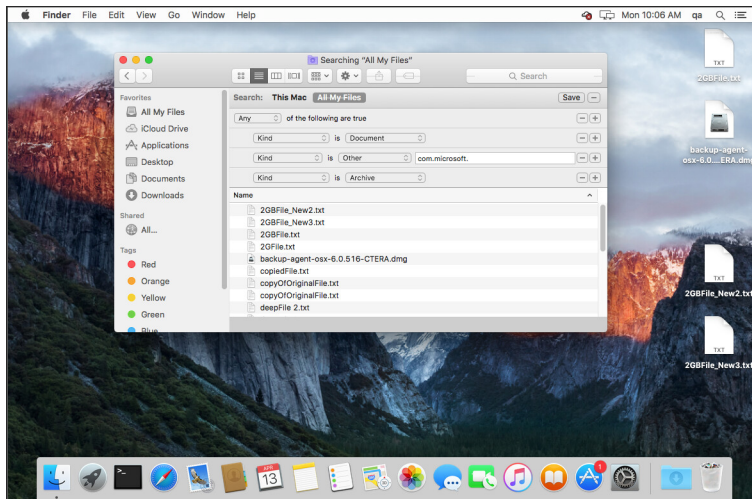
You can search for file names but not for file types, such as .doc or .pdf files. However, you can search for a file type that is part of the file name, for example, *mypdffile.pdf*.

**To search for a file type that is part of the file name:**

1. In Finder, open the drop-down search criteria menu. The advanced search settings are displayed.



2. Enter the search term in the name field rather than in the main search bar.





---

## Chapter 6. Managing Local Shares

Folders and files that are required locally, but not required to be part of the global namespace, can be stored on the HCP Anywhere Enterprise Edge Filer and not synced with the HCP Anywhere Enterprise Portal. This content can be shared locally over the network and backed up to the cloud. Files can be shared in any of the following ways:

- Using **Windows File sharing**. Every share is exposed through Windows File Sharing so that Windows clients on the network can access the shares through Windows.
- Using **FTP**. You can use the HCP Anywhere Enterprise Edge Filer as an FTP server to transfer files or folders over the local network. The FTP protocol is disabled by default.
- Using **NFS**. You can use the HCP Anywhere Enterprise Edge Filer as an NFS server, enabling clients with specified IP addresses to access network shares on the HCP Anywhere Enterprise Edge Filer, as if the shares were located on the client's hard drive. Both NFS versions 3 and 4 protocols are supported, depending on the protocol used by the client.

To make any local folder accessible to other HCP Anywhere Enterprise Edge Filer requires the following basic steps:

1. Assign the user a HCP Anywhere Enterprise Edge Filer user account. See [Managing the HCP Anywhere Enterprise Edge Filer Users](#).
2. Configure the relevant protocol (Windows File Sharing, FTP, NFS) that you want the users to use to access the files. See [Network Sharing Protocols](#).
3. Make a network share on the folder you want to share. See [Managing Network Shares](#).
4. Provide access to the share. See [Accessing Network Shares](#).

### Configuring HCP Anywhere Enterprise Edge Filer Shares

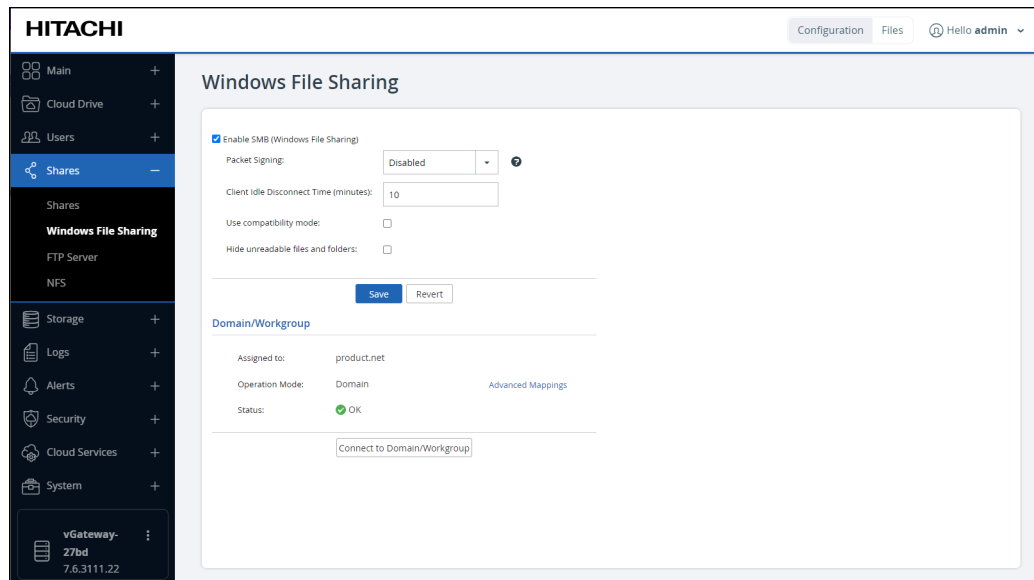
Files on a HCP Anywhere Enterprise Edge Filer can be shared by users both over a LAN and WAN and are synced to each HCP Anywhere Enterprise Edge Filer using a HCP Anywhere Enterprise Portal.

Configuring file sync and share requires that the HCP Anywhere Enterprise Portal is configured before the HCP Anywhere Enterprise Edge Filer. For details, see *Configuring the HCP Anywhere Enterprise Portal as a Precondition to Setting Up the HCP Anywhere Enterprise Edge Filer* in the installation guide.

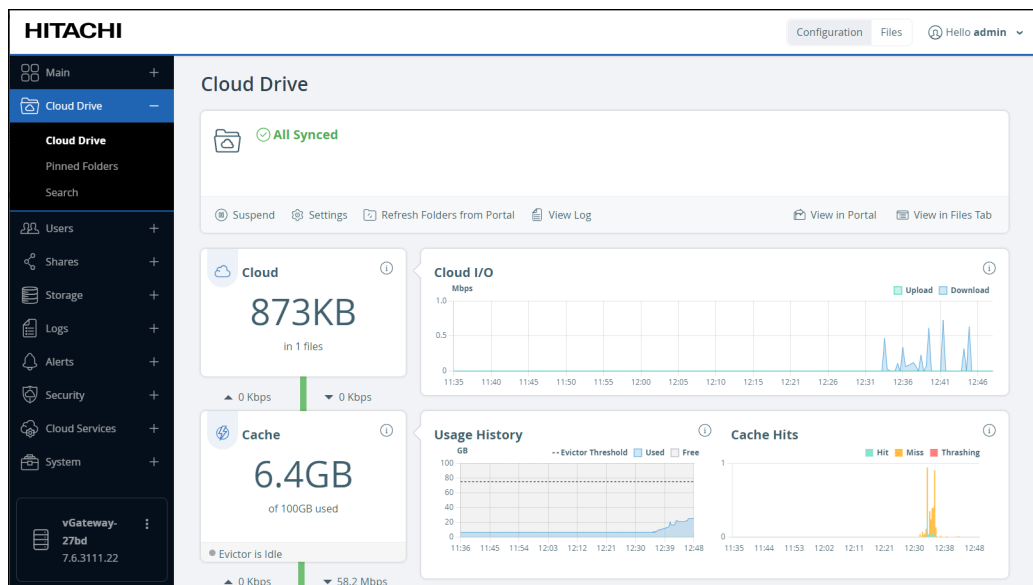
**Note:** When using HCP Anywhere Enterprise Migrate to migrate shares from a file system to a HCP Anywhere Enterprise Edge Filer, the shares are setup in the HCP Anywhere Enterprise Portal as part of the migration process.

#### To configure HCP Anywhere Enterprise Edge Filer shares:

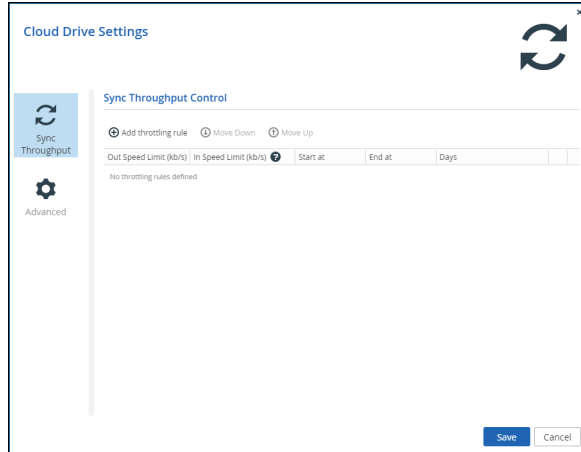
1. Verify that the HCP Anywhere Enterprise Edge Filer is connected to Active Directory.
  - a) Log in to the HCP Anywhere Enterprise Edge Filer as an administrator.
  - b) In the **Configuration** view, select **Shares > Windows File Sharing** in the navigation pane. The **Windows File Sharing** page is displayed.



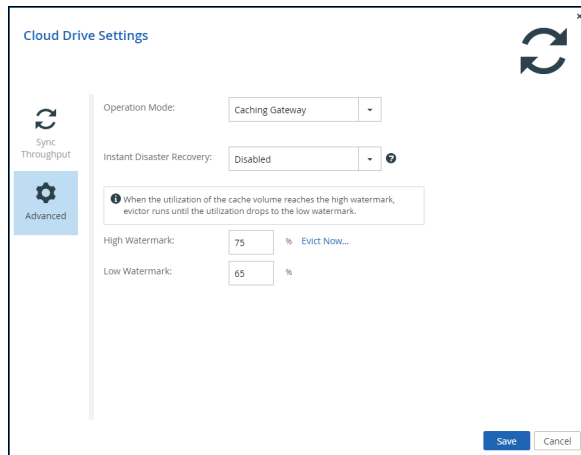
- c) In the **Domain/Group** section, verify that the **Operation Mode** is **Domain** and that the **Status** is **OK**. Otherwise, click **Connect to Domain/Workgroup** to connect to an Active Directory domain.
2. In the **Configuration** view, select **Cloud Drive > Cloud Drive** in the navigation pane. The **Cloud Drive** page is displayed.



3. Click **Settings**. The **Cloud Drive Settings** window is displayed.



4. Select the **Advanced** option and make sure the **Operation Mode** is **Caching Gateway**.



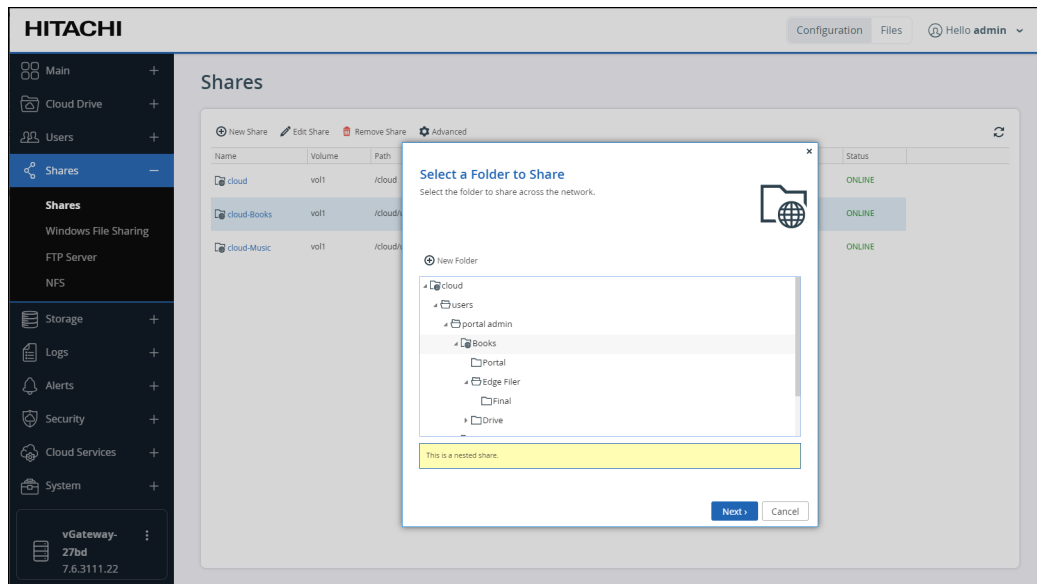
5. Click **Save**.

To work with Windows ACL, the sharing protocol must be **Windows ACL Emulation Mode**. Windows ACL enabled folders on the HCP Anywhere Enterprise Portal cannot be synced unless the cloud share is defined as **Windows ACL Emulation Mode**.

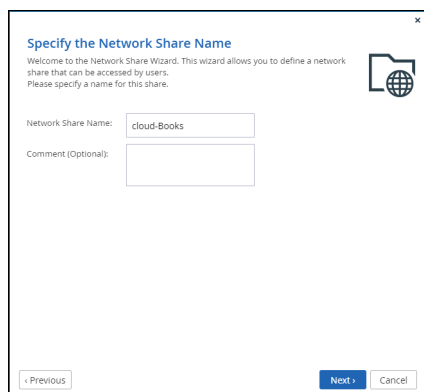
**To configure HCP Anywhere Enterprise Edge Filer shares with ACL support:**

1. In the **Configuration** view, select **Shares > Shares** in the navigation pane.
2. Click the cloud share that was automatically created when it synced to the HCP Anywhere Enterprise Portal.

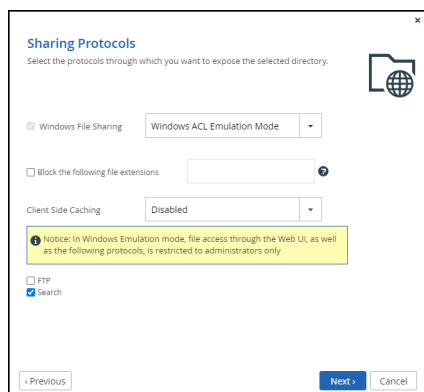
The **Select a Folder to Share** wizard opens, displaying the volumes and folders on the HCP Anywhere Enterprise Edge Filer.



3. Select the cloud folder to share and click **Next**.  
The **Specify the Network Share Name** window is displayed.



4. Optionally, change the **Network Share Name** and click **Next**.  
The **Sharing Protocols** window is displayed.



Users access the shared files and folders through standard Windows client computers; for

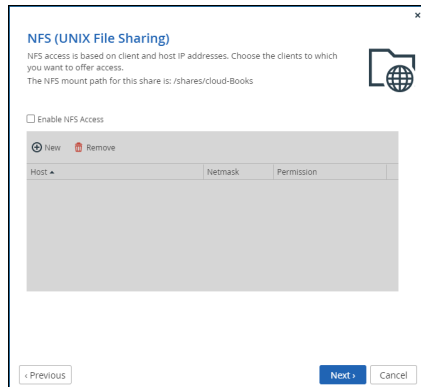
example, using Windows File Explorer through the SMB access provided by the HCP Anywhere Enterprise Edge Filer.

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.

**Note:** **Windows File Sharing** is checked by default and cannot be deselected.

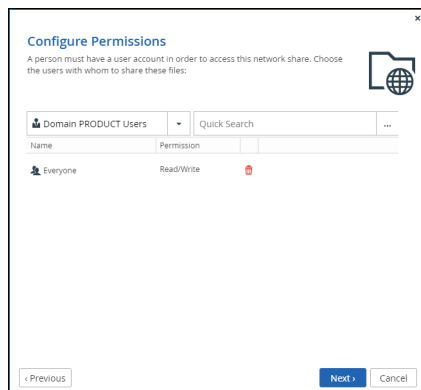
5. Click **Next**.

The **NFS (UNIX File Sharing)** window is displayed.



6. Click **Next**.

The **Configure Permissions** window is displayed.



7. Specify the share permissions.

**Note:** These permissions are not inherited from the HCP Anywhere Enterprise Portal.

8. Click **Next** and then click **Finish**.

9. Repeat for all the shares you want to work with Windows ACLs.

The shares are displayed in the **Shares** page.

Users can access their files directly with SMB by mapping the share name in the file manager. Both Windows File Explorer and macOS Finder report that the total space and available free space for the mapped drive is a very high number to simulate the caching ability of infinite storage.

**Note:** Share names cannot include 2 spaces together in the name.

You can achieve the nested sharing without imposing Windows ACLs.

### **To configuring HCP Anywhere Enterprise Edge Filer shares without ACL support:**

- When configuring the HCP Anywhere Enterprise Portal, on each cloud drive folder group that you do not want ACL support, uncheck Enable Windows ACLs.
- When configuring the HCP Anywhere Enterprise Edge Filer, set Only Authenticated Users and not Windows ACL Emulation Mode, which is set by default.

## **Network Sharing Protocols**

HCP Anywhere Enterprise Edge Filers support the following protocols for sharing files and folders over the network:

**Windows File Sharing** – Enabled on all network shares and enables Windows clients on the network to access the shares through Windows. For more details, see [Configuring Windows File Sharing](#).

**FTP** – A protocol used to transfer files from one device to another over a network. You can set up an FTP server on the HCP Anywhere Enterprise Edge Filer and share files by FTP. Users can access and download the files you share using a web browser. You can set up the FTP server to require username-password authentication or to allow anonymous connections. See [Configuring FTP Access](#). The FTP protocol is disabled by default.

**NFS (Network File System)** – Clients with certain IP addresses can access network shares on the HCP Anywhere Enterprise Edge Filer, as if the shares were located on the client's hard drive. See [Configuring NFS Access](#).

## **Configuring Windows File Sharing**

Windows files that you want to share via the HCP Anywhere Enterprise Edge Filer can be protected using one of the following access levels:

- Only Authenticated Users
- Windows ACL Emulation Mode

### **Only Authenticated Users**

Users are 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 is a Windows ACL emulation mode share supporting a full Windows file system folder structure and permissions, including enforcement and settings, known as NT ACLs, and extended attributes such as read-only and hidden.

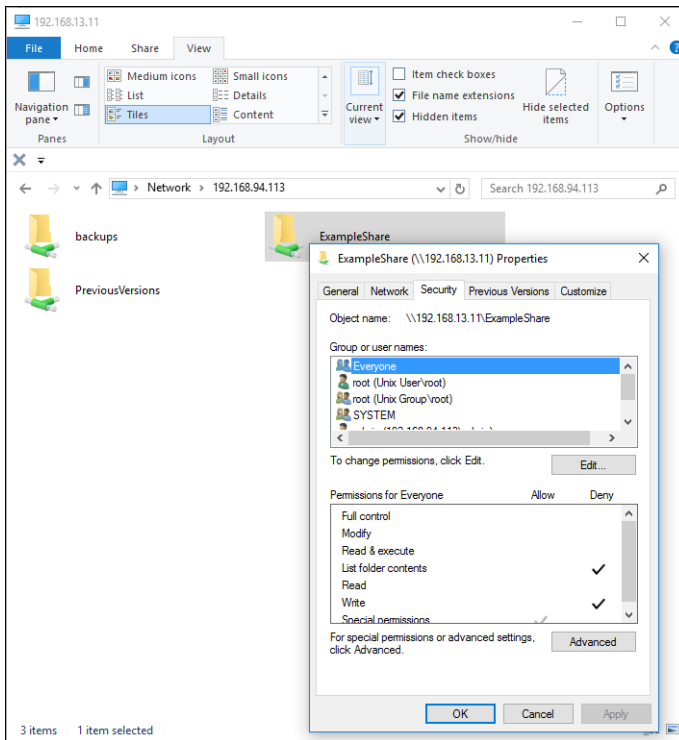
End users who are familiar with a given folder structure and shares, as well as a given permission scheme, while using the Windows file server, continue to see the same folder structure, shares, and permission scheme after migration to the HCP Anywhere Enterprise Edge Filer. This enables the migration from a current Windows Server-based 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. The migration is entirely transparent to the end user.

Transition of the mapped network drives and share names available on the Windows client from the Windows file server location to the HCP Anywhere Enterprise Edge Filer location is performed seamlessly using AD GPO capabilities.

File and folder access continue to be available following the migration in the same way they were in the Windows Server-based file system. Access after the migration is through the SMB protocol provided by the HCP Anywhere Enterprise Edge Filer.

Users continue to access the files and folders through standard Windows client computers; for example, using Windows File Explorer.

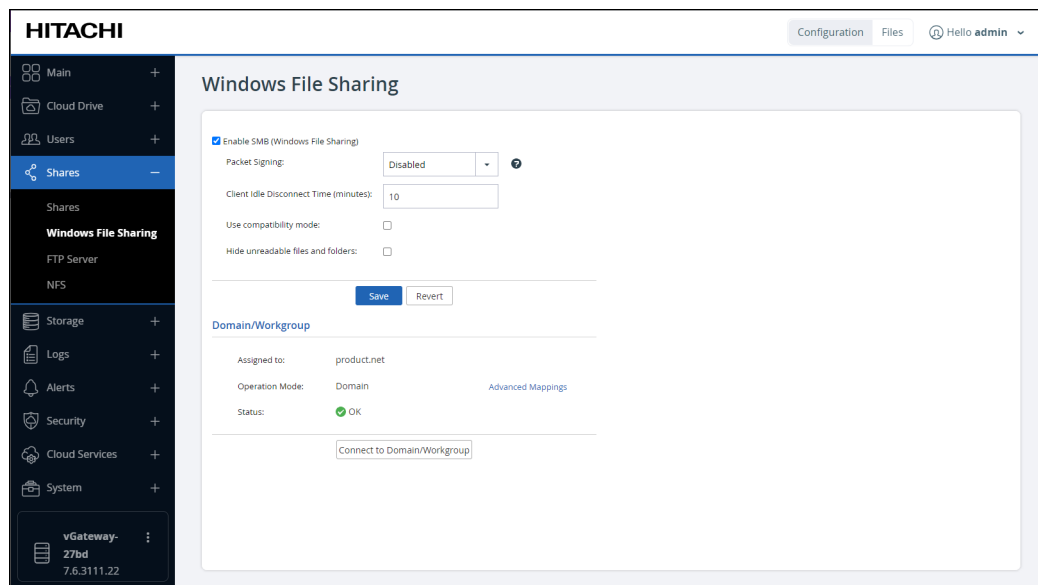


To set up shares in the HCP Anywhere Enterprise Edge Filer with NT ACL permissions, you need to do the following:

- Set up the users that will access the file system. HCP Anywhere Enterprise recommends taking the users from Active Directory. For more details, see [Configuring Windows File Sharing for Active Directory](#).
- Set up the share with ACL emulation in the HCP Anywhere Enterprise Edge Filer. For more details, see [Managing Network Shares](#).
- Copy the files from the Windows File Server. For more details, see [Copying Files From an External File Server to the HCP Anywhere Enterprise Edge Filer](#).

## To configure Windows File Sharing:

1. In the **Configuration** view, select **Shares > Windows File Sharing** in the navigation pane. The **Windows File Sharing** page is displayed.



Where:

**Enable SMB (Windows File Sharing)** – Enable or disable Windows file sharing. If Windows file sharing is disabled, Windows shared folders, defined via Shares > Shares, as described in [Managing Network Settings](#), are no longer accessible.

**Packet Signing** – Whether SMB packet signing is required or not, or whether it is dependent on the agreement of the client.

**Client Idle Disconnect Time (minutes)** – The amount of time in minutes after which a client should be disconnected, if the connection is idle. There is usually no need to change this setting. The default is 10 minutes.

**Use compatibility mode** – Enable access by Windows versions 2000 or earlier. Enabling this option reduces security.

**Hide unreadable files and folders** – Hide unreadable files or folders, or shares to which users do not have access, when users access shares via Windows File Sharing.

2. Click **Save** to save the Windows File Sharing settings.
3. Specify the **Domain/Workgroup** information:

**Assigned to** – The name of an Active Directory domain or Windows workgroup to which the HCP Anywhere Enterprise Edge Filer's Windows File Sharing service is connected.

**Operation Mode** – Whether the HCP Anywhere Enterprise Edge Filer's Windows File Sharing service is connected to an Active Directory domain or to a **Windows workgroup**.

**Status** – The status of the connection to an Active Directory domain or Windows workgroup.

**Advanced Mappings** – When connected to an Active Directory domain. See [Defining Users From an Active Directory Domain, Tree or Forest](#).

4. Click **Connect to Domain/Workgroup** to join an Active Directory domain or Windows workgroup:
  - For a network with a Active Directory with either a single domain or multi-domain environment: a tree or forest, see [Configuring Windows File Sharing for Active Directory](#).
  - For a network with no domain controller, see [Configuring Windows File Sharing for a](#)



Workgroup.

## Configuring Windows File Sharing for Active Directory

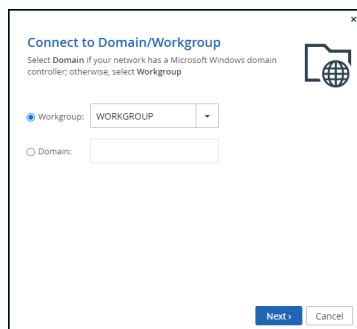
To configure Windows file sharing for an individual Active Directory domain and for an Active Directory tree or forest, see [Defining Users From an Active Directory Domain, Tree or Forest](#).

## Configuring Windows File Sharing for a Workgroup

### To configure Windows file sharing for a workgroup:

1. In the **Configuration** view, select **Shares > Windows File Sharing** in the navigation pane. The **Windows File Sharing** page is displayed.
2. Click **Connect to Domain/Workgroup**.

The **Windows File Sharing** wizard opens, displaying the **Connect to Domain/Workgroup** window.



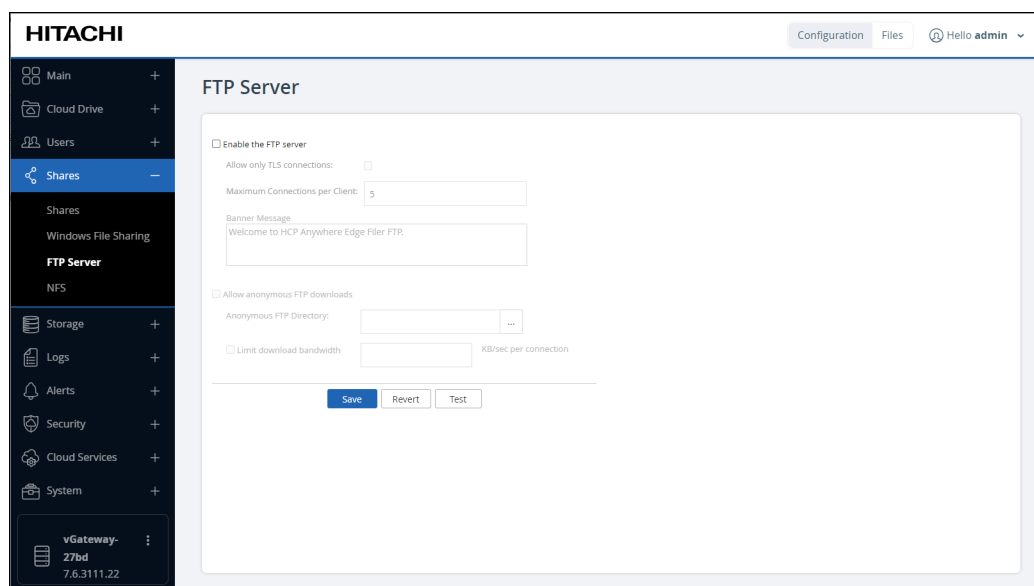
3. Choose **Workgroup**, and then select the workgroup you want or else type the name of the workgroup in the empty field.  
**Note:** You must assign this same workgroup name to all of the computers in the network. In most Windows versions, the default workgroup name is WORKGROUP. The HCP Anywhere Enterprise Edge Filer automatically scans for available workgroups in the LAN. The results of these scans can be selected from the **Workgroup** list.
4. Click **Next** and then click **Finish**.

# Configuring FTP Access

**Note:** By default, the FTP sharing protocol is disabled.

## To configure FTP access:

1. In the **Configuration** view, select **Shares > FTP Server** in the navigation pane. The **FTP Server** page is displayed.



2. Check **Enable the FTP server** and specify the FTP details.
  - Allow only TLS connections** – Allow only Transport Layer Security (TLS) connections to the network shares on the FTP Server.
  - Maximum Connections per Client** – Type the maximum number of concurrent FTP connections allowed per client. The default value is 5.
  - Banner Message** – The message to display at the top of the page when accessing the network shares via FTP.
  - Allow anonymous FTP downloads** – Allow users to access and download files from a specific directory on the FTP server, without authenticating.
    - **Anonymous FTP Directory** – The directory you want to allow users to download by FTP without authenticating.
    - **Limit download bandwidth** – Restrict the bandwidth used for FTP downloads. Enter the maximum bandwidth to use for FTP downloads in kilobytes per second.
3. Click **Revert**, if you made changes that you did not save, to revert to display the saved values.
4. Click **Save**.
5. Test the settings. FTP testing is not available if you check **Allow only TLS connections**.
  - a) Click **Test** and in the **Authentication Required** window, enter the HCP Anywhere Enterprise Edge Filer user name and password.
  - b) Click **Login**.

The FTP index opens, displaying all the shares you have access to that are FTP enabled.

# Configuring NFS Access

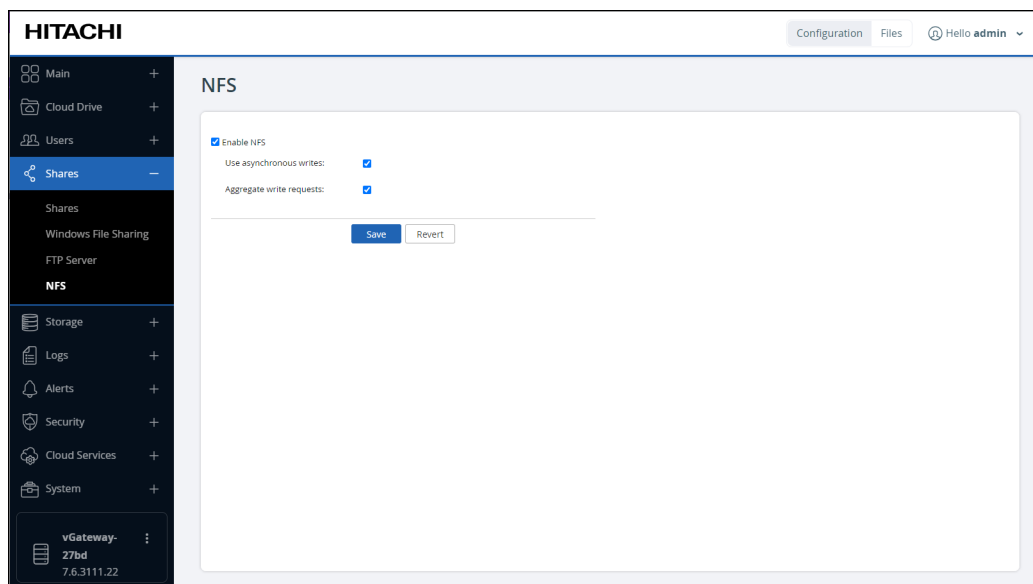
When Network File System (NFS) access is enabled, clients with certain IP addresses can access network shares on the HCP Anywhere Enterprise Edge Filer as if the shares were located on the client's hard drive. For information, see [Mounting Network Shares Using NFS](#).

Both NFS versions 3 and 4 protocols are supported, depending on the protocol used by the client.

**Note:** When enabling NFS on the share, the cloud share, /cloud, is not available. To make the cloud share available, contact Hitachi Vantara Support.

## To configure NFS access:

1. In the **Configuration** view, select **Shares > NFS Settings** in the navigation pane. The **NFS Settings** page is displayed.



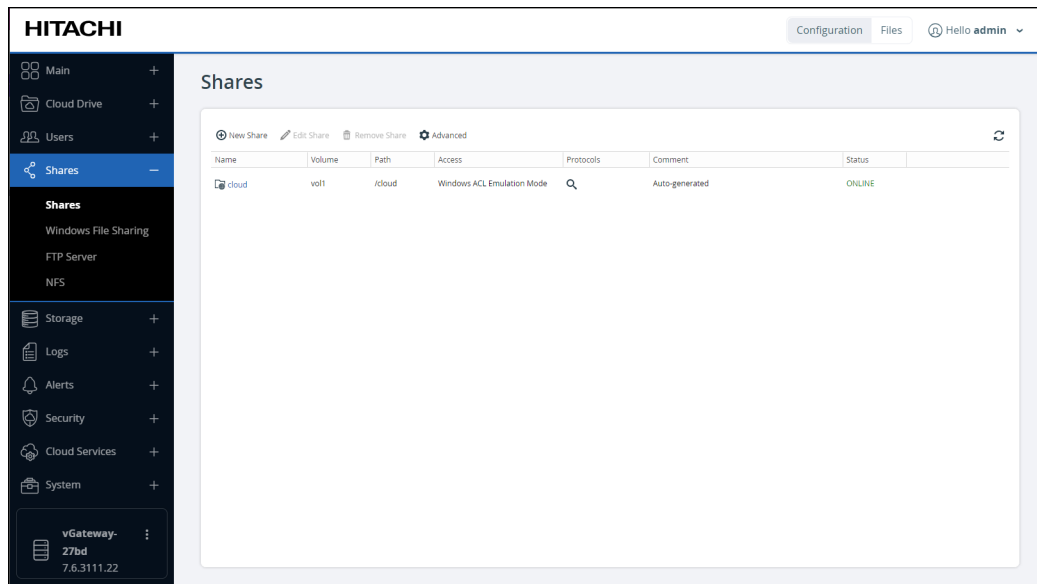
2. Check **Enable NFS** and specify the details.  
**Use asynchronous writes** – Enable asynchronous writes. When a client attempts to write data to the HCP Anywhere Enterprise Edge Filer, the HCP Anywhere Enterprise Edge Filer sends the client an acknowledgment of the write request, before actually writing the data to the disk. This enables the client to post additional write requests to the HCP Anywhere Enterprise Edge Filer, while the HCP Anywhere Enterprise Edge Filer is still writing data from the first request to disk, thereby improving throughput.  
**Aggregate write requests** – Write requests are aggregated and sent in a single batch, instead of one at a time, to improve throughput.
3. Click **Revert**, if you made changes that you did not save, to revert to display the saved values.
4. Click **Save**.

# Managing Network Shares

The **Shares** page allows you to manage all network shares on the HCP Anywhere Enterprise Edge Filer, both for content that is synced with a HCP Anywhere Enterprise Portal and content that is only available locally.

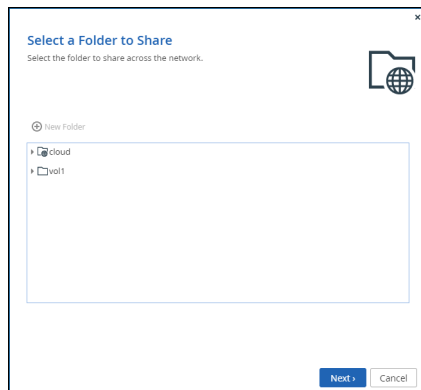
## To define a network share:

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



2. Click **New Share**.

The **Select a Folder to Share** window opens, displaying the volumes and folders on the HCP Anywhere Enterprise Edge Filer.



3. Select the volume, folder, or subfolder on which you want to define the share.
  - To create a new subfolder to select as a nested share, select the parent folder, click **New Folder**, and then assign the subfolder a name.
  - You can define nested shares based on subfolders within the 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:

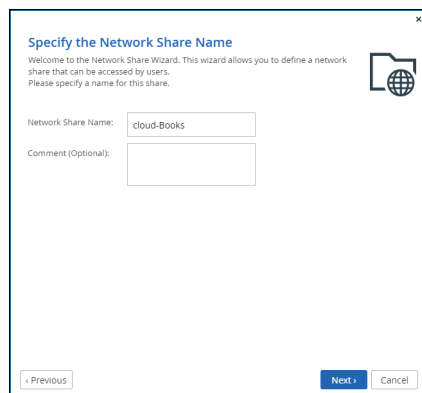
```
/Cloud
/WIN-File-Server
  /Share1
  /Share2
/My Files
/Shared with me
```

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:

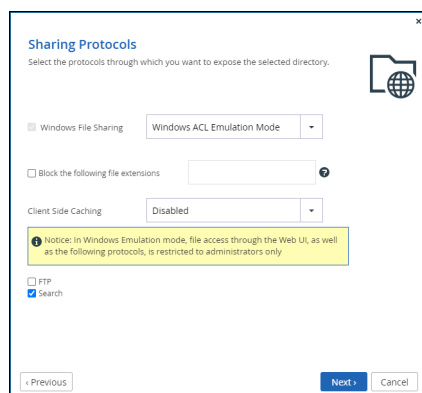
Share1 = \\MyGateway\Cloud\WIN-File-Server\Share1

Share2 = \\MyGateway\Cloud\WIN-File-Server\Share2

4. Click **Next** and then assign the network share a name.



5. Click **Next** and choose through which sharing protocols to expose this share.



**Windows File Sharing** is checked by default and cannot be deselected. From the drop-down, select one of these access levels for the share:

- **Windows ACL Emulation Mode** – The share will be a Windows ACL emulation mode share.

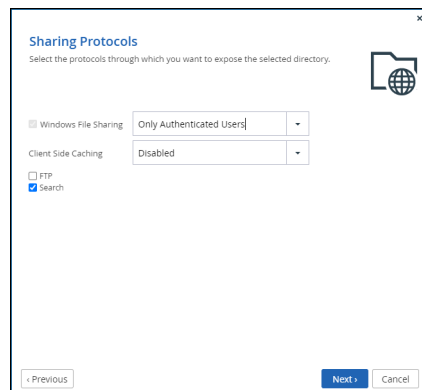
Users access the shared files and folders through standard Windows client computers; for example, using Windows File Explorer through the SMB access provided by the HCP

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.

To copy the files with their ACLs to the HCP Anywhere Enterprise Edge Filer, see [Copying Files From an External File Server to the HCP Anywhere Enterprise Edge Filer](#).

- **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.



For more information, see [Configuring Windows File Sharing](#).

**Block the following file extensions** – Prevent the creation of files with the listed extensions, with each extension separated by 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.

**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.

**Manual caching for documents** – Users must cache files manually.

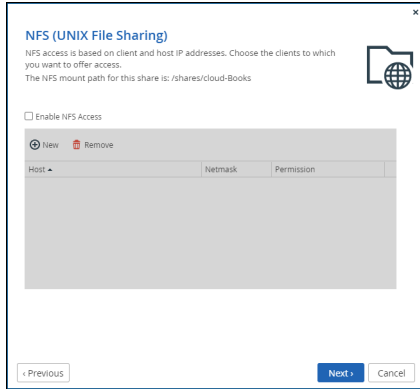
6. Specify how you want to share the files.

**FTP** – Users will be able to access and download files on this share from the FTP site. To configure the FTP server, go to **Shares > FTP Server**.

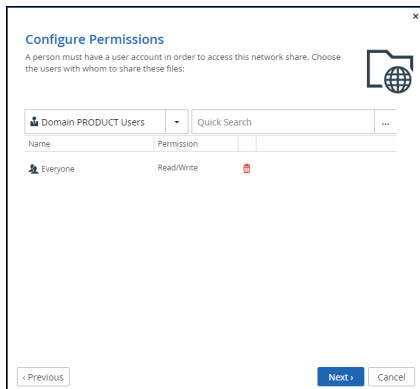
**Search** – macOS users will be able to search for files in this share.

7. Click **Next**.

The **NFS (UNIX File Sharing)** window is displayed.



- Note:** The NFS mount path for the share, when NFS access is enabled, is displayed.
8. Check the **Enable NFS Access** option to enable NFS clients to access the share. Both NFS versions 3 and 4 protocols are supported, depending on the protocol used by the client. 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**, **Read Only**, or **Read/Write**.
 Or,  
 Click **Remove** and then select the client's IP address to remove the client from the list.
  9. Click **Next** and set which users can access this network share.

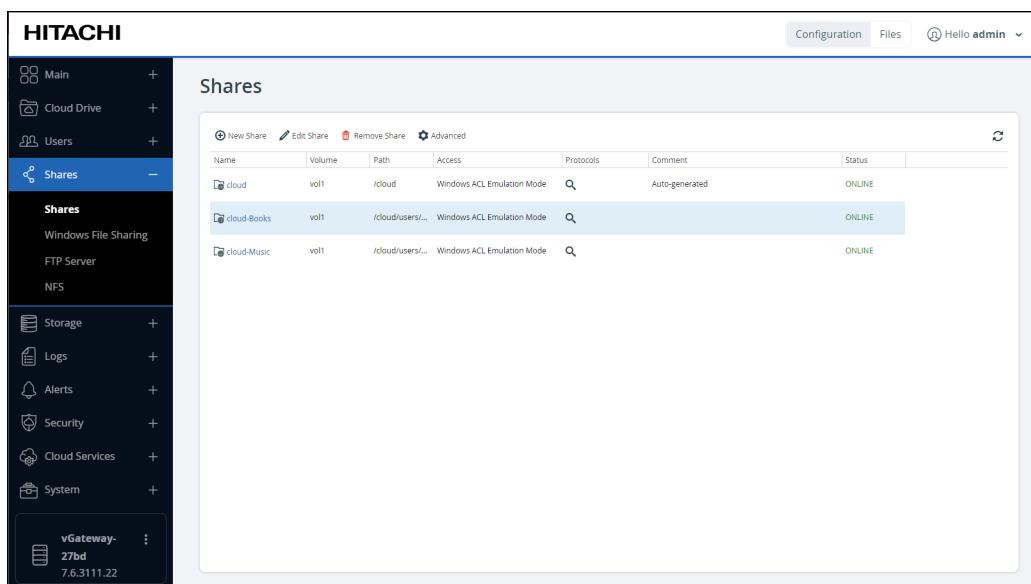


- a) In the Local Users drop-down list, select one of the following:
  - Local Users** – Search the users defined locally on the HCP Anywhere Enterprise Edge Filer.
  - Domain *domain* Users** – Search the users belonging to the domain called *domain*.
  - Local Groups** – Search the user groups defined 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 list 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.

10. Click **Next** and then **Finish** to complete the wizard.



## Blocking File Types from Network Shares

HCP Anywhere Enterprise Edge Filer administrators can block users from writing specific file types into the HCP Anywhere Enterprise Edge Filer share or gaining control of the content located on it. The file types that are blocked are set per network share.

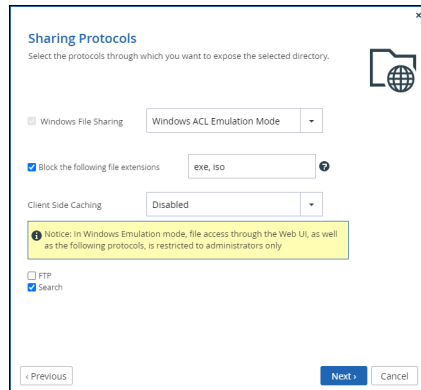
When file types are blocked, share users cannot create files or write to files with a blocked extension or rename a file to a forbidden extension. However, if you block extensions for a pre-existing share that already contains files with the forbidden extension, the pre-existing files are not deleted.

### To block files:

1. In the **Configuration** view, select **Shares > Shares** in the navigation pane.
2. Click **New Share** to create a new share with blocked file type, or **Edit Share** to block file types on an existing share.
3. Proceed through the procedure to define a network share. In the **Sharing Protocols** window:
  - a) Define the access level for **Windows File Sharing** as **Windows ACL Emulation Mode**. Users will be able to access the share using the SMB protocol and configure permissions for files and folders in the same way they would on a Windows file server.
  - b) Select the **Block the following file extensions** check box, and then define the file extensions for the types of files you want to block. You can block multiple file extensions, as shown in the image below. List only the letters of each file extension, using a comma to separate between them. For example, to block EXE files, list the `exe` file extension; to block PDF files, list the `pdf` file extension. To block both EXE and PDF files, list them as `exe, pdf`. Blocked extensions are not case sensitive.



Wildcards (for example, \*.exe) are not supported.



4. Click **Next** and continue with the wizard to create the new share or edit the existing share.

## Copying Files From an External File Server to the HCP Anywhere Enterprise Edge Filer

**Note:** To copy a whole file server (such as a Windows or NetApp file server) by migrating it to the HCP Anywhere Enterprise Edge Filer requires in-depth planning and should be done in conjunction with Hitachi Vantara support.

To copy individual shares from a file server, use the procedure described in *Migrating Shares* in the installation guide. You can also perform a delta migration when you previously set up the migration, as described in the installation guide.

## Modifying Shares

Select the share and click **Edit Share**. Proceed as for defining a new network share.

## Removing Shares

Select the share, click **Remove Share** and then **Yes** to confirm. This removes the share from the volume or folder it was defined on.

## Accessing Network Shares

This section includes the following topics:

- [Viewing Network Shares Using Windows File Sharing](#)
- [Accessing Network Shares Using FTP](#)
- [Mounting Network Shares Using NFS](#)
- [Accessing the Volumes Share](#)

## Viewing Network Shares Using Windows File Sharing

Use this procedure to view network shares when Windows File Sharing is configured. For information, see [Configuring Windows File Sharing](#).

1. On a computer connected to the same switch as the HCP Anywhere Enterprise Edge Filer, view the network neighborhood. The network neighborhood is accessed in different ways, dependent on the operating system. For example, in Microsoft Windows 10, click **Start > Settings** and then click **Network & Internet**.
2. Double-click the HCP Anywhere Enterprise Edge Filer icon.

A list of network shares is displayed.

**Note:** When accessing a network share, if the user name and password on the computer are identical to a user name and password on the HCP Anywhere Enterprise Edge Filer, the computer automatically logs in to the share using that user name and password. You will not be prompted to authenticate. In all other cases, a pop-up window will appear, and you must authenticate using a valid user name and password.

## Accessing Network Shares Using FTP

You can access the network shares through the FTP site.

1. In a web browser go to `ftp://deviceIP`.  
Where *deviceIP* is the HCP Anywhere Enterprise Edge Filer IP address.
2. Enable the FTP server on the HCP Anywhere Enterprise Edge Filer.
3. Enter the user name and password defined for you in the HCP Anywhere Enterprise Edge Filer in order to authenticate the access to the FTP.

If you enabled anonymous (unauthenticated) downloads from a specific directory, authentication is not required in order to access and download from that directory.

## Mounting Network Shares Using NFS

When NFS access is configured, use the following procedure to access network shares from a Linux/UNIX computer.

- Run the following command to mount the share: `mount deviceIP:mountPath`  
Where:

**deviceIP** – The HCP Anywhere Enterprise Edge Filer DNS namer or IP address.  
**mountPath** – The network share's mount name and path.

- Run the following command: `mount deviceIP:mountPath localFolder`  
Where:

**deviceIP** – The HCP Anywhere Enterprise Edge Filer DNS namer or IP address.  
**mountPath** – The network share's mount path.  
**localFolder** – The name of the local folder.

**Note:** To view a network share's mount path, in the **Shares > Shares** page, click the name of the network share. The **Network Share** wizard's **NFS (UNIX File Sharing)** window displays the network share's mount path in title area.

For example, if the HCP Anywhere Enterprise Edge Filer IP address is 10.1.1.1, the mount path is `/shares`, and the name is `share9` and you want to mount this network share on the local folder `/var/mnt/share9`, the relevant command is:

```
mount 10.1.1.1:/shares/share9 /var/mnt/share9
```

For more information, see [Configuring NFS Access](#).

You can use the `showmount` utility with the `-e` flag to display the path in a friendly way. For example, with NFS version 4 the results are similar to the following:

```
$ showmount -e 192.168.9.137
Export list for 192.168.9.137:
/nfs/shares/cloud-My Files 192.168.9.101/255.255.255.255
```

```
/nfs/shares/cloud-ACL_192.168.9.176/255.255.255.255,192.168.9.101/255.255.255.255
```

## Accessing the Volumes Share

Administrators can access a hidden administrative share called */volumes* using Windows File Sharing. Alternatively, they can access this share via the HCP Anywhere Enterprise Edge Filer user interface's **Files** view.

The administrative share allows direct access to the files on each of the HCP Anywhere Enterprise Edge Filer's volume.

### To access the volumes share via Windows File Sharing:

- On a computer connected to the same switch as the HCP Anywhere Enterprise Edge Filer, browse to `\\devicename\volumes\` where *devicename* is the name of the HCP Anywhere Enterprise Edge Filer. For information on viewing the HCP Anywhere Enterprise Edge Filer's name, see [Viewing HCP Anywhere Enterprise Edge Filer Details](#).

The administrative share is displayed.

**Note:** If the user name and password on the computer are identical to a user name and password on the HCP Anywhere Enterprise Edge Filer, the computer automatically logs in to the share using that user name and password. You will not be prompted to authenticate. In all other cases, a pop-up window will appear, and you must authenticate using a valid user name and password.

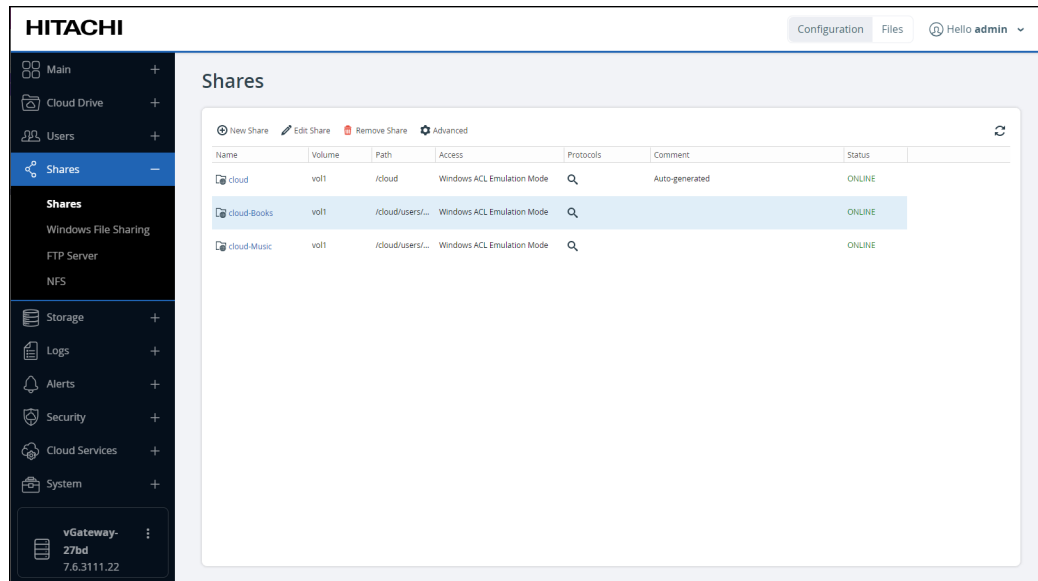
### To access the volumes share via the Files view:

- In the **Files** view, change to the **Volumes** view. The administrative share opens, displaying all volumes.

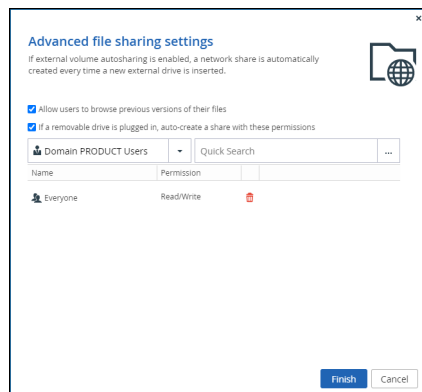
# Enabling Non-administrators to Access Previous Versions

By default, only administrators can browse and retrieve previous file versions. You can enable non-administrator users to browse and retrieve previous versions of files that they have permissions to view.

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



2. Click **Advanced**. The **Advanced file sharing settings** window is displayed.



3. Check **Allow users to browse previous versions of their files**.
4. Click **Finish**.

## To prevent users from browsing previous versions of their files:

1. In the **Configuration** view, select **Shares > Shares** in the navigation pane. The **Shares** page is displayed.
2. Click **Advanced**. The **Advanced file sharing settings** window is displayed.

3. Uncheck **Allow users to browse previous versions of their files**.
4. Click **Finish**.

# Chapter 7. Protecting the Data

## Ransomware Protection

Ransomware attacks have become an increasingly imposing threat to organizations. In most ransomware attacks, encryption restricts access to critical files, systems, and applications. This encryption process happens silently in the background.

Taking proactive measures against ransomware attacks helps safeguard your data and ensures the continuity of your operations. Each user's behavior is monitored and fed in to a machine learning algorithm trained on an extensive dataset of attack flows. Via this monitoring *HCP Anywhere Enterprise Ransom Protect* is able to detect and block ransomware attacks within seconds.

**Note:** HCP Anywhere Enterprise Ransom Protect monitors Windows File Sharing (SMB) traffic. It does not monitor user behavior on other file sharing protocols such as NFS or FTP.

Key Features of HCP Anywhere Enterprise Ransom Protect include:

- Real-time detection: Advanced machine learning algorithms identify behavioral anomalies suggesting fraudulent file activity, and block offending users within seconds.
- Zero-day protection: HCP Anywhere Enterprise Ransom Protect does not rely on traditional signature update services.
- Incident management: An administrator dashboard provides real-time attack monitoring, comprehensive incident evidence logging and post-attack forensics.
- Instant recovery: Near-instant recovery of any affected files from snapshots.

In addition, HCP Anywhere Enterprise Ransom Protect requires minimal configuration, requiring a single click to activate ransomware protection on the HCP Anywhere Enterprise Edge Filer.

## Requirements

HCP Anywhere Enterprise Ransom Protect requires a Portal Plus license on the HCP Anywhere Enterprise Portal.

In order to notify administrators by email when a suspected ransomware attack has happened, the mail server must be correctly configured. For details, see [Configuring Email Alerts](#).

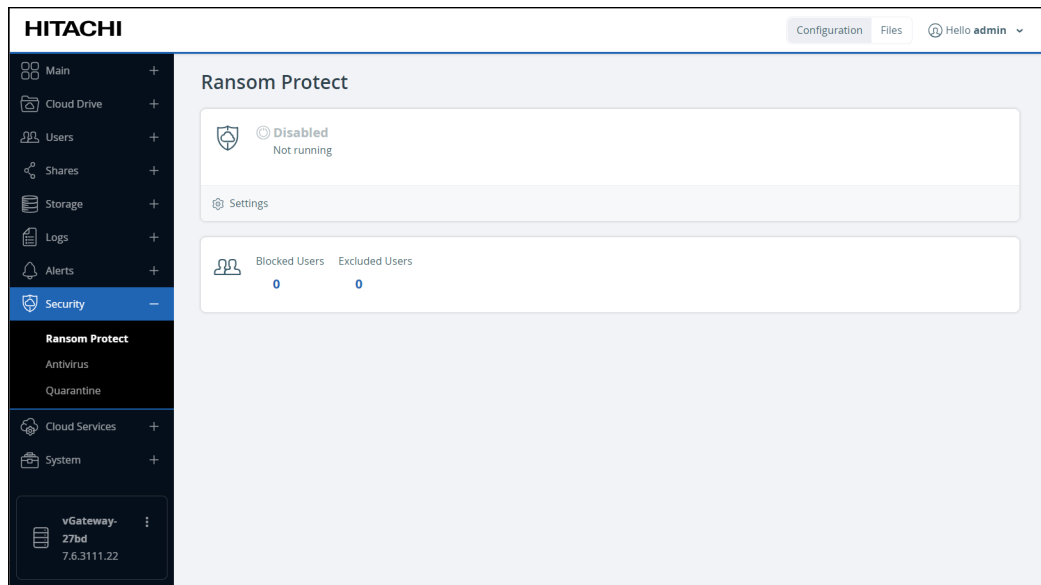
**Note:** HCP Anywhere Enterprise Ransom Protect operates on the HCP Anywhere Enterprise Edge Filer and does not rely on an Internet connection. It works even when the connection to the HCP Anywhere Enterprise Portal is down.

## Setting Up Ransom Protect

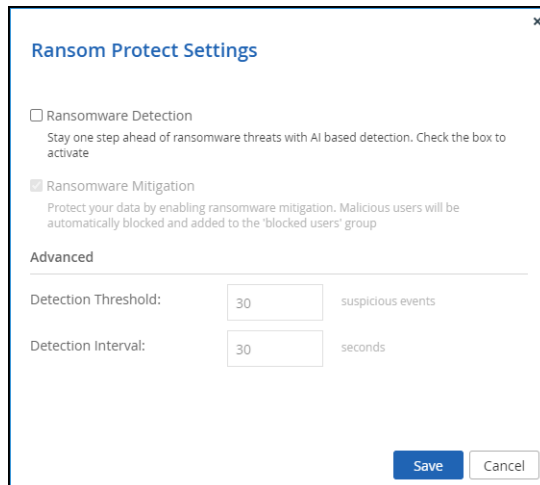
**Note:** To prevent false positive events, Hitachi Vantara recommends initially enabling HCP Anywhere Enterprise Ransom Protect in *Ransomware Detection* mode. In this mode, HCP Anywhere Enterprise Ransom Protect only monitors the traffic without blocking malicious users. After the system has proven to work well for a while, you can then enable *Ransomware mitigation*. If you encounter false positives, refer to [Coping with False Positive Detections](#).

**To enable Ransom Protect:**

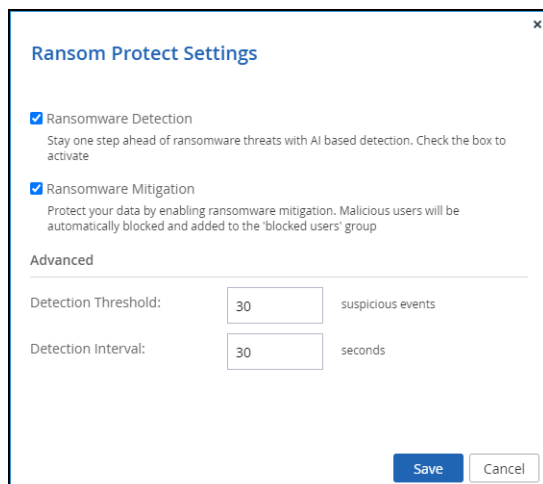
1. In the **Configuration** view, select **Security > Ransom Protect** in the navigation pane. The **Ransom Protect** page is displayed.



2. Click **Settings**.  
The **Ransom Protect Settings** window is displayed.



3. Check **Ransomware Detection**.



4. Leave the **Advanced** settings with the default values unless you encounter too many false positives. If this happens, see [Coping with False Positive Detections](#).

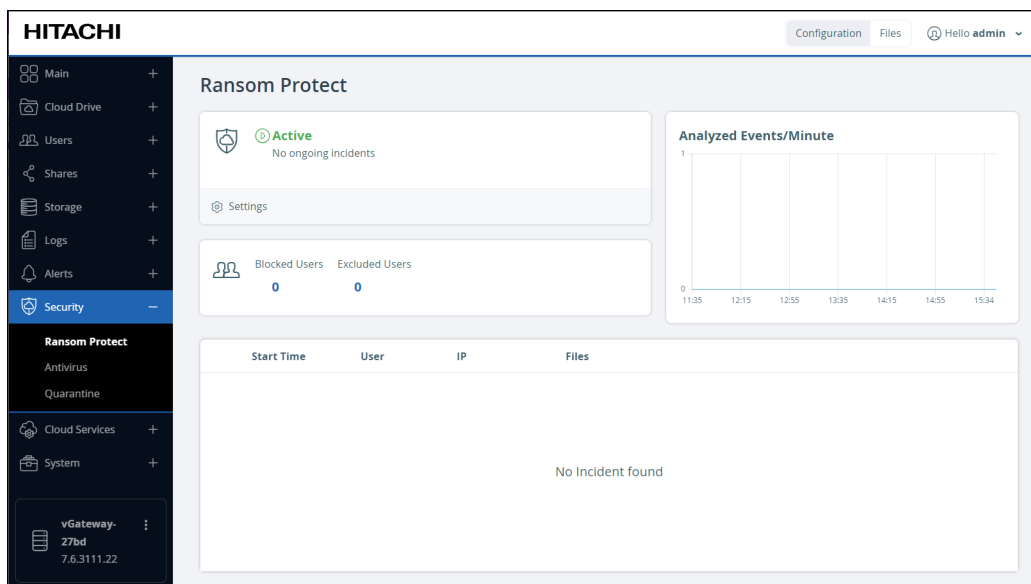
**Note:** The advanced settings default values are based on extensive testing but can be tuned if needed.

**Detection Threshold** is the number of suspicious events that must occur before ransomware protection is triggered. If the threshold is set too high, an attack could cause more damage than necessary or may go undetected. On the other hand, if it's set too low, the number of false positive detections may increase.

**Detection Interval** is the number of seconds between checks on user behavior records for potential attacks. Choosing a lower value leads to quicker ransomware detection, but it may also increase CPU load.

5. Click **Save**.

HCP Anywhere Enterprise Ransom Protect is active.





**Note:** To disable HCP Anywhere Enterprise Ransom Protect, click **Settings** in the **Ransom Protect** page and uncheck **Ransomware Detection** and then click **Save**.

## Coping with False Positive Detections

If you find that you are getting too many false positive results, you can reduce this number by Tuning the [Tuning the Detection Threshold](#) or [Excluding Specific Users From Detection](#).

### Tuning the Detection Threshold

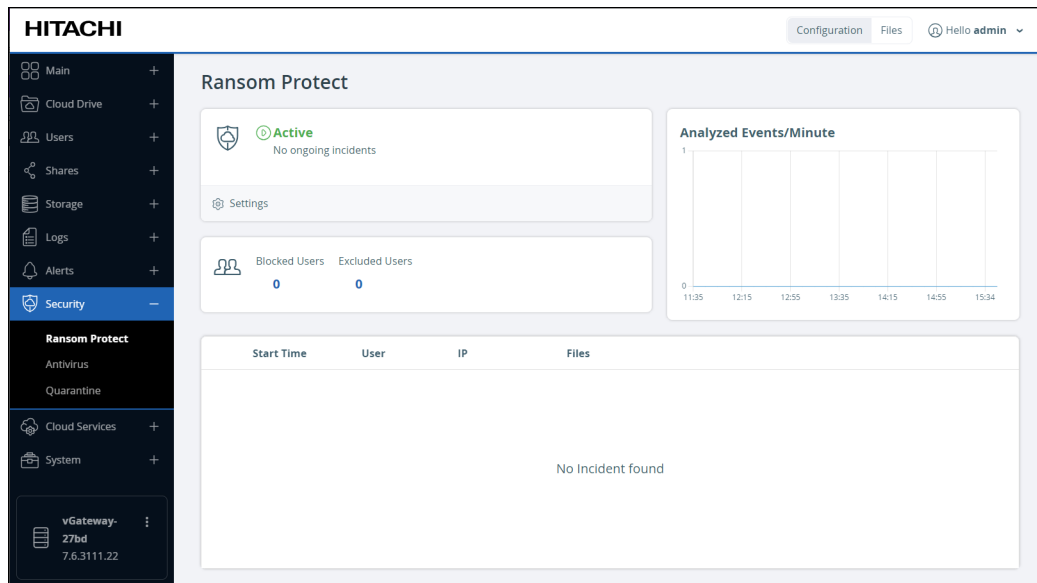
The **Detection Threshold** is the number of suspicious events that must occur before ransomware protection is triggered. To reduce the detection sensitivity, and as a consequence, the number of false positive results, you can increase the value of **Detection Threshold**.

### Excluding Specific Users From Detection

If you get false positive results for specific users, you might find that some users perform actions that are acceptable within the organization but would trigger a false positive result. You can exclude these users from having their actions checked by HCP Anywhere Enterprise Ransom Protect.

**To exclude users from ransomware detection:**

1. In the **Configuration** view, select **Security > Ransom Protect** in the navigation pane. The **Ransom Protect** page is displayed.



2. Click the number below **Exclude Users**. The **Specify Group Name** window is displayed.

**Specify Group Name**

Specify a name for this group, and optionally enter a description of this group.

Group Name:

Group GID (Optional):

Comment (Optional):

**Next >** **Cancel**

3. Click **Next**.  
The **Select Group Members** window is displayed.

**Select Group Members**

Select the members of this group:

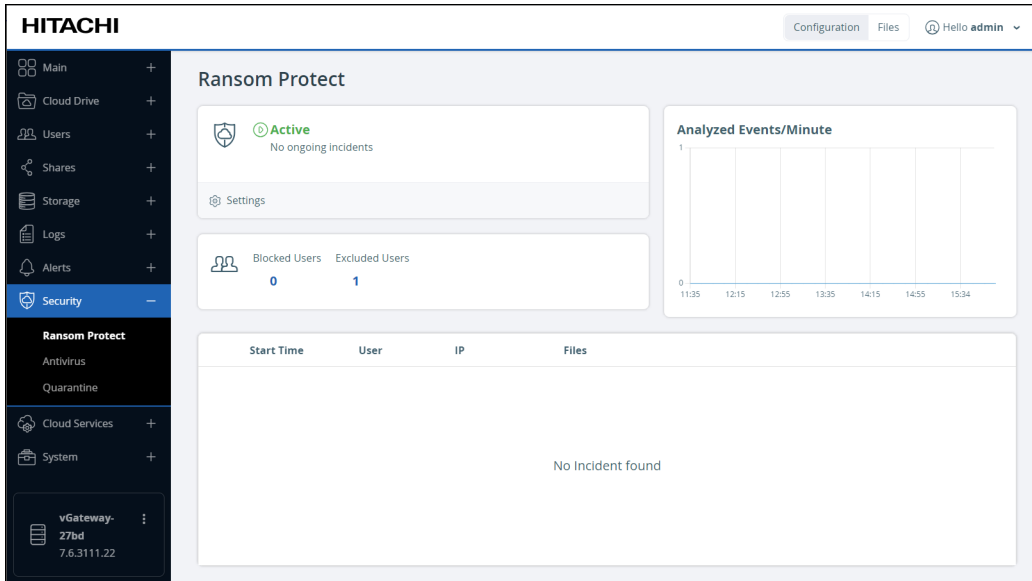
Quick Search ...

Name
------

**< Previous** **Next >** **Cancel**

4. Select the user to exclude from ransomware detection.
  - a) Select **Local Users**, **Domain *domainName* Users**, or **Domain *domainName* Groups**.
  - b) In the **Quick Search** box start entering the name of the user or group to exclude or click ... and select the user from the list.
5. Click **Next**.  
The **Wizard Completed** window is displayed.
6. Click **Finish**.

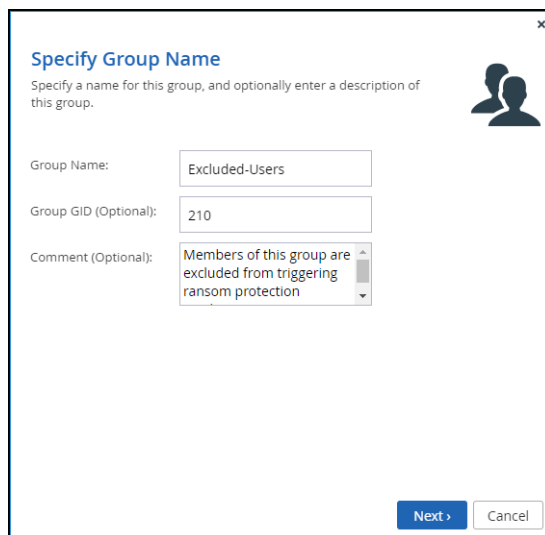
The user is excluded from ransomware detection.



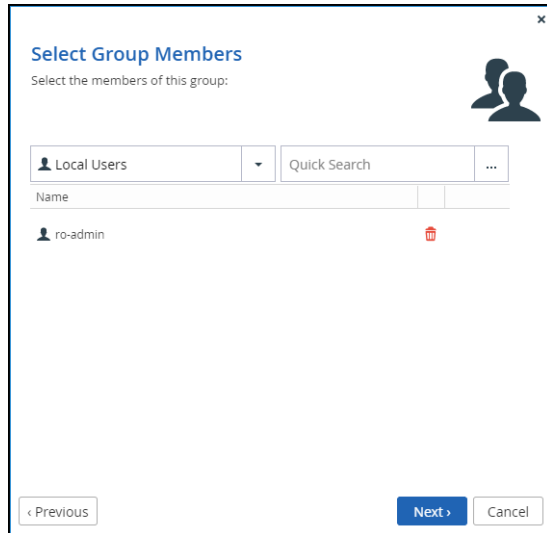
A user that has been excluded from being detected can be removed from the excluded group (for example if the user leaves the organization).


**To remove a user from the Excluded Users group:**

1. In the **Configuration** view, select **Security > Ransom Protect** in the navigation pane. The **Ransom Protect** page is displayed.
2. Click the number below **Exclude Users**. The **Specify Group Name** window is displayed.



3. Click **Next**. The **Select Group Members** window is displayed.



4. Select **Local Users**, **Domain *domainName* Users**, or **Domain *domainName* Groups** and click the  icon next to the user to remove from the list.

The user is removed from the exclude list.

## Blocking Malicious Users

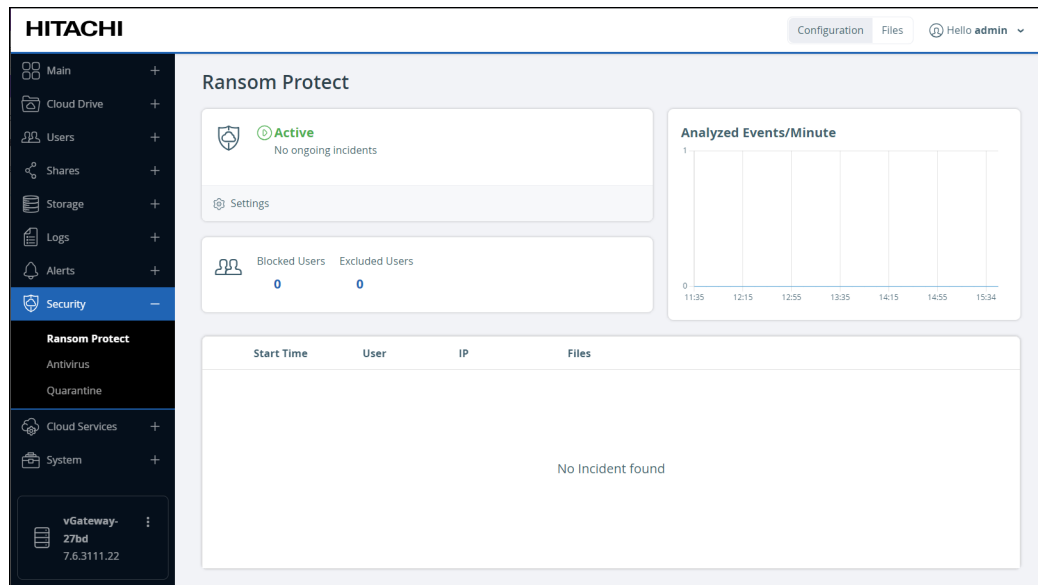
Users that you suspect of triggering ransomware attacks can be blocked by adding them to a *Blocked Users* group. Blocked users are prevented from accessing the edge filer by all authenticated protocols, including SMB, NFSv4, FTP and the HCP Anywhere EnterpriseEdge Filer user interface.

Users can be blocked automatically or manually. Users that trigger a ransomware incident can be automatically added to the *Blocked Users* group.

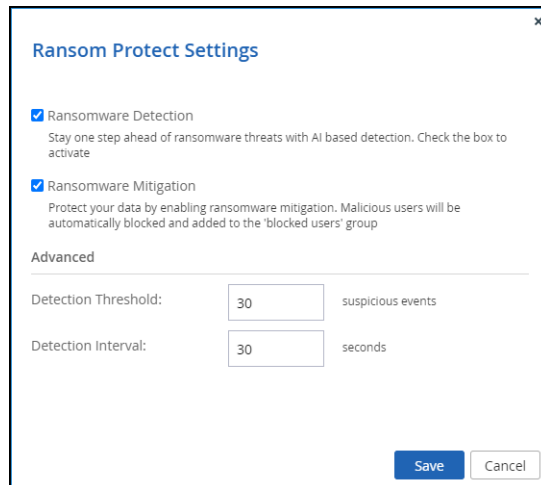
**Note:** When users are added to the *Blocked Users* group, their existing SMB sessions are immediately closed. Existing connections via other protocols are not immediately terminated, but the user is not able to create a new session.

**To block users automatically:**

1. In the **Configuration** view, select **Security > Ransom Protect** in the navigation pane. The **Ransom Protect** page is displayed.



2. Click **Settings**.  
The **Ransom Protect Settings** window is displayed.



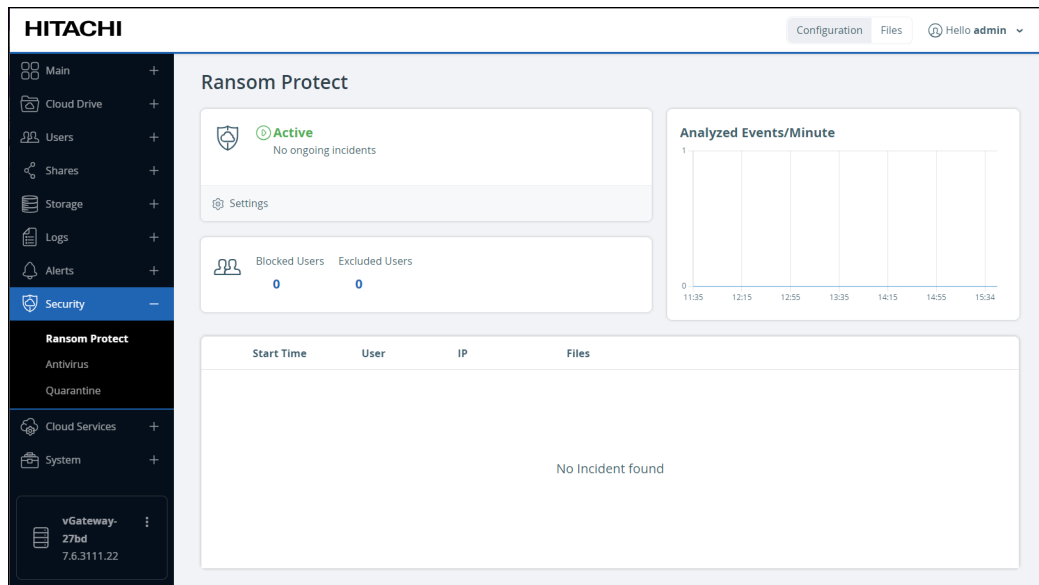
3. Make sure **Ransomware Mitigation** is checked and click **Save**.

Any incident that HCP Anywhere Enterprise Ransom Protect identifies as a ransomware attack causes the user who initiated the incident to automatically be added to the **Blocked Users** group.

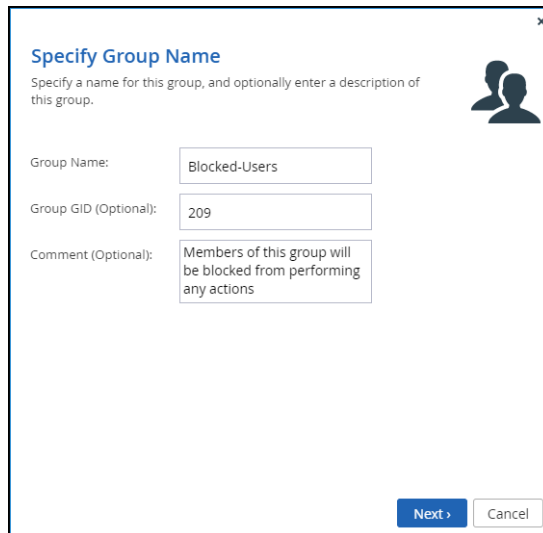
**Note:** Hitachi Vantara recommends blocking the user in Active Directory as well.

**To block users manually:**

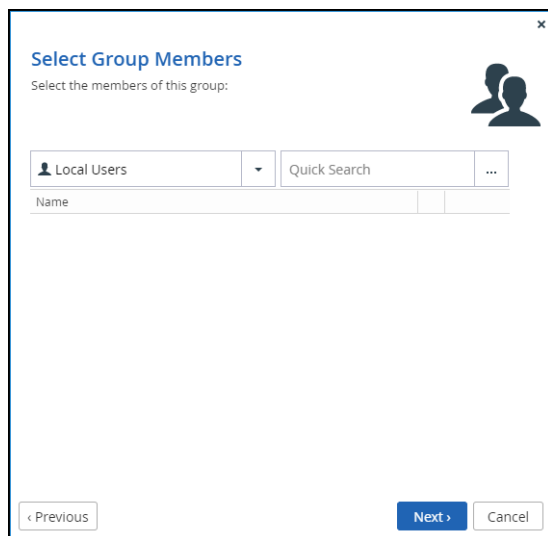
1. In the **Configuration** view, select **Security > Ransom Protect** in the navigation pane. The **Ransom Protect** page is displayed.



2. Click the number below **Blocked Users**. The **Specify Group Name** window is displayed.

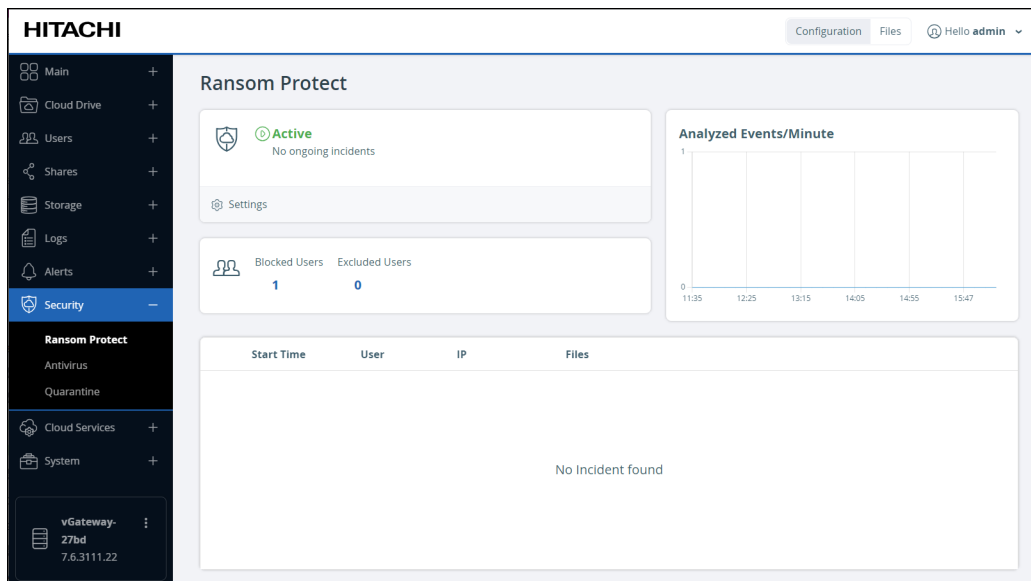


3. Click **Next**. The **Select Group Members** window is displayed.



4. Select the user to block.
  - a) Select **Local Users**, **Domain *domainName* Users**, or **Domain *domainName* Groups**.
  - b) In the **Quick Search** box start entering the name of the user or group to exclude or click . . . and select the user from the list.
5. Click **Next**.  
The **Wizard Completed** window is displayed.
6. Click **Finish**.

The user is blocked from access to the HCP Anywhere Enterprise Edge Filer.\

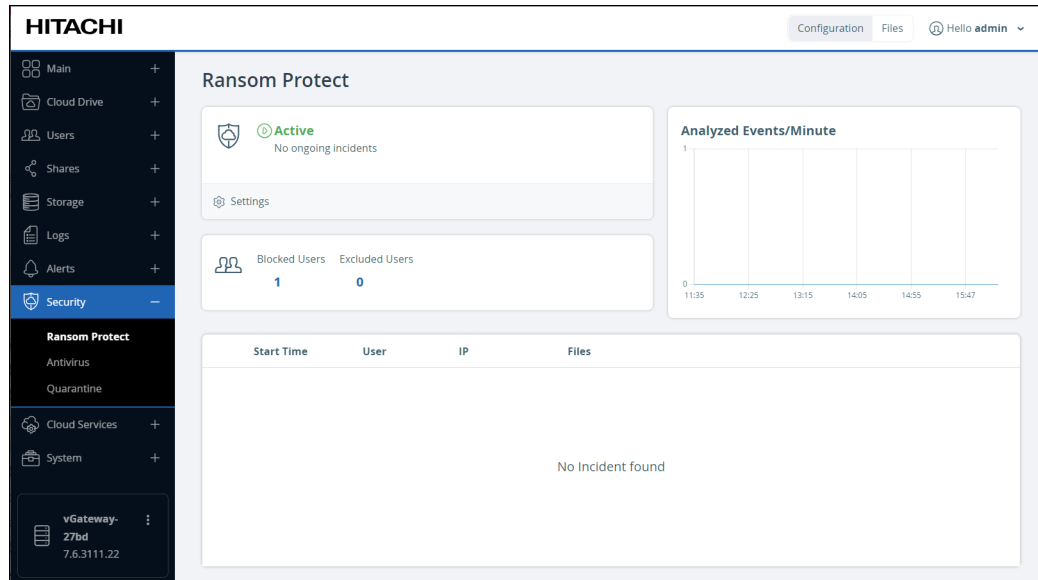


## Removing Users From the Blocked Users Group

A user that has been blocked from accessing the edge filer, can be unblocked.

### To remove a user from the Blocked Users group:

1. In the **Configuration** view, select **Security > Ransom Protect** in the navigation pane. The **Ransom Protect** page is displayed.



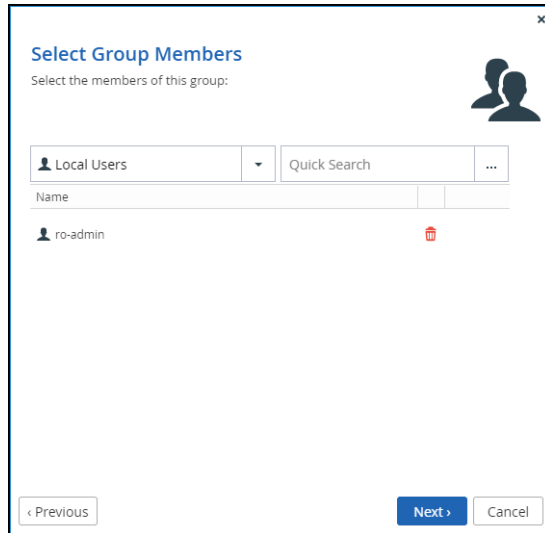
2. Click the number below **Blocked Users**. The **Specify Group Name** window is displayed.


The 'Specify Group Name' dialog box is shown. It contains the following fields and text:

- Title: Specify Group Name
- Description: Specify a name for this group, and optionally enter a description of this group.
- Group Name: Blocked-Users
- Group GID (Optional): 209
- Comment (Optional): Members of this group will be blocked from performing any actions
- Buttons: Next, Cancel

3. Click **Next**. The **Select Group Members** window is displayed.





4. Select **Local Users**, **Domain *domainName* Users**, or **Domain *domainName* Groups** and click the  icon next to the user to remove from the list.

The user is removed from the **Blocked Users** list.

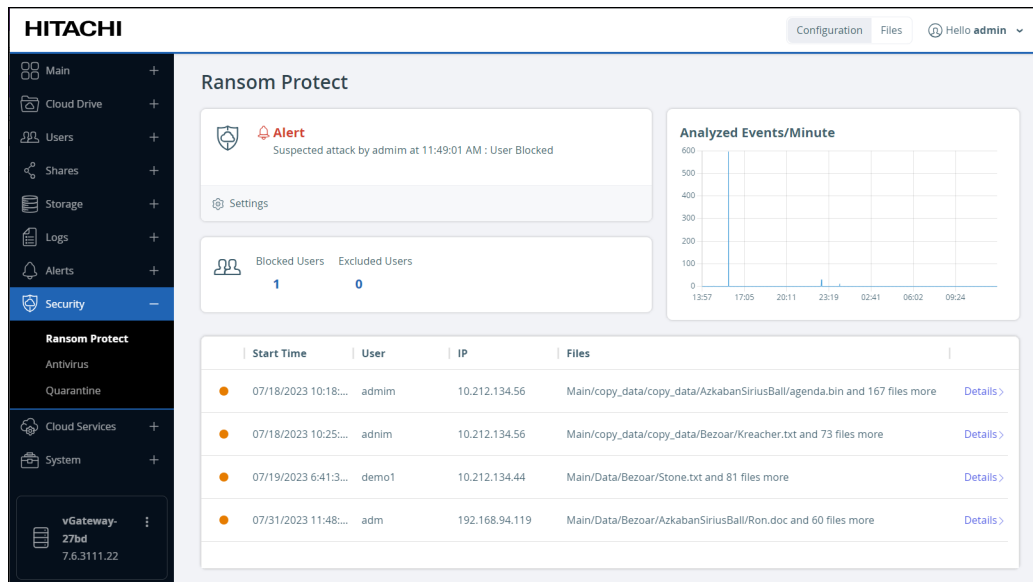
## Handling a Ransomware Incident

If a ransomware attack is identified by HCP Anywhere Enterprise Ransom Protect, the following occurs:

- The **Ransom Protect** page displays the analyzed events over time and the status changes from **Active** to **Alert**.

Start Time	User	IP	Files
07/18/2023 10:18:...	admin	10.212.134.56	Main/copy_data/copy_data/AzkabanSiriusBall/agenda.bin and 167 files more
07/18/2023 10:25:...	admin	10.212.134.56	Main/copy_data/copy_data/Bezoar/Kreacher.txt and 73 files more
07/19/2023 6:41:3...	demo1	10.212.134.44	Main/Data/Bezoar/Stone.txt and 81 files more
07/31/2023 11:48:...	adm	192.168.94.119	Main/Data/Bezoar/AzkabanSiriusBall/Ron.doc and 60 files more

- If **Ransomware Mitigation** is checked in the **Ransom Protect Settings** window, the user who initiated the suspected attack is added to the **Blocked Users** group.



An email is also sent to the administrator by the edge filer describing the attack.

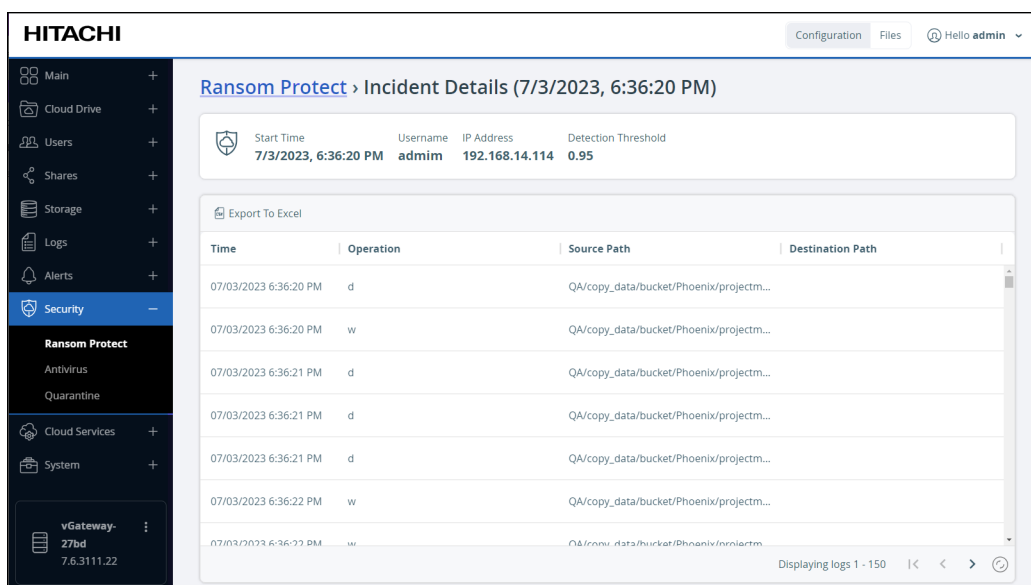
**Note:** The alert status is displayed for one hour.

## Recovering From a Ransomware Attack

Once a ransomware attack has been identified, every affected file is listed. You can then go through the list and rollback the affected files to the state immediately prior to the attack. For details, see [Accessing Previous File Versions](#).

You display the list of affected files by clicking **Details** to the right of the attack details.

The **Incident Details** page is displayed.



The top part of the Incident Details report provides the following information about the incident:

- Start Time** – The date and time that the suspected ransomware attack started.
- Username** – The name of the user that initiated the suspected attack.
- IP Address** – The IP address from where the attack was initiated.
- Detection Threshold** – A number between zero and one that is used to determine the detection sensitivity.

The second part of the **Incident Details** report provides detailed information about each operation:

- Time** – The date and time that the suspect operation started.
- Operation** – The operation that is suspected of being a ransomware attack.
- Source Path** – The full path and file name of the file that the suspected attack affected.
- Destination Path** – If the file was moved, the full path and file name of the destination.

#### **To export the incident details report to Microsoft Excel:**

1. Access the **Incident Details** page for the ransomware incident.
2. Click **Export to Excel**.

The incident details are exported as an Excel file to your computer.

## **Investigating Ransomware Incidents**

Hitachi Vantara is dedicated to providing the best user experience possible and can investigate false positive incidents to better configure HCP Anywhere Enterprise Ransom Protect.

To analyze ransomware incident, send the support report to Hitachi Vantara support. The support report includes the HCP Anywhere Enterprise Ransom Protect service logs, as well as the incident details report. For details about sending a support report to Hitachi Vantara Support, see [Generating a Support Report](#).

## **Antivirus File Scanning**

Antivirus software is used to prevent malware from infecting files in the organization. When antivirus is enabled, every file that is copied, moved, or edited on the HCP Anywhere Enterprise Edge Filer is automatically and transparently scanned for malware before the user can access the file. HCP Anywhere Enterprise Edge Filers integrate with *McAfee Endpoint Security for Linux Threat Prevention* to ensure data protection.

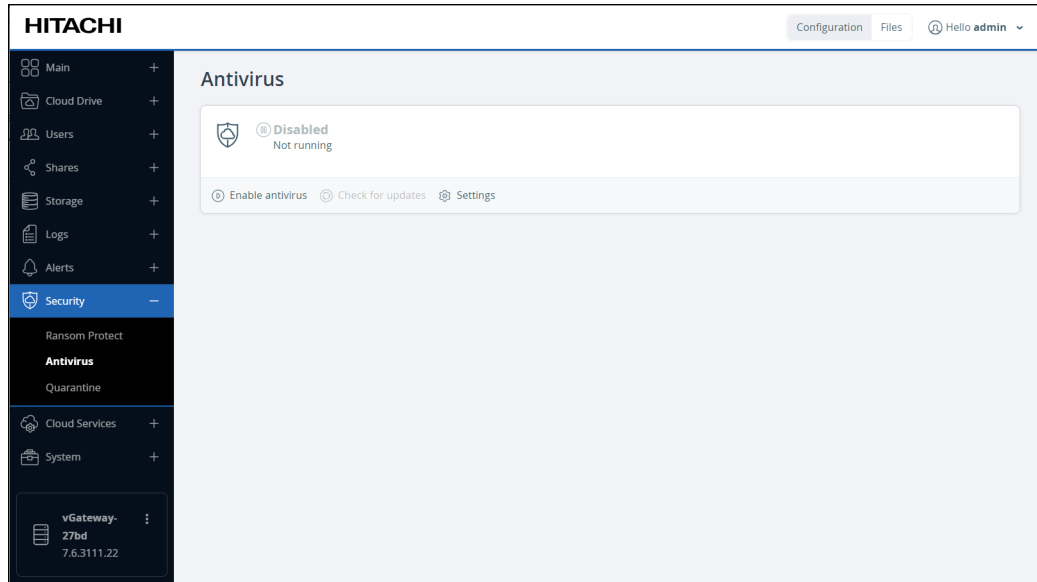
**Note:** Stub files are not scanned for viruses until the files are downloaded from the HCP Anywhere Enterprise Portal.

Infected files are quarantined so that they are no longer available and not synced to the HCP Anywhere Enterprise Portal. The administrator is informed so that any action that might be necessary can be determined.

## Setting up Antivirus File Scanning

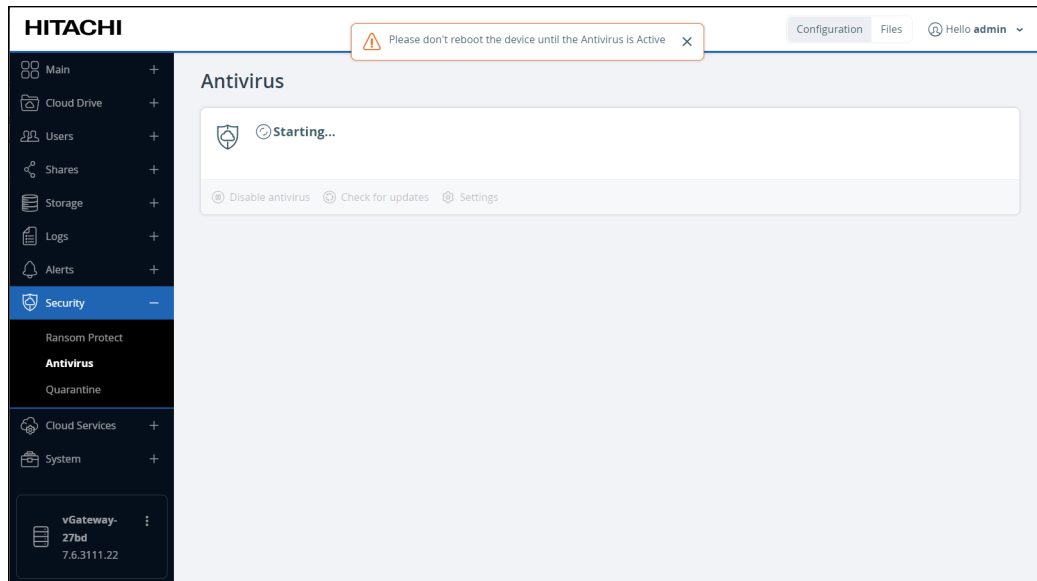
### To enable antivirus scanning:

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

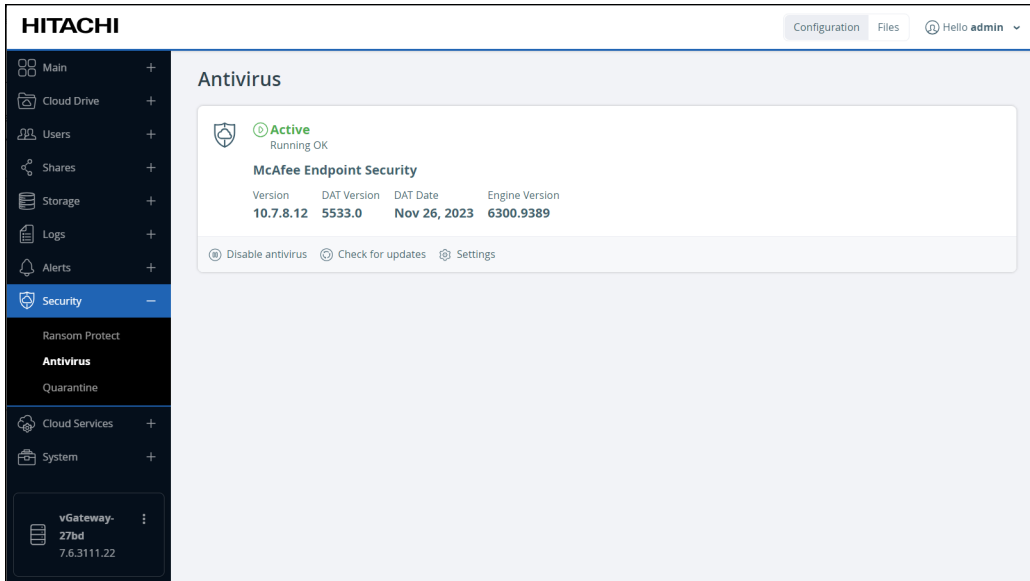


2. Click **Enable antivirus**.

**Warning:** You must not restart the edge filer while the antivirus software is starting up.



Antivirus scanning is enabled and a check for the latest DAT file is run after which antivirus protection is active.



Scanning for malware will occur on every file that is accessed from the HCP Anywhere Enterprise Edge Filer.

**To disable antivirus scanning:**

1. In the **Configuration** view, select **Security > Antivirus** in the navigation pane. The **Antivirus** page is displayed.
2. Click **Disable** antivirus.

Antivirus scanning is disabled.

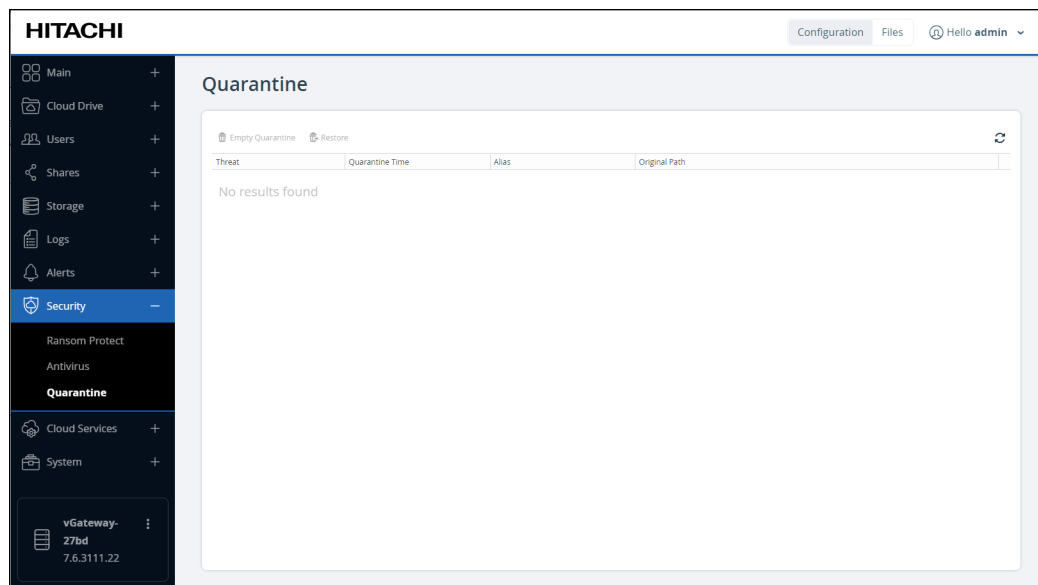
## Managing Quarantined Files

Files that have been identified as a threat to the system are placed in quarantine and removed from their source location. These files are also not synced to the HCP Anywhere Enterprise Portal.

An administrator is alerted when a file is quarantined. The administrator can check the list of quarantined files and either delete files permanently or restore them. Quarantined files are only displayed when antivirus has been enabled. If the signature for the file has not changed, it will immediately be added back to quarantine, but a file that an updated DAT file recognizes as not being a virus, can be restored.

### To manage quarantined files:

- In the **Configuration** view, select **Security > Antivirus** in the navigation pane. The Quarantine page is displayed.



Each quarantined file is displayed with the following information:


**Threat** – The name of the threat.

**Quarantine Time** – The time the file was accessed and then moved to quarantine.


**Alias** – The virus alias recognized by the DAT file.

**Original Path** – The name and location of the file before it was quarantined.


### To empty the quarantine of all files:

1. Without selecting any of the quarantined files, click the  icon.
1. Click **Yes** to confirm the delete.  
All the quarantined files are permanently deleted. The quarantine folder is cleaned every 30 days.

### To select one or more quarantined files to permanently delete:

1. Select the files to delete and click the  icon.
1. Click **Yes** to confirm the delete.  
The quarantined files are permanently deleted.

### To restore one or more quarantined files to their original location:

1. Select the files to restore and click the  icon.
1. Click **Yes** to confirm the restore.  
The quarantined files are restored to their original location. If the signature for the file has not changed, it will immediately be added back to quarantine.

## Updating the Antivirus DAT File

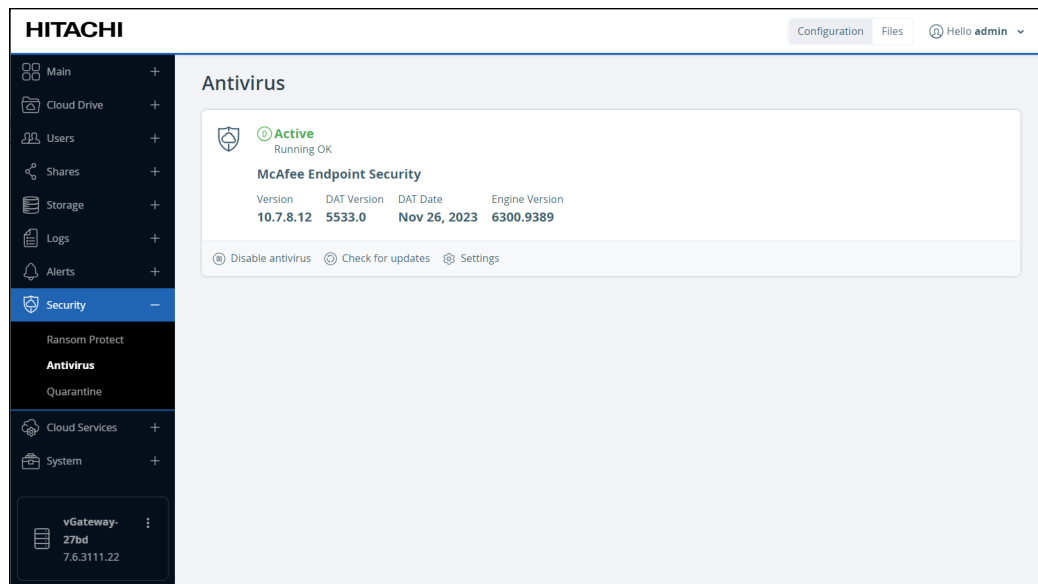
Antivirus software is constantly being updated to be able to identify the new viruses. Virus definition or DAT files contain virus signatures and other information used to protect the HCP Anywhere Enterprise Edge Filer against existing and new potential threats. Generally, DAT files are released daily.

You can schedule the HCP Anywhere Enterprise Edge Filer to check for new DAT files which are then used when scanning files for viruses. You can also manually check for updates, for example when you think a new DAT file has been released before the scheduled update is set to run.

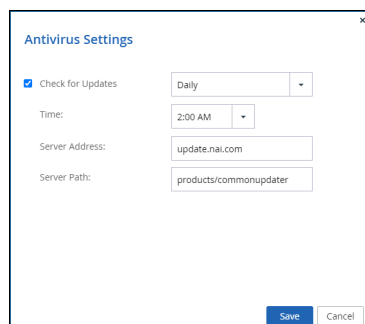
**Note:** To check for updates to DAT files, the HCP Anywhere Enterprise Edge Filer must be able to connect to antivirus update site.

### To schedule checking for DAT updates:

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



2. Click **Settings**. The **Antivirus Settings** window is displayed.

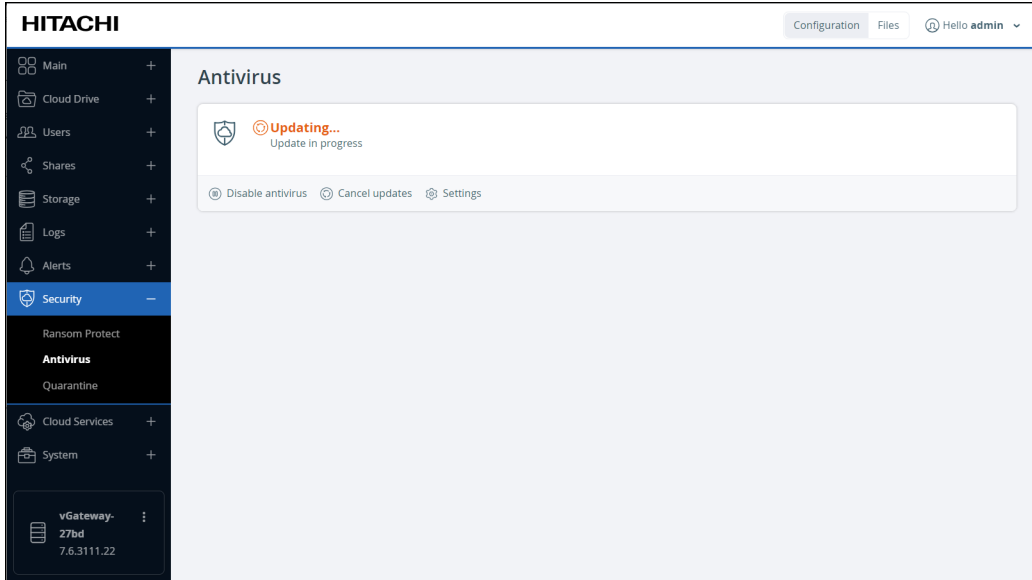


3. Make sure **Check for Updates** is checked and then set the update details. You can set the scheduler to check for new DAT files daily, weekly or monthly. HCP Anywhere

Enterprise recommends keeping the default daily check.  
You set the scheduler to access the antivirus provider to use the latest DAT file from the relevant server, specifying the server address and path.

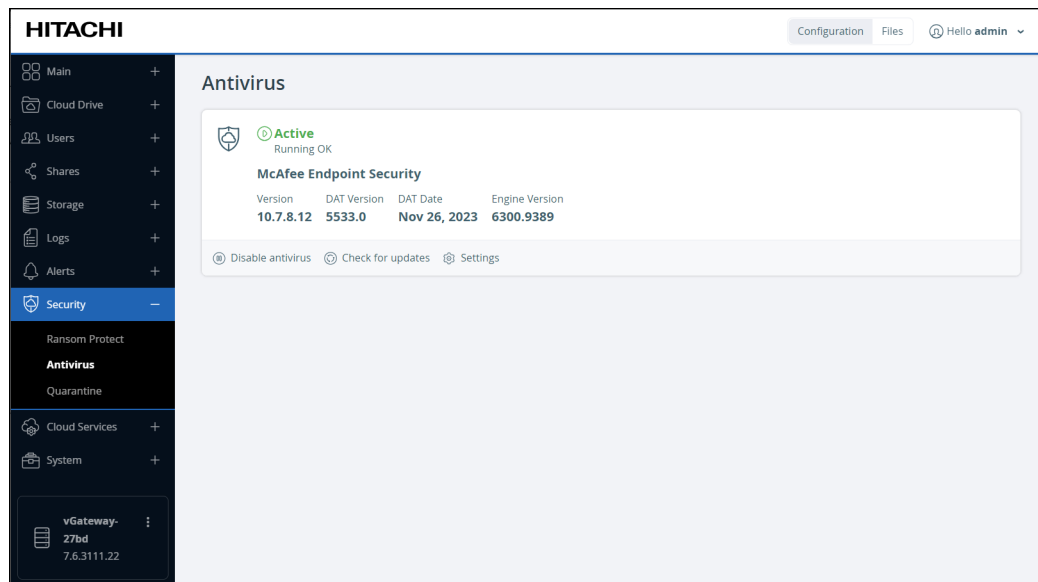
4. Click **Save**.

At the selected time, the system checks for the latest DAT file to use when scanning files.



### To manually check for DAT updates:

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



2. Click **Check for updates**.



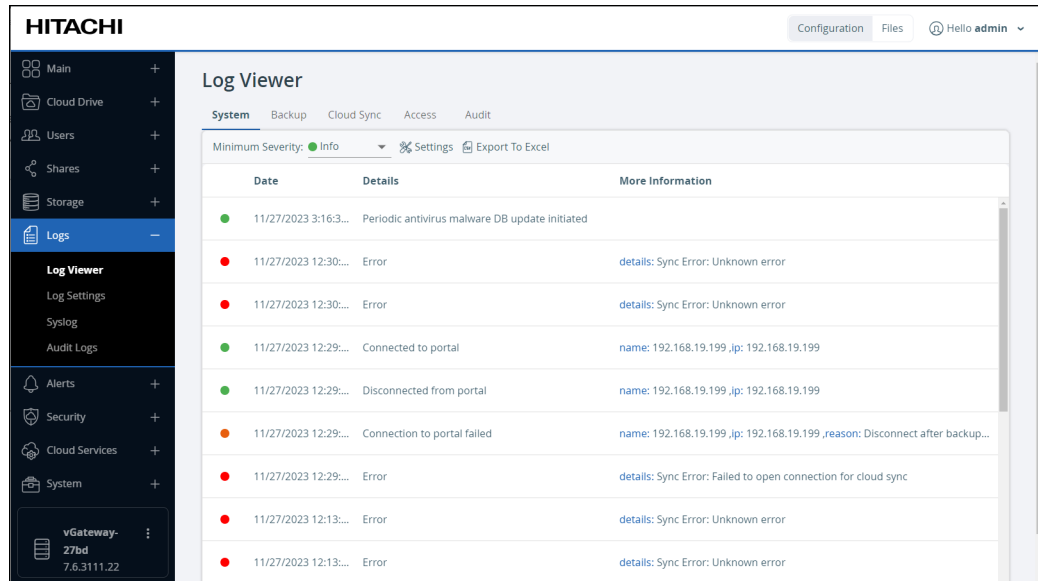
The system checks for the latest DAT file to use when scanning files.

## Antivirus Logs

Log entries for the antivirus are part of the System log. The System log shows whether a file is in quarantine or has been restored from quarantine.

### To view logs:

- In the **Configuration** view, select **Logs > Log Viewer** in the navigation pane. The **Log Viewer** page opens, displaying the **System** log that includes any antivirus log entries.



The screenshot displays the Hitachi Log Viewer interface. The top navigation bar includes 'Configuration', 'Files', and 'Hello admin'. The left sidebar shows a navigation menu with 'Logs' selected. The main content area is titled 'Log Viewer' and shows a table of system logs. The table has columns for 'Date', 'Details', and 'More Information'. The logs include entries for 'Periodic antivirus malware DB update initiated', 'Error', 'Connected to portal', 'Disconnected from portal', 'Connection to portal failed', and 'Sync Error: Failed to open connection for cloud sync'.

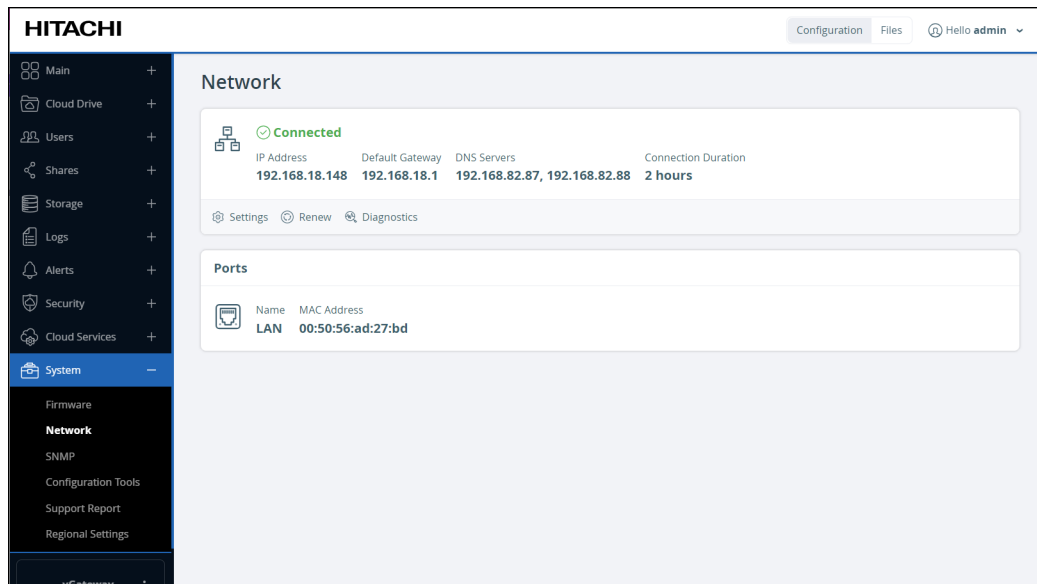
Date	Details	More Information
11/27/2023 3:16:3...	Periodic antivirus malware DB update initiated	
11/27/2023 12:30:...	Error	details: Sync Error: Unknown error
11/27/2023 12:30:...	Error	details: Sync Error: Unknown error
11/27/2023 12:29:...	Connected to portal	name: 192.168.19.199, jip: 192.168.19.199
11/27/2023 12:29:...	Disconnected from portal	name: 192.168.19.199, jip: 192.168.19.199
11/27/2023 12:29:...	Connection to portal failed	name: 192.168.19.199, jip: 192.168.19.199, reason: Disconnect after backup...
11/27/2023 12:29:...	Error	details: Sync Error: Failed to open connection for cloud sync
11/27/2023 12:13:...	Error	details: Sync Error: Unknown error
11/27/2023 12:13:...	Error	details: Sync Error: Unknown error

For log details, see [Viewing Different Types of Logs](#).

# Chapter 8. Managing Network Settings

To view HCP Anywhere Enterprise Edge Filer's network and port settings:

- In the **Configuration** view select **System > Network** in the navigation pane. The **Network** page is displayed.



The Network page displays the following:

- The HCP Anywhere Enterprise Edge Filer's IP address.
- The IP address of the default HCP Anywhere Enterprise Edge Filer.
- The IP addresses of the primary and secondary DNS servers.
- The status of the HCP Anywhere Enterprise Edge Filer's network connection: Connected or Disconnected.
- The amount of time that the HCP Anywhere Enterprise Edge Filer has been connected to the network.
- The MAC address of this HCP Anywhere Enterprise Edge Filer.

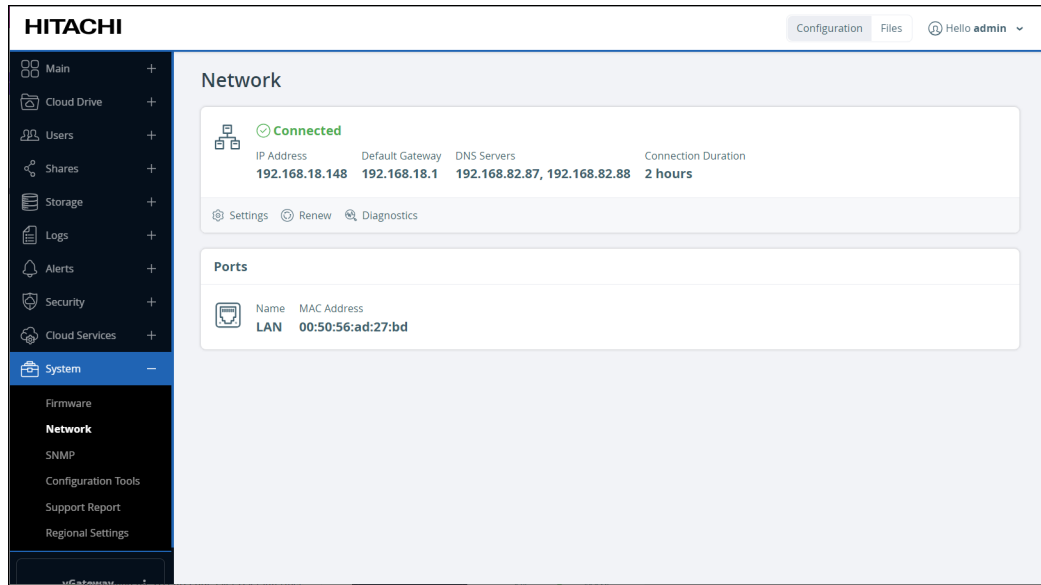
## Configuring Network Settings

By default, the HCP Anywhere Enterprise Edge Filer is automatically assigned an IP address and DNS settings by the DHCP server. If the network uses static IP addresses instead of DHCP, you must configure the HCP Anywhere Enterprise Edge Filer's network settings.

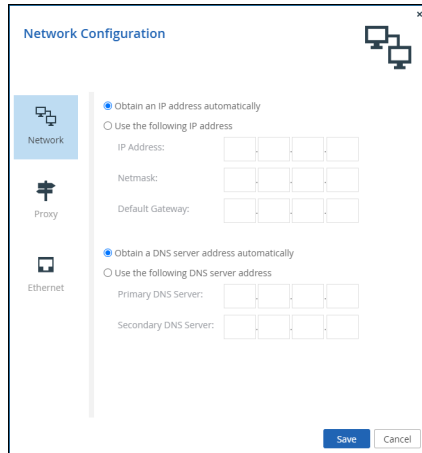
- Note:** If a DHCP server is not available, then, after one minute, the HCP Anywhere Enterprise Edge Filer uses IP address 192.168.192.5.  
You can apply a custom DNS configuration to each HCP Anywhere Enterprise Edge Filer according to its DHCP class identifier.

**To configure network settings:**

1. In the **Configuration** view select **System > Network** in the navigation pane. The **Network** page is displayed.



2. Click **Settings**. The **Network Configuration** window is displayed.



3. Configure the settings.
  - Obtain an IP address automatically** – The HCP Anywhere Enterprise Edge Filer obtains an IP address automatically from the DHCP server in the network.
  - Use the following IP address** – Assign the HCP Anywhere Enterprise Edge Filer a static IP address and specify the IP address, netmask, and default HCP Anywhere Enterprise Edge Filer.
  - Obtain a DNS server address automatically** – The HCP Anywhere Enterprise Edge Filer obtains DNS server addresses automatically from the DHCP server in the network.
  - Use the following DNS server address** – Specify DNS servers for the HCP Anywhere Enterprise Edge Filer and specify the address of the primary and secondary DNS servers.

**Note:** If you configure these settings incorrectly, you may lose network connectivity to the HCP Anywhere Enterprise Edge Filer.

4. Click **Save**.

## Configuring Proxy Server Settings

The HCP Anywhere Enterprise Edge Filer can be configured to connect to the network via a proxy server. To configure proxy settings, see [Configuring Access to a Proxy Server](#).

## Configuring Ethernet Port Settings

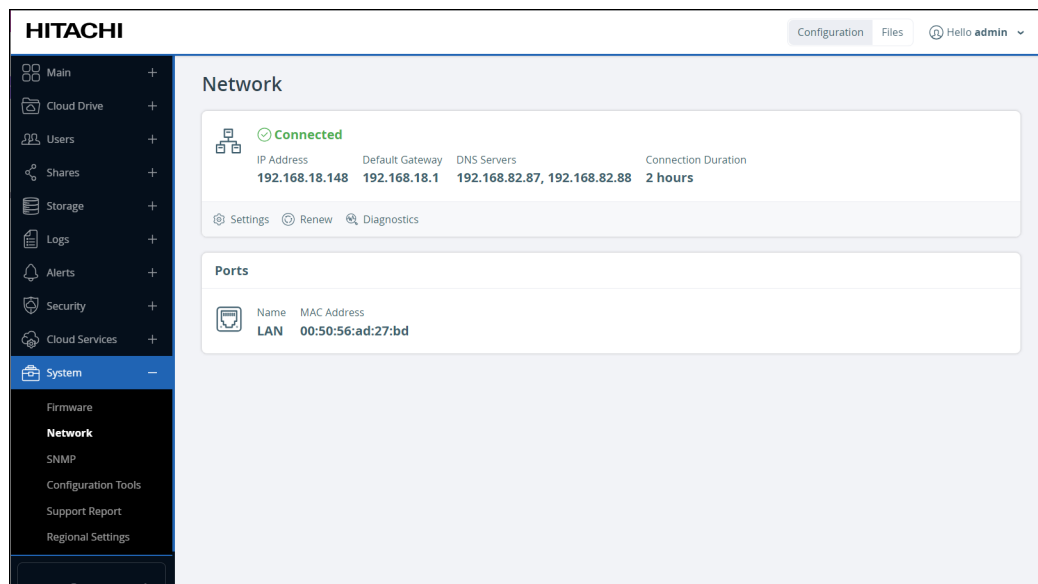
By default, the HCP Anywhere Enterprise Edge Filer automatically detects the Ethernet port's link speed and duplex. If desired, you can manually restrict the Ethernet port to a specific link speed and duplex.

You can also configure HCP Anywhere Enterprise Edge Filer to use jumbo frames. While the standard Ethernet frame is 1500 bytes, jumbo frames are larger, with the conventional jumbo frame size being 9000 bytes.

**Warning:** If you enable jumbo frames, you must configure all computers in the HCP Anywhere Enterprise Edge Filer's network segment to use the same Ethernet frame size (maximum transmission unit, or MTU). If you do not set all computers to the same MTU, you may lose connectivity to the HCP Anywhere Enterprise Edge Filer.

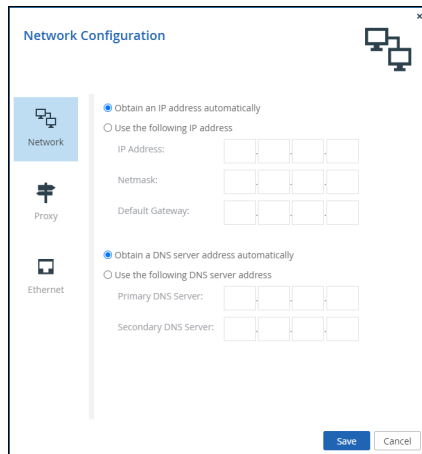
**To configure the Ethernet port settings:**

1. In the **Configuration** view select **System > Network** in the navigation pane. The **Network** page is displayed.

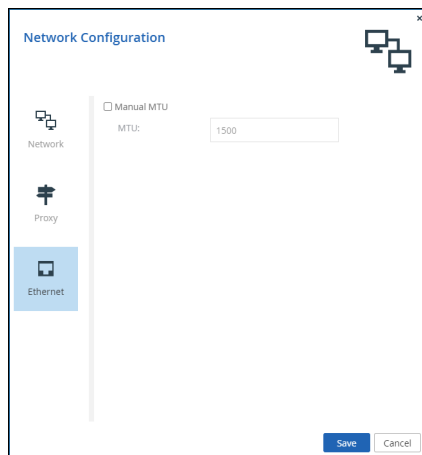


2. Click **Settings**.

The **Network Configuration** window is displayed.



3. Select the **Ethernet** option.



4. Specify the Ethernet settings.

**Manual MTU** – Manually set the maximum transmission unit (MTU), for example for jumbo frames.

- **MTU** – The maximum transmission unit in bytes. The minimum MTU for jumbo frames is 1500.

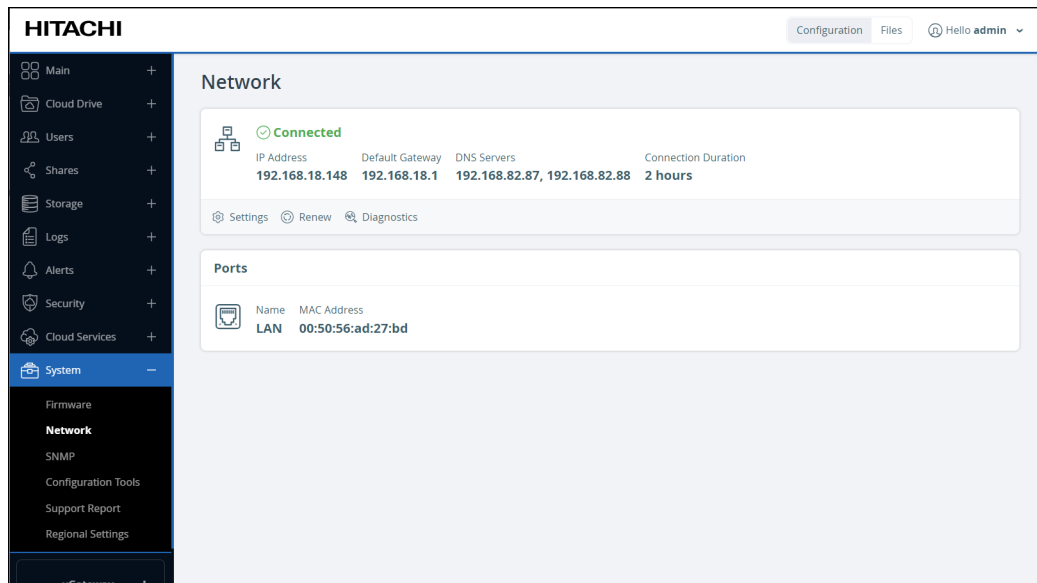
5. Click **Save**.

# Renewing the DHCP Lease

The DHCP lease is renewed automatically as needed. However, you can manually renew the DHCP lease, if necessary.

## To manually renew the DHCP lease:

1. In the **Configuration** view select **System > Network** in the navigation pane. The **Network** page is displayed.



2. Click **Renew**.

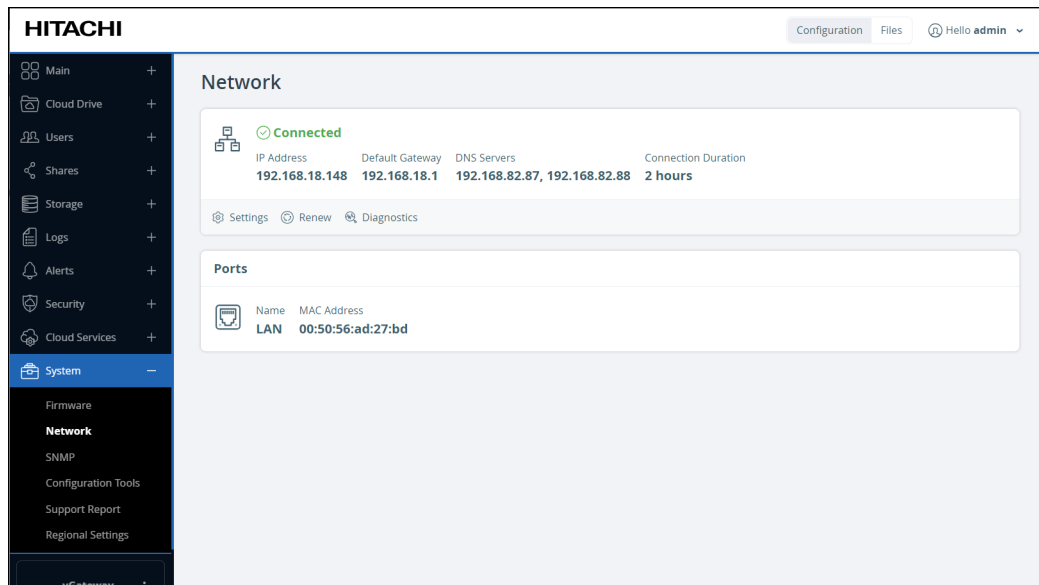
# Network Diagnostics

The HCP Anywhere Enterprise Edge Filer provides diagnostic tools directly through the user interface for network troubleshooting:

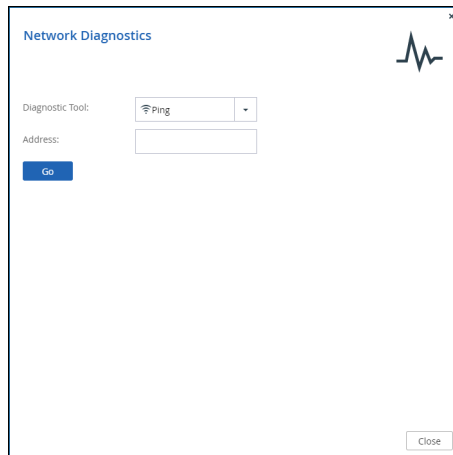
- Ping** – Tests the reachability of a host on the network.
- DNS lookup** – Queries the DNS.
- Traceroute** – Displays the route packets across the network.
- TCP Connect** – Tests whether a specific TCP port is open.
- Wake** – Remotely awakens computers using the WoL (Wake on LAN) command.
- iPerf** – Measures the maximum achievable upload and download bandwidths using either TCP or UDP.

**To use network diagnostics:**

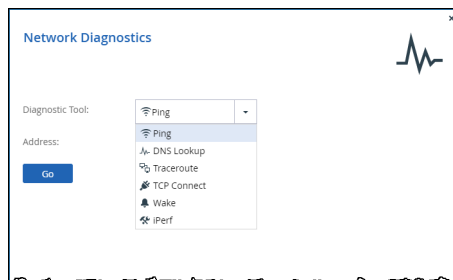
1. In the **Configuration** view select **System > Network** in the navigation pane. The **Network** page is displayed.



2. Click **Diagnostics**. The **Network Diagnostics** window is displayed.



3. In the **Diagnostic Tool** field, select the tool you want to use.

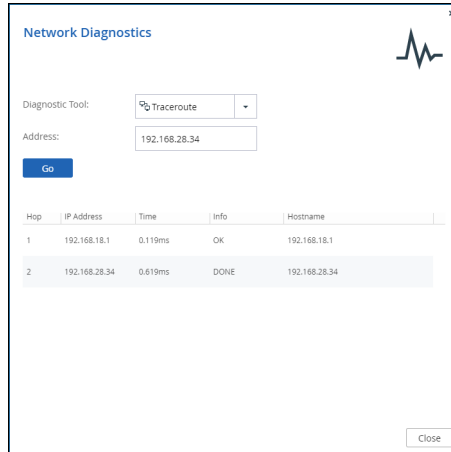


The window changes to reflect the diagnostic test requested. **Ping**, **DNS Lookup**, and **Traceroute** all require an address.

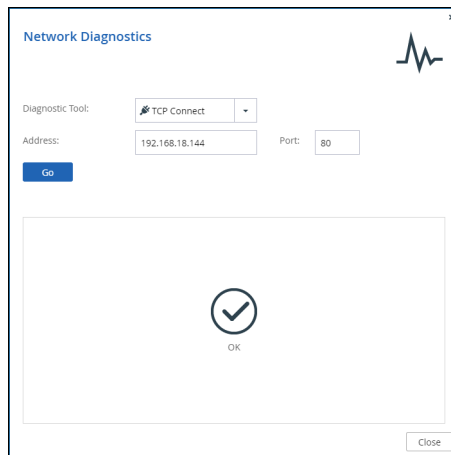
**Ping** – Tests the reachability of a host on the network.

**DNS Lookup** – Queries the DNS.

**Traceroute** – Displays the route packets across the network. For example:

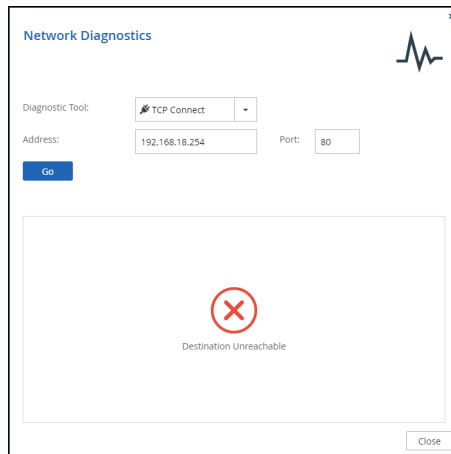


**TCP Connect** – Tests whether a specific TCP port is open.



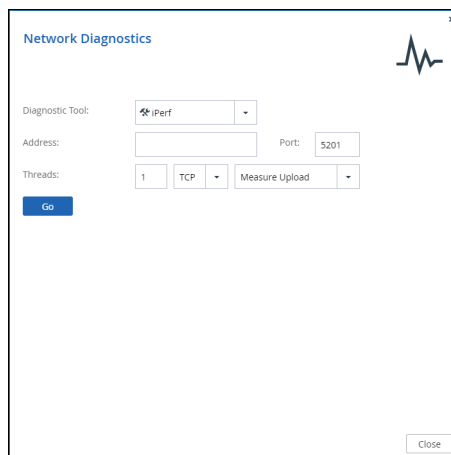


Or:



**Wake** – Remotely awakens computers using the WoL (Wake on LAN) command based on the MAC address of the computer. For more details, see [Remotely Awakening Computers](#).

**iPerf** – Measures the maximum achievable upload and download bandwidths using either TCP or UDP.



Where:

**Address** – The address of the computer to measure.

**Port** – The port to measure.

**Threads** – The number of threads to test the connection.

**TCP or UDP** – The protocol to measure.

**Measure Upload or Measure Download** – The direction to measure. The following command is run: `iperf -c {Address} -fM -m -i5 -t25 -p {Port}`

If the number of threads is changed from the default, 1, the command is run with the `-P` flag with the thread number. For example,

```
iperf -c {Address} -fM -m -i5 -t25 -p {Port} -P 10
```

If UDP is specified, the command is run with the `-u` flag. For example:

```
iperf -c {Address} -fM -m -i5 -t25 -p {Port} -u
```

4. Enter the information required for the test, such as the IP address you want to ping.
5. Click **Go**.

The test results are displayed in the window, under the tool details.

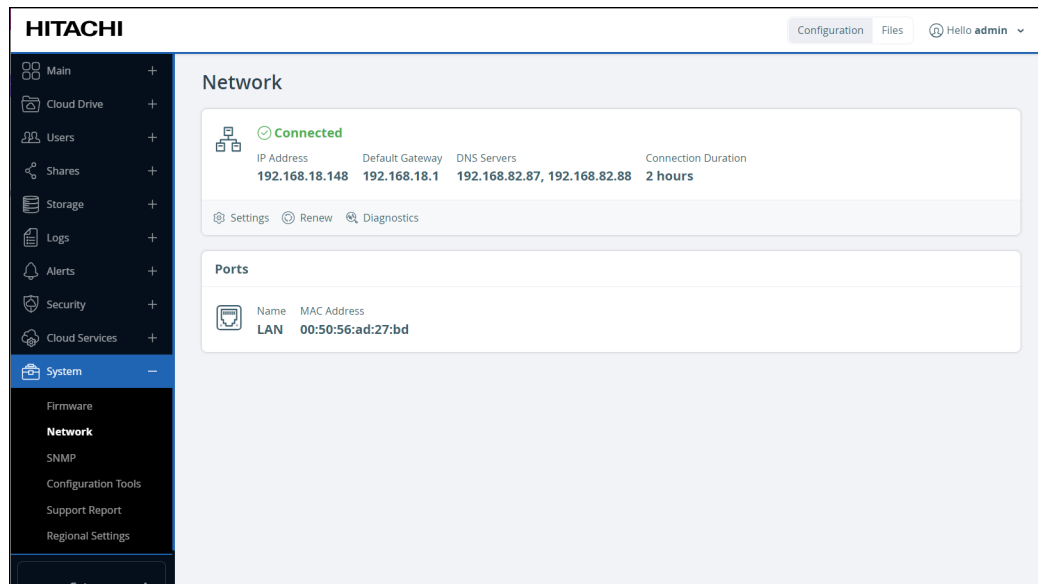
6. Click **Close** when you have completed the diagnostic tests.

## Remotely Awakening Computers

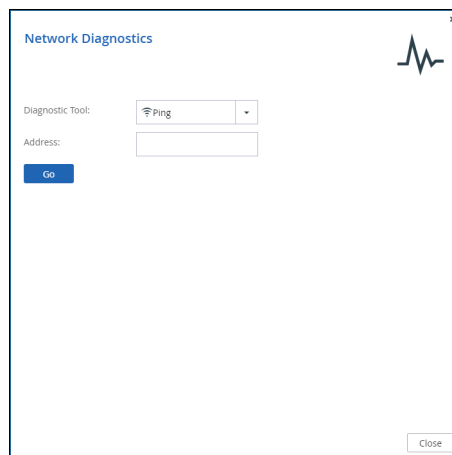
Administrators can remotely turn on or awaken computers via using the WoL (Wake on LAN) command. This is useful, for example, when there is a need to release a software update. The command wakes up a single device, so must be run multiple times to wake up more than one computer.

### To wake up a device:

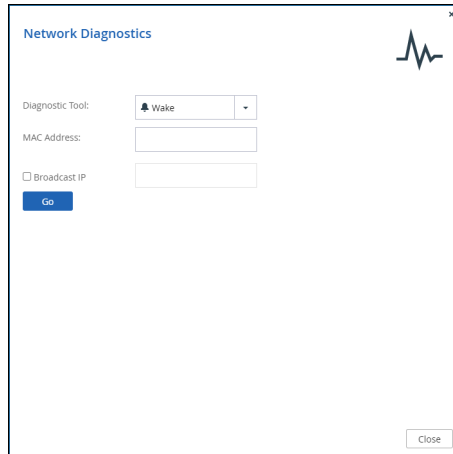
1. In the **Configuration** view select **System > Network** in the navigation pane. The **Network** page is displayed.



2. Click **Diagnostics**. The **Network Diagnostics** window is displayed.



3. Select **Wake** as the diagnostic tool.



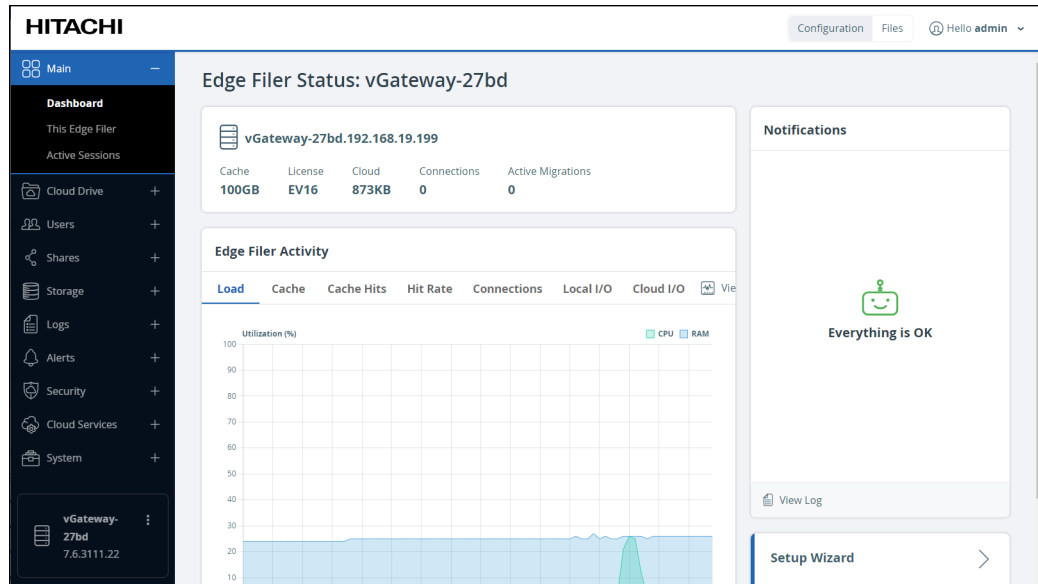
4. Enter the device's MAC address.
5. Optionally, check **Broadcast IP** and enter a broadcast address for the broadcast.
6. Click **Go**.  
An **OK** message is displayed when the device is awakened.
7. Click **Close**.

# Chapter 9. Monitoring the HCP Anywhere Enterprise Edge Filer

The HCP Anywhere Enterprise Edge Filer dashboard provides an overview of the HCP Anywhere Enterprise Edge Filer's current status.

**To view the status dashboard:**

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



The dashboard displays the following information:

- An overview of the edge filer:
  - The edge filer name and IP.
  - The total storage available locally on the edge filer.
  - The license.
  - The amount of storage that is synced from the portal.
  - The number of connections to the edge filer.
  - The number of active migrations.
- **Device Activity** – The edge filer activity over time, displayed graphically
  - **Load** – The CPU and RAM usage.  
When the Load activity is displayed, you can also display the processes currently running:  
Click **View Processes**.  
The **Top Processes** window is displayed.

Top Processes						
PID	Name	RAM	RAM (%)	CPU (%)	Threads Count	
1	/usr/lib/systemd/systemd	5.8MB	0%	0%	1	
448	/usr/lib/systemd/system...	3.4MB	0%	0%	1	
773	/usr/lib/systemd/system...	2.9MB	0%	0%	1	
774	/usr/sbin/smartd	4.7MB	0%	0%	1	
775	csrrdd:	25.4MB	0%	0%	1	
777	/usr/bin/vmtoolsd	7.7MB	0%	0%	2	
779	php	25.8MB	0%	0%	1	

Total Rows: 93

Close

Where:

**PID** – The process identifier.

**Name** – The process name.

**RAM** – The amount of RAM used by this process.

**RAM (%)** – The percentage of the RAM used by this process.

**CPU** – The percentage of CPU used by this process.

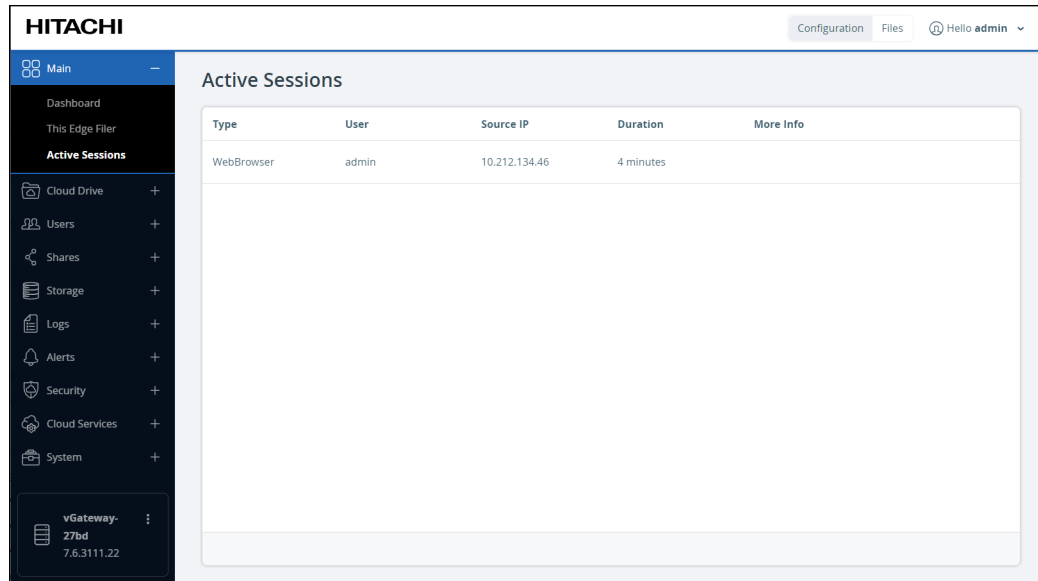
**Threads Count** – The number of threads spawned by the process.

- **Cache** – The amount of storage used in the cache.
- **Cache Hits** – The cache hits, misses and thrashing when accessing files and performing operations, such as *write*, on the files.
  - Hit** – The file was accessed from the cache: it was not a stub file.
  - Miss** – The file was a stub file that was downloaded from the portal. However, the file had not been accessed within the last 24 hours.
  - Thrashing** – The file was a stub file that was downloaded from the portal. The file was not in the cache for less than 24 hours. Thrashing means that files that were recently evicted are needed.
- **Hit Rate** – The hit rate: A measurement of how many content requests a cache is able to fill successfully, *hits*, compared to how many requests it receives. The higher the cache hit ratio, the healthier the system.
  - Note:** You can use the cache hit rate to determine peak usage times.
- **Connections** – The number of SMB/CIF and NFS connections.
- **Local I/O** – The I/O between the HCP Anywhere Enterprise Edge Filer and local connections.
- **Cloud I/O** – The I/O between the HCP Anywhere Enterprise Edge Filer and HCP Anywhere Enterprise Portal.
- **Notifications** – Notifications for the administrator about the edge filer. You can go straight to the **Log Viewer** to get more information by clicking **View Log**.
- Links to the **Setup Wizard** and **File Server Migration**.

## Viewing Session Activity

### To view edge filer Activity:

- In the **Configuration** view, select **Main > Active Sessions** in the navigation pane. The **Active Sessions** page is displayed.



The following information is displayed:

**Type** – The session type:

- **NFS**
- **CIFS** (Windows File Sharing)
- **Web Browser**

**User** – The user connected to the HCP Anywhere Enterprise Edge Filer.

**Source IP** – The IP address from which the user connected to the HCP Anywhere Enterprise Edge Filer.

**Duration** – The amount of time that the user has been connected to the HCP Anywhere Enterprise Edge Filer.

**More Info** – Additional information about the session, such as the client port when the type is NFS.

**Note:** The data is refreshed automatically every few seconds.

## Using SNMP Monitoring

You can configure the HCP Anywhere Enterprise Edge Filer for monitoring using SNMP. This enables you to gather a wide range of information about the devices.

SNMP can be used with all HCP Anywhere Enterprise Edge Filers. SNMP v1, v2c, and v3 are supported. SNMPv3 security level is set to Authentication and Privacy with SHA + AES algorithms.

HCP Anywhere Enterprise Edge Filer includes Net-SNMP. For details, refer to <http://www.net-snmp.org>.

Information is collected for the following MIBS:

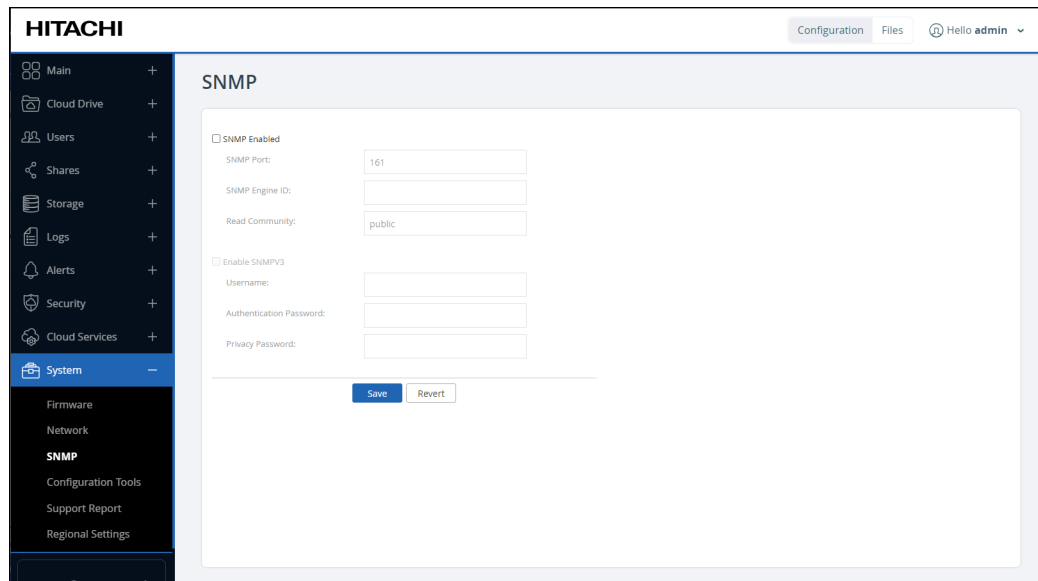
- **MIB-II (IF-MIB):** Basic description of the monitored system, such as the system name, uptime, and network interfaces. For details of this MIB, refer to <http://www.net-snmp.org/docs/mibs/interfaces.html> and <http://www.net-snmp.org/docs/mibs/ifMIBObjects.html>.
- **HOST-RESOURCES-MIB:** Computer management information, hardware and software configuration, such as information regarding system initialization, processes, storage, memory, processors, and devices. For details of this MIB, refer to <http://www.net-snmp.org/docs/mibs/host.html>.
- **UCD-SNMP-MIB:** System performance data, such as system statistics and performance. For details of this MIB, refer to <http://www.net-snmp.org/docs/mibs/ucdavis.html>.

The MIBs are stored on the SNMP server on the HCP Anywhere Enterprise Edge Filer. You can monitor the HCP Anywhere Enterprise Edge Filer MIBs using a management tool, such as the tool from <https://www.paessler.com/>.

## Setting Up SNMP Monitoring on the HCP Anywhere Enterprise Edge Filer

### To set up SNMP monitoring:

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



2. Check the **SNMP Enabled** check box to activate SNMP, and then configure the following settings:

**SNMP Port** – The default is TCP 161.

**Note:** SNMP Engine ID is defined automatically based on the MAC address and cannot be changed.

**Read Community** – Configure as Read-Only. The SNMP Read-Only Community String is like a password. It is sent along with each SNMP Get-Request and allows or denies access to device.

If you are using SNMP v3, check the **Enable SNMPV3** check box, and then enter a user name,

- authentication password, and the privacy password, which must be a minimum of 8 characters.
3. Click **Save** to save the settings and activate SNMP monitoring.



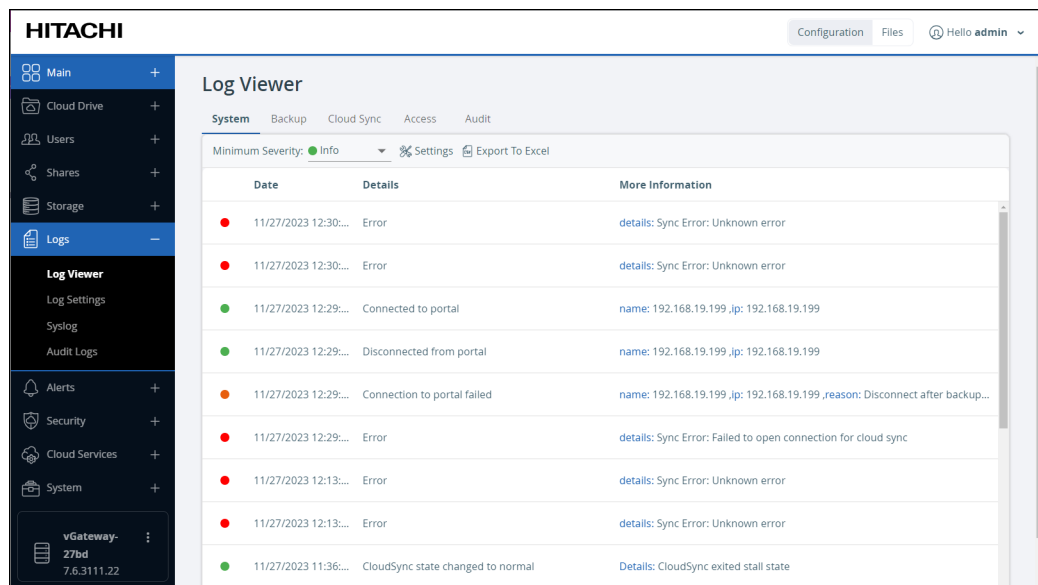
# Chapter 10. HCP Anywhere Enterprise Edge Filer Logs

Each HCP Anywhere Enterprise Edge Filer includes logs to facilitate managing the site.

The HCP Anywhere Enterprise Edge Filer contains a log viewer that displays the different actions on the HCP Anywhere Enterprise Edge Filer. You can change what is displayed, such as the log levels to display.

## To access the Log Viewer:

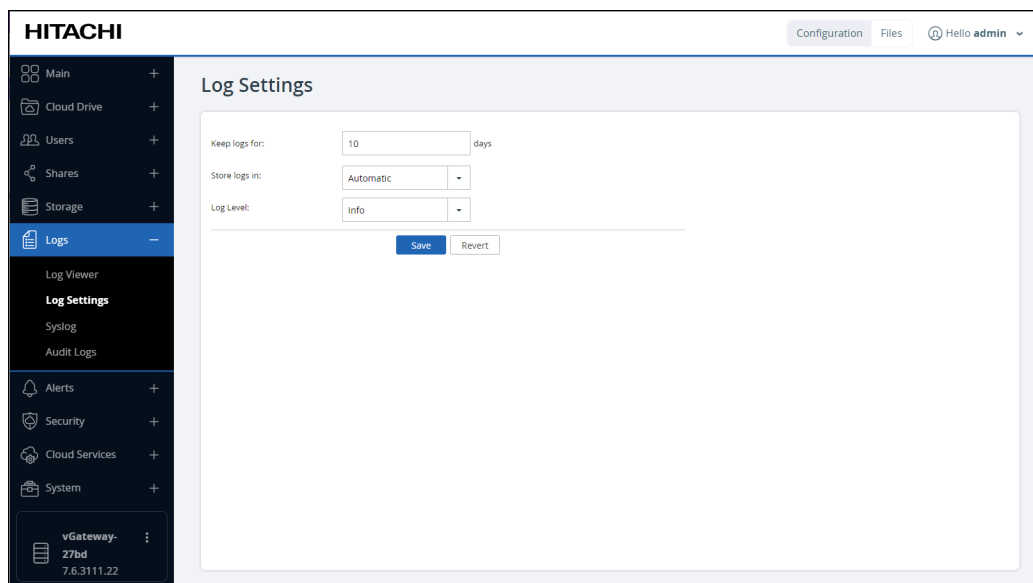
- In the **Configuration** view, select **Logs > Log Viewer** in the navigation pane. The **Log Viewer** page is displayed.



# Configuring Logging

## To configure log settings:

1. In the **Configuration** view, in the navigation pane:  
Either, select **Logs > Log Settings**,  
Or, select **Logs > Log Viewer** and click **Log Settings**.  
The **Log Settings** page is displayed.



2. Configure the settings as required:  
**Keep logs for** – The number of days that the HCP Anywhere Enterprise Edge Filer stores logs.  
**Store logs in** – The volume where the HCP Anywhere Enterprise Edge Filer stores logs. If you choose Memory, the logs are deleted each time you reboot the HCP Anywhere Enterprise Edge Filer.  
**Log Level** – The minimum log level to display in the HCP Anywhere Enterprise Edge Filer user interface. For example, if you select **Critical**, then only **Critical**, **Alert**, and **Emergency** logs are displayed in the HCP Anywhere Enterprise Edge Filer user interface. The logs are filtered accordingly.
3. Click **Save**.

You can also configure the HCP Anywhere Enterprise Edge Filer to send logs to a syslog server, described in [Configuring Syslog Settings](#). While the HCP Anywhere Enterprise Edge Filer log is limited by the amount of available storage space, a syslog server can store an unlimited number of logs.

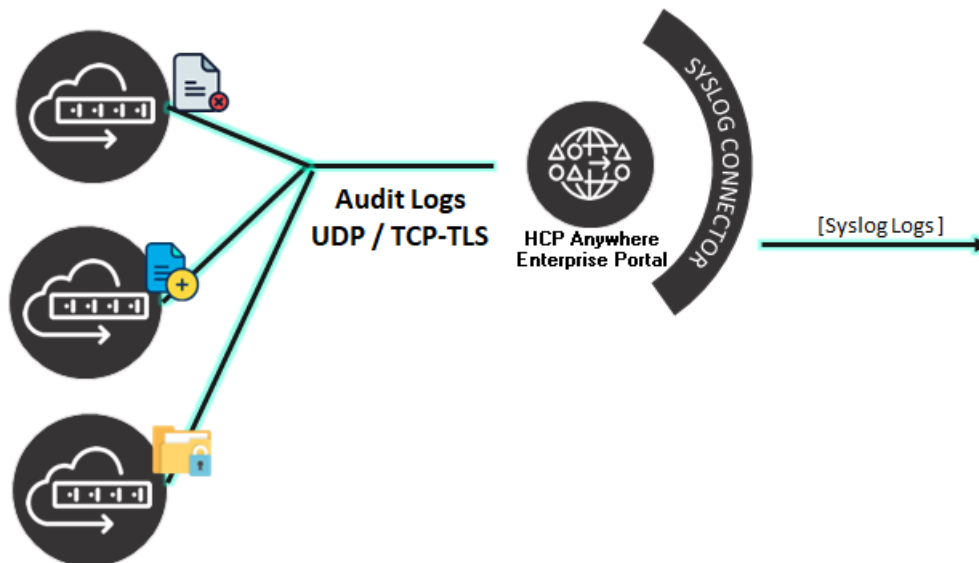
**Note:** Free syslog servers are available, such as Kiwi Syslog Daemon:  
<http://www.kiwisyslog.com/>.

## Configuring Syslog Settings

You can configure syslog logging only for this edge file, or, using the HCP Anywhere Enterprise Portal *Edge Filer Syslog* service, HCP Anywhere Enterprise Portal can function as a centralized hub to collect logs from all the edge filers and send these logs to one or more syslog servers.

The protocol used to send logs from a HCP Anywhere Enterprise Edge Filer to the HCP Anywhere Enterprise Portal uses a protocol that ensures messages are not lost. By using the *Edge Filer Syslog* service:

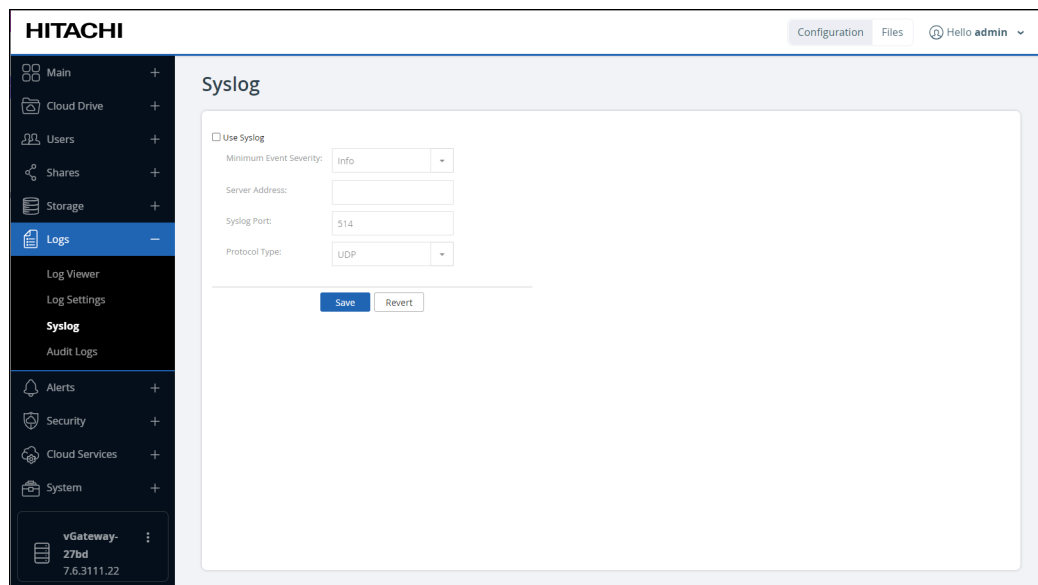
- You can manage multiple HCP Anywhere Enterprise Edge Filer logs to Syslog.
- You ensure that logs are never lost. For example, when a HCP Anywhere Enterprise Edge Filer connects directly to Syslog, if the WAN connection goes down to a Syslog server in the cloud, logs will be lost. Using the Edge Filer Syslog server, the logs are not lost, and when the WAN connection is re-established, sending logs resumes with no loss.
- You can use multiple Syslog destinations by defining more than one Syslog server.



For details, see *Managing the Edge Filer Syslog Service* in the *Hitachi Content Platform Anywhere Enterprise Portal Global Administration Guide*.

**To configure syslog logging only for this HCP Anywhere Enterprise Edge Filer:**

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



2. Select the **Use Syslog** option to enable syslog logging.
3. Configure the syslog:
  - Minimum Event Severity** – The minimum event level to send to the Syslog server. For example, if you select **Critical**, then only **Critical**, **Alert**, and **Emergency** log entries are sent to the syslog server.
  - Server Address** – The syslog server's IP address.
  - Syslog 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 Type** – The protocol to use for sending logs to the syslog server: **UDP** or **TCP/TLS**.
4. Click **Save**.

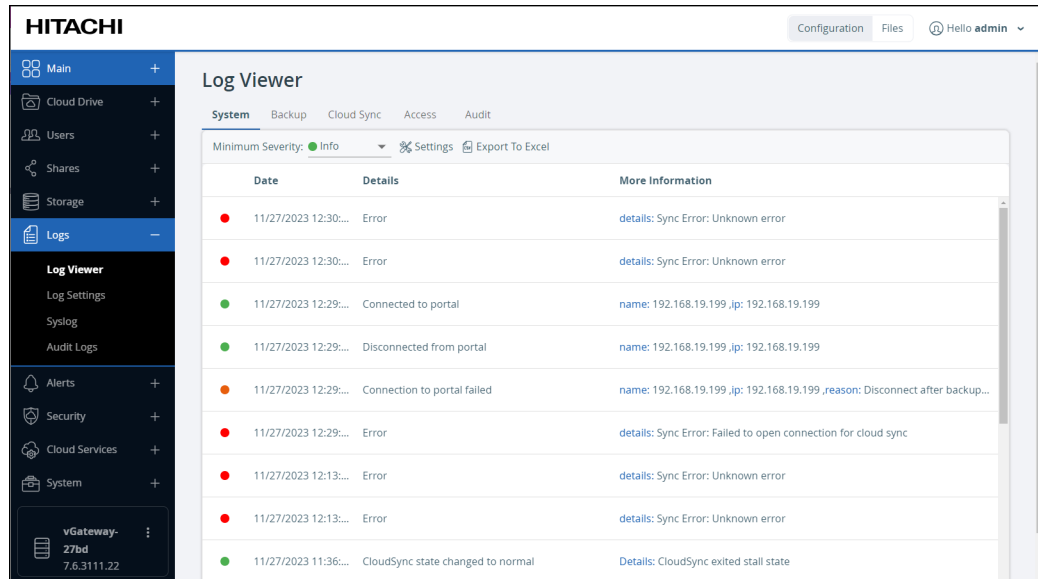
## Configuring Audit Log Settings

See [Auditing SMB File Access](#).

# Viewing Different Types of Logs

## To view different types of logs:

1. In the **Configuration** view, select **Logs > Log Viewer** in the navigation pane. The **Log Viewer** page is displayed.



2. Select the type of log you want to view:
  - System** – General HCP Anywhere Enterprise Edge Filer events, including starting up, connecting to the network and the HCP Anywhere Enterprise Portal, disconnecting from the network and the HCP Anywhere Enterprise Portal, and antivirus events.
  - Backup** – For future use.
  - Cloud Sync** – Events related to cloud drive synchronization operations.
  - Access** – Events related to user access to the HCP Anywhere Enterprise Edge Filer.
  - Audit** – Changes to the HCP Anywhere Enterprise Edge Filer configuration.
3. Optionally, change the minimum severity that is displayed. Ordered from most severe to least severe:
  - Red** – Error
  - Orange** – Warning
  - Green** – Info

## System Log

The System log displays the following details:

An icon indicating whether the event was successful (a green icon) or not (a red icon) or a warning (an orange icon).

**Date** – The date and time at which the event occurred.

**Details** – A description of the event

**More Information** – Additional information about the event.

## Cloud Sync Log

The Cloud Sync log displays the following details:

An icon indicating whether the event was successful (a green icon) or not (a red icon) or a warning (an orange icon).

**File Name** – The name of the file and the folder it is in, transferred during the synchronization operation.

**Operation** – The synchronization operation performed and the direction: inbound or outbound.

**Start Time** – The date and time at which the synchronization operation started.

**Duration** – The amount of time the synchronization operation took.

**Size** – The size of the synchronized file and the percentage saved.

**Result** – The result of the synchronization operation, such as the file was renamed.

**More Information** – Additional information about the event.

## Access Log

The Access log displays the following details:

An icon indicating whether the event was successful (a green icon) or not (a red icon) or a warning (an orange icon).

**Date** – The date and time at which the event occurred.

**User** – The user who triggered the event.

**Protocol** – The protocol used when triggering the event.

**Details** – A description of the event.

**Client Address** – The IP address from which the user triggered the event.

**More Information** – Additional information about the event.

## Audit Log

The Audit log displays the following details for the HCP Anywhere Enterprise Edge Filer:

**Action** – The action type.

**Date** – The date and time at which the event occurred.

**User** – The user who performed the action.

**Type** – The type of setting that was affected by the action. For example, if user `JohnS` was deleted, this column displays `Users`.

**Target** – The object that was affected by the action. For example, if user `JohnS` was deleted, this column displays `JohnS`.

**More Information** – Additional information about the event.

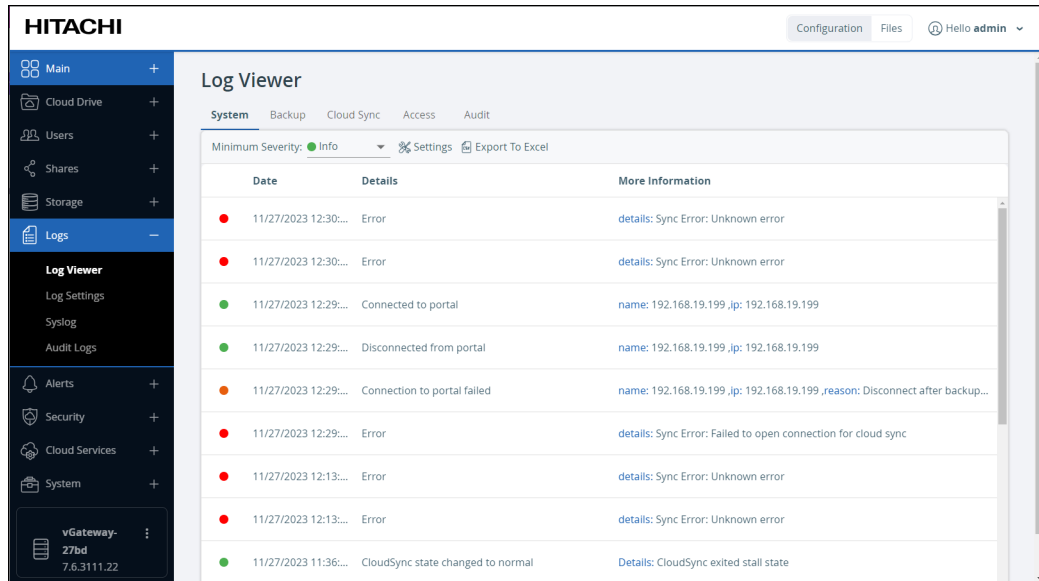
# Filtering Logs

For a log, you can filter the log so that only those with a specific minimum log level are displayed.

**Note:** For information on configuring the default minimum log level to display in all log pages, see [Configuring Logging](#).

## To filter logs:

1. In the **Configuration** view, select **Logs > Log Viewer** in the navigation pane. The **Log Viewer** page is displayed.



2. Select the type of log.
3. Click **Minimum Severity** and select from the list the minimum log level to display.

The logs are filtered accordingly.

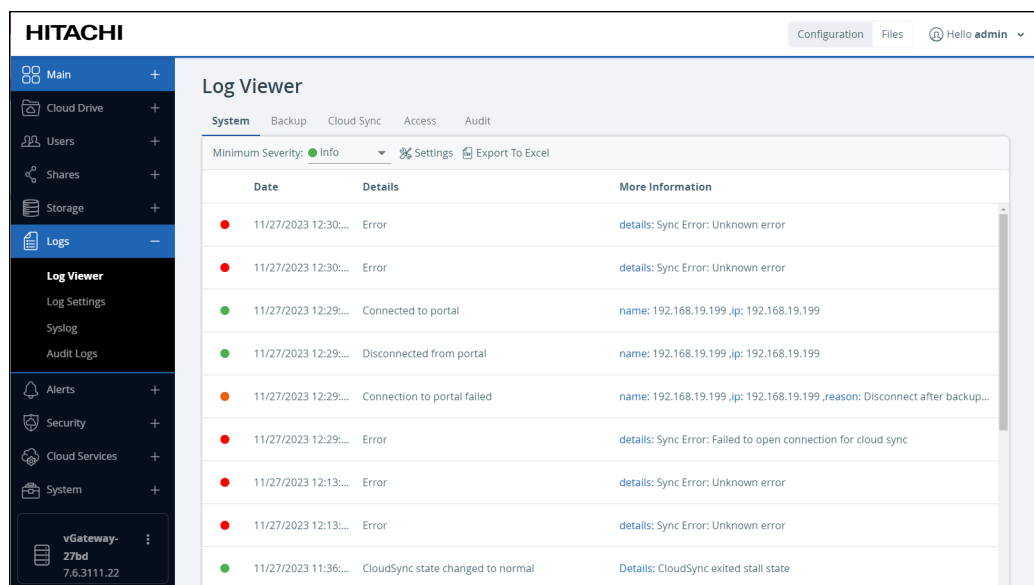
## Exporting Logs

You can export the most recent 10000 log entries to a Comma-Separated Values (CSV) file on your computer. You can then view the file as a worksheet in Microsoft Excel.

**Note:** The export only exports the most recent 10000 log entries.

### To export logs in a log category:

1. In the **Configuration** view, select **Logs > Log Viewer** in the navigation pane. The **Log Viewer** page is displayed.



2. Select the type of log.
3. Click **Export to Excel**.

## Understanding HCP Anywhere Enterprise Log File Entries

HCP Anywhere Enterprise products generate log messages upon various events. The log messages are divided by severity levels.

Level	Required Response
<b>Emergency</b>	System is unusable.
<b>Alert</b>	Action must be taken immediately.
<b>Critical</b>	Critical condition. A situation such as storage nearing full capacity has occurred. Action should be taken as soon as possible.
<b>Error</b>	Error condition. Action must be taken as soon as possible.
<b>Warning</b>	Warning messages. An indication that an error may occur if action is not taken.
<b>Notice</b>	Normal but significant condition.
<b>Info</b>	Informational message.
<b>Debug</b>	Debug-level messages, useful for debugging and troubleshooting.



Within each severity level, the log messages are divided into topics. These topics enable you to understand the source of the message. For example, messages dealing with signing-in are included in the access topic.

Log messages are divided into one of the following topics:

- access
- accounting
- allTopics
- antivirus
- audit
- cloudsync
- files
- sync
- system

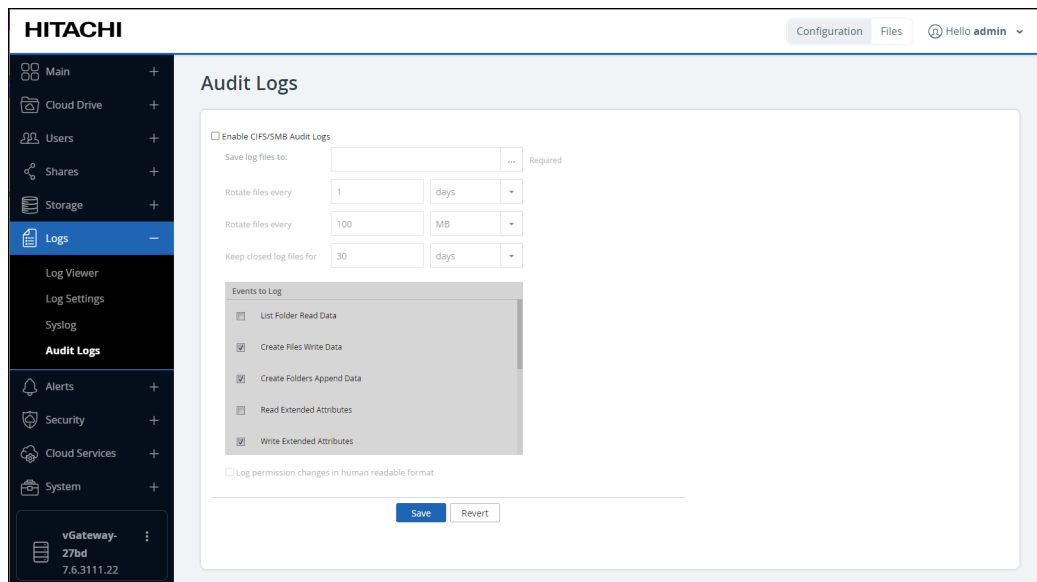
## Auditing SMB File Access

The HCP Anywhere Enterprise Edge Filer provides audit logs of the SMB file access operations performed on the HCP Anywhere Enterprise Edge Filer. This enables organizations to ensure compliance with internal policies and regulations.

**Note:** The SMB audit log does not record sync operations between the HCP Anywhere Enterprise Edge Filer and a HCP Anywhere Enterprise Portal.

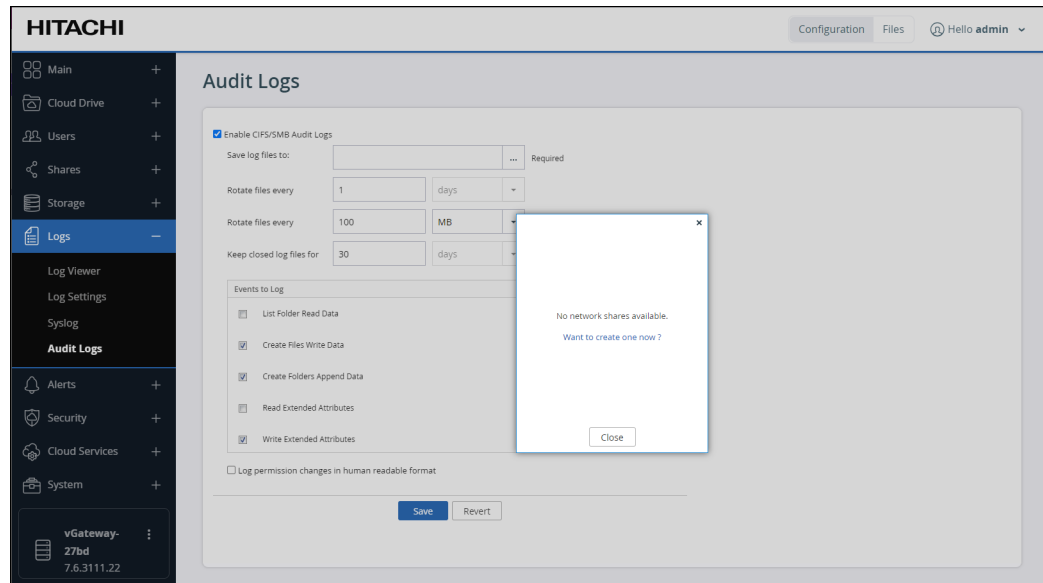
### To enable SMB audit logs:

1. In the **Configuration** view, select **Log Viewer > Audit Logs** in the navigation pane. The **Audit Logs** page is displayed.



2. Select the **Enable CIFS/SMB Audit Logs** option.

3. In the **Save log files to** field, click . . .
  - If you have created network shares, the following window is displayed, listing the network shares.  
Select the network share for the destination to save the log files.  
Click **Close** if you want to create a different network share for the audit logs and then create the network share, as described in [Managing Network Shares](#).
  - If you have not created a network share, the following window is displayed.



- a) To create a network share to use as the destination for the audit logs, click the **Want to create one now?** link.  
The **Select a Folder to Share** wizard opens, displaying the volumes and folders on the HCP Anywhere Enterprise Edge Filer.
- b) Follow the wizard to define the network share, as described in [Managing Network Shares](#).  
The network share is selected as the destination to save the log files.  
Click **Close** if you do not want to create a network share for the audit logs.  
The audit log will be saved to `/network_share/audit.log.dir/audit.log`.

4. Optionally, change the logging details as desired.

**Rotate files every** (time limit) – How often to rollover the log files. You can define the rotation time in minutes, hours or days.

**Rotate files every** (size limit) – When to rollover the log files if they grow large. You can define the rotate size in KB, MB, or GB.

**Keep closed files for** – The number of days to keep closed log files.

A background task is run every 10 minutes and checks these values. For example, if the time to rotate the file has passed or if the size is over the specified size the log file is rotated. Note that this can mean that the file can be larger than the specified value as it will grow until the 10-minute check is performed.

The task also checks if closed log files have exceeded the specified time and any closed log file that has exceeded this time is deleted.

**Note:** If closed log files have exceeded the time specified in **Keep closed files for** and are deleted, and these deleted log files were not sent to the portal, the information in these deleted log files is lost. An example of when this might happen is when the connection to the portal is down for a long time.

This should never normally happen if the default for **Keep closed files for** is not set to too short a time.

- In the **Events to log** area, optionally change the events to log, based on your organization's needs. To add or delete events to log, scroll through the list and select or clear the appropriate check boxes. The events you can log are:

Flag in User Interface	Meaning
List Folder Read Data	Log when data is read from a file.
Create Files Write Data	Log when data is written or appended to a file.
Create Folders Append Data	Log when a directory is created.
Read Extended Attributes	Log when an extended attribute is fetched.
Write Extended Attributes	Log when an extended attribute is replaced or a new extended attribute is created.
Traverse Folder Execute File	Log an attempt to open a file.
Delete Subfolders and Files	—
Write Attributes	Log when the file attributes, such as the system and hidden attributes, are changed.
Delete	Log when a file or directory is deleted.
Change Permissions	Log any change to a file or directory access permission.
Change Owner	Log when the owner of a file or directory is modified.

- Optionally, check Log permission changes in human readable format, for changes in ACL permissions to files and folders to be reported in the audit log in an understandable format. Where:

ace-type indicates the type of ACE (allow/deny)

ace-rights indicates the type of permissions/AccessMask

ace-flags indicates the ACE behavior

**Warning: Setting the log to be readable degrades performance. Hitachi Vantara recommends not setting this option, unless you really need it.**

- Click **Save**.

HCP Anywhere Enterprise Edge Filer generates audit log messages upon various operations.

## Example Log Entries

open

```
July 30 08:33:42 2022EdgeFiler smbd:
|2022EdgeFiler|hcp_audit|fs|ok|0x00000000|user=2022EDGEFILER\admin|sid=S
-1-5-21-2761415951-3033486807-2004858877-
1402|op=open|timestamp=1609310022|local_time=1609302822|rootPath=/var/vol
1/syncgateway/ cloudshare|share=cloud|path=users/portal admin/My
Files/Photos/CopiedFile -
Copy.png|access=01101001100000000100100000000000|remote
hostname=10.212.134.55||
```

## OpenDenied

```
July 30 08:34:06 2022EdgeFiler smbd:  
|2022EdgeFiler|hcp_audit|fs|fail|0xc0000034|user=2022EDGEFILER\admin|sid=S-1-5-21-  
2761415951-3033486807-2004858877-1402|op=OpenDenied|timestamp=1609310046  
|local_time=1609302846|rootPath=/var/vol/syncgateway/cloudshare|share=cloud|path=users/portal admin/My  
Files/Photos/E0EAEC4D.tmp|access=00000100000000000000000000000000|remote  
hostname=10.212.134.55|isDir=1||
```

## read

```
July 30 08:33:41 2022EdgeFiler smbd:  
|2022EdgeFiler|hcp_audit|fs|ok|0x00000000|user=2022EDGEFILER\admin|sid=S-1-5-21-  
2761415951-3033486807-2004858877-1402|op=read|timestamp=1609310021|local_time=1609302821|rootPath=/var/vol/syncgateway/cloudshare|share=cloud|path=users/portal admin/My  
Files/Photos/CopiedFile - Copy.png|type=file|remote  
hostname=10.212.134.55|fileSize=148071|dataRW=4096||
```

## write

```
July 30 08:33:51 2022EdgeFiler smbd:  
|2022EdgeFiler|hcp_audit|fs|ok|0x00000000|user=2022EDGEFILER\admin|sid=S-1-5-21-  
2761415951-3033486807-2004858877-1402|op=write|timestamp=1609310031|local_time=1609302831|rootPath=/var/vol/syncgateway/cloudshare|share=cloud|path=users/portal admin/My Files/Photos/~$w Microsoft Word  
Document1.docx|type=file|remote  
hostname=10.212.134.55|fileSize=54|dataRW=113||
```

## move

```
July 30 08:34:06 2022EdgeFiler smbd:  
|2022EdgeFiler|hcp_audit|fs|ok|0x00000000|user=2022EDGEFILER\admin|sid=S-1-5-21-  
2761415951-3033486807-2004858877-1402|op=move|timestamp=1609310046|local_time=1609302846|rootPath=/var/vol/syncgateway/cloudshare|share=cloud|source path=users/portal admin/My  
Files/Photos/New Microsoft Word Document1.docx|destination  
path=users/portal admin/My Files/Photos/E0EAEC4D.tmp|type=file|remote  
hostname=10.212.134.55||
```

## create

```
July 30 08:33:51 2022EdgeFiler smbd:  
|2022EdgeFiler|hcp_audit|fs|ok|0x00000000|user=2022EDGEFILER\admin|sid=S-1-5-21-  
2761415951-3033486807-2004858877-1402|op=create|timestamp=1609310031|loc
```

```
al_time=1609302831|rootPath=/var/vol/syncgatewa  
y/cloudshare|share=cloud|path=users/portal admin/My Files/Photos/~$w  
Microsoft Word Document1.docx|type=file|remote hostname=10.212.134.55||
```

## delete

### fail operation

```
July 30 08:33:42 2022EdgeFiler smbd:  
|2022EdgeFiler|hcp_audit|fs|fail|0xc0000034|user=2022EDGEFILER\admin|sid  
=S-1-5-21-  
2761415951-3033486807-2004858877-1402|op=delete|timestamp=1609310022|loc  
al_time=1609302822|rootPath=/var/vol/syncgatewa  
y/cloudshare|share=cloud|path=users/portal admin/My  
Files/Photos/._CopiedFile - Copy.png|type=file|remote  
hostname=10.212.134.55|fileSize=10000|dataRW=18446744073709551615||
```

### ok operation

```
July 30 08:33:42 2022EdgeFiler smbd:  
|2022EdgeFiler|hcp_audit|fs|ok|0x00000000|user=2022EDGEFILER\admin|sid=S  
-1-5-21-  
2761415951-3033486807-2004858877-1402|op=delete|timestamp=1609310022|loc  
al_time=1609302822|rootPath=/var/vol/syncgatewa  
y/cloudshare|share=cloud|path=users/portal admin/My  
Files/Photos/CopiedFile - Copy.png|type=file|remote  
hostname=10.212.134.55|fileSize=10000|dataRW=18446744073709551615||
```

## setattrib

```
July 30 08:33:42 2022EdgeFiler smbd:  
|2022EdgeFiler|hcp_audit|fs|ok|0x00000000|user=2022EDGEFILER\admin|sid=S  
-1-5-21-  
2761415951-3033486807-2004858877-1402|op=setattrib|timestamp=1609310022|  
local_time=1609302822|rootPath=/var/vol/syncgat  
eway/cloudshare|share=cloud|path=users/portal admin/My  
Files/Photos/CopiedFile -
```

## getea

```
July 29 10:30:47 2022EdgeFiler smbd:  
|2022EdgeFiler|hcp_audit|fs|fail|0xc0000225|user=2022EDGEFILER\admin|sid  
=S-1-5-21-  
2761415951-3033486807-2004858877-1402|op=getea|timestamp=1609230647|loca  
l_time=1609223447|rootPath=/var/vol/syncgateway/cloudshare|share=cloud|p  
ath=/var/vol/syncgateway/cloudshare|att=org.netatalk.Metadata|remote  
hostname=10.212.134.70||
```

Each field in the message is separated by the | character. The fields in the examples have the following meaning:

**Timestamp and edge filer name** – Each line in the audit log starts with the timestamp when it was written to the log and the edge filer connected to. For example, July 30 08:33:42

2022EdgeFiler smbd:

**Edge filer name** – The name of the device on which the operation was executed. For example, 2022EdgeFiler

**Log name** – The name of the audit log: hcp\_audit.

**Type** – The audit type.

**Operation result** – The result, either **ok** or **fail**.

**Operation result code** – The result code for the operation. 0xc0000000 for ok. fail is 0xc0000225.

**User name** – The name of the user who executed the operation. For example, user=2022EDGEFILER\admin

**User SID** – The security identifier. For example, sid=S-1-5-21-2278938113-1352723297-1199027263-1402

**Operation** – The operation that was executed. For example, op=open

**Timestamp** – The UTC time the operation was executed. For example, timestamp=1609230647

**Local time** – The local time the operation was executed. For example, local\_time=1609223447

**Root Path** – The root path for the share. For example, rootPath=/var/vol/syncgateway/cloudshare|share=cloud

**Share** – The name of the share. For example, share=cloud

**Path** – The path to a file being handled. For example, path=users/portal admin/My Files/Photos/New Microsoft Word Document1.docx

**Destination** – The destination for a move or copy operation. For example, destination path=users/portal admin/My Files/Photos/E0EAEC4D.tmp

**Type** – Whether the operation is on a folder or file.

**Attributes** – The attributes, either in readable format, for example, att=org.netatalk.Metadata or machine readable, for example, dosattrib=0000dosattrib=0000

**Access code** – The access code. For example, access=00000100000000000000000000000000

**Remote hostname** – The IP address of the device connected using SMB to the HCP Anywhere Enterprise Edge Filer. For example, remote hostname=10.212.134.70

**File size** – The size of the file being operated on. For example, Size=18446744073709551615

**Data Read/Write** – For example, dataRW=18446744073709551615

**Directory** – Whether the operation is on a directory or not. For example, isDir=1

The operations have the following meanings:

Operation in Log	Description	Flag in User Interface
read, OpenDenied	Open a file for reading	List Folder Read Data
create, write, createDenied, OpenDenied, move	Create or write to a file Create Files	Write Data
create, createDenied, OpenDenied	Create a folder	Create Folders Append Data
getea	Get the extended attributes	Read Extended Attributes
setea	Set the extended attributes	Write Extended Attributes
delea	Delete an extended attribute	Write Extended Attributes

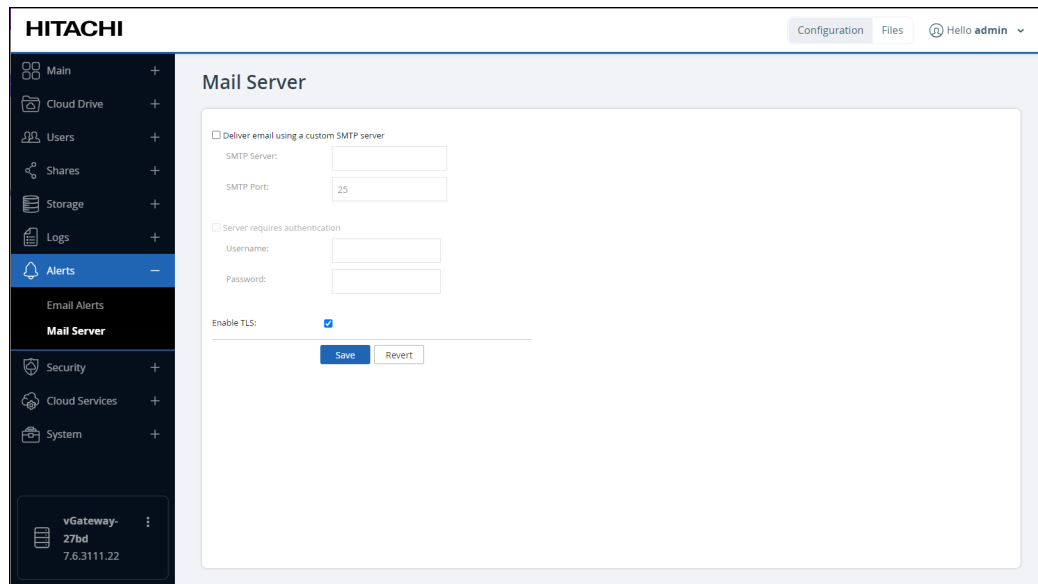
<b>Operation in Log</b>	<b>Description</b>	<b>Flag in User Interface</b>
<b>open</b>	Open a file	Traverse Folder
<b>delete, move</b>	Delete a file or folder	Delete
<b>getattrib</b>	Get the attributes	—
<b>setattrib</b>	Set the attributes	Write Attributes
<b>ACEChanged</b>	Change permissions	Change Permissions
<b>ACLAdded, ACLDeleted, ACLProtectionAdded, ACLProtectionDeleted</b>	Change access permissions	Change Permissions
<b>setdacl</b>	Set permissions	Change Permissions
<b>getsd</b>	The security descriptor of a file or directory is fetched	—
<b>setsd, AcIDenied</b>	The security descriptor of a file or directory is set	Change Permissions
<b>chown, AcIDenied</b>	Change the owner	Change Owner
<b>deleteDenied</b>	Don't allow deleting a file or folder	Delete Subfolders and Files

# Chapter 11. Configuring Email Alerts

You can configure the HCP Anywhere Enterprise Edge Filer to send alerts upon important events. The alerts can be sent to up to two email addresses.

## To configure the HCP Anywhere Enterprise Edge Filer to send email alerts:

1. In the **Configuration** view, select **Alerts > Mail Server** in the navigation pane. The **Mail Server** page is displayed.



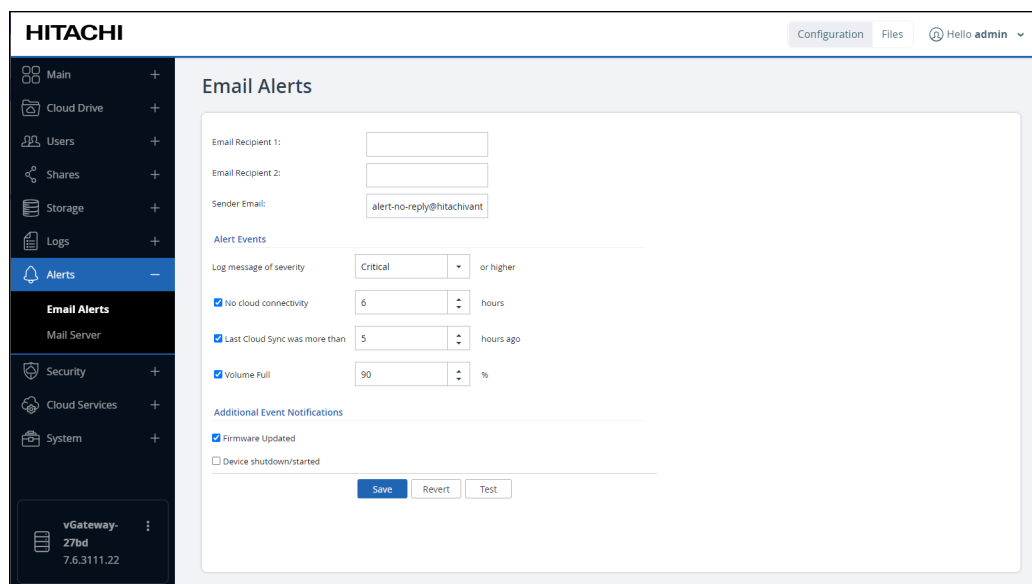
The screenshot shows the HITACHI web interface. The top navigation bar includes 'Configuration', 'Files', and 'Hello admin'. The left sidebar contains a navigation menu with options: Main, Cloud Drive, Users, Shares, Storage, Logs, Alerts (selected), Email Alerts, Mail Server (selected), Security, Cloud Services, and System. The main content area is titled 'Mail Server' and contains the following configuration options:

- Deliver email using a custom SMTP server
  - SMTP Server: [text input]
  - SMTP Port: [text input with value 25]
- Server requires authentication
  - Username: [text input]
  - Password: [text input]
- Enable TLS:

At the bottom of the form are 'Save' and 'Revert' buttons.

2. Configure the settings according to the requirements:
  - Deliver email using a custom SMTP server** – Enable email alerts.
    - **SMTP Server** – The SMTP server's IP address.
    - **SMTP Port** – The SMTP server's port number. The default is 25.
  - Server requires authentication** – The SMTP server requires authentication.
    - **Username** – The user name when authenticating to the SMTP server.
    - **Password** – The password for the user.
  - Enable TLS** – Use Transport Layer Security (TLS) encryption for sending email messages from the HCP Anywhere Enterprise Edge Filer.
3. Click **Save**.
4. In the **Configuration** view, select **Alerts > Email Alerts** in the navigation pane. The **Email Alerts** page is displayed.





5. Configure the settings according to the requirements:

**Email Recipient 1** – An email address to which email alerts are sent.

**Email Recipient 2** – A second email address to which email alerts are sent.

**Sender Email** – The email address for the From field of email alerts.

**Log message of severity** – The minimum event severity level for which to send email alerts. For example, if you select **Critical**, then only **Critical**, **Alert**, and **Emergency** logs are sent to the email recipients.

Select each type of alert event for which you want emails to be sent:

- **No cloud connectivity** – When there is no cloud connectivity for more than the specified number of hours.
- **Last Cloud Sync was more than** – When the last cloud synchronization operation was performed more than the specified number of hours ago.

Select each type of additional event for which you want emails to be sent:

- **Firmware Updated** – When the HCP Anywhere Enterprise Edge Filer firmware has been updated.
- **Device shutdown/started** – When the HCP Anywhere Enterprise Edge Filer starts up and shuts down.

6. Click **Revert**, if you made changes that were not saved, to revert to display the saved values.

7. Click **Save**.

8. To test the configuration, click **Test**.

A test email is sent to the specified email addresses.

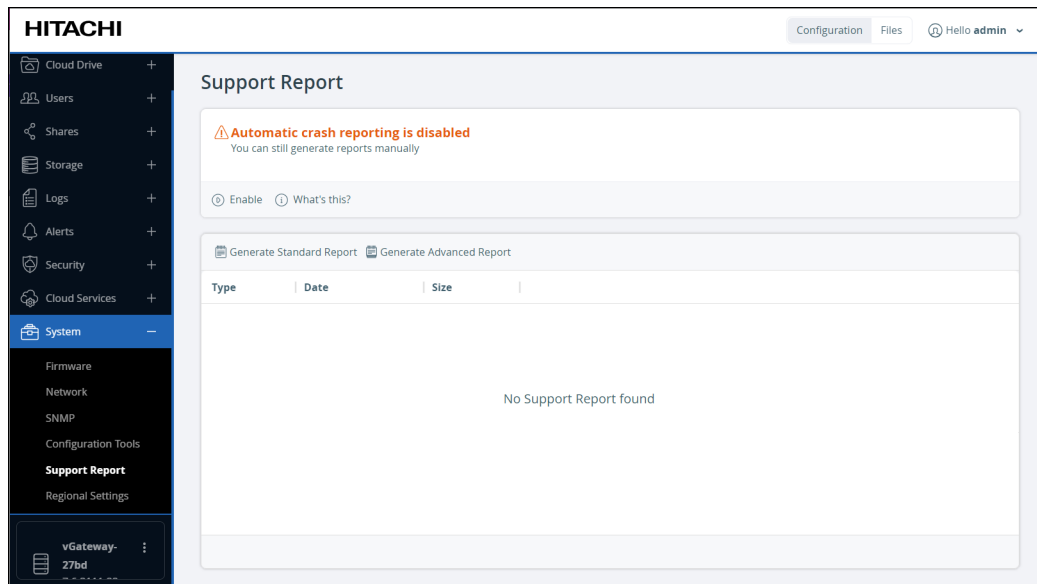
## Configuring Email Alerts

# Chapter 12. Generating a Support Report

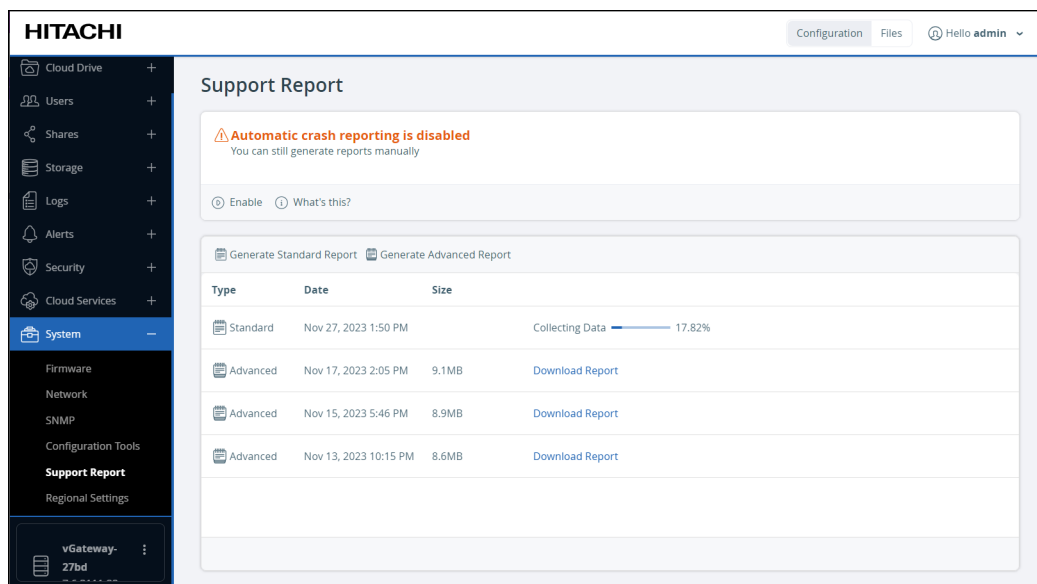
If a problem arises with the HCP Anywhere Enterprise Edge Filer, you can generate a report for Hitachi Vantara support to use to identify and resolve the problem.

## To generate a support report:

1. In the **Configuration** view, select **System > Support Report** in the navigation pane. The **Support Report** page is displayed.



2. Click either **Generate Standard Report** or **Generate Advanced Report**. The report is generated displaying the type of report. **Standard** or **Advanced**, and with the status, for example **Collecting Data**. On completion the status is **Download Report**.



3. Click **Download Report** to download the report to the local PC.

Send the report to Hitachi Vantara support.

## Automatically Sending Crash Reports to Support

If an edge filer crash occurs, you can have the edge filer automatically send a report to Hitachi Vantara support so that analysis of the crash can begin as early as possible.

Crash reports do not include sensitive or personal information. The reports are sent encrypted. The only identifying content in the crash report is the DNS name.

Click **Enable** to have the HCP Anywhere Enterprise Edge Filer automatically upload crash reports to the Hitachi Vantara support center in the event of a crash.

Click **Disable** if you no longer need to use this service after you enabled it.

# Chapter 13. Maintaining a HCP Anywhere Enterprise Edge Filer

## Upgrading the Edge Filer

You can configure the HCP Anywhere Enterprise Edge Filer to automatically download firmware updates from the HCP Anywhere Enterprise Portal it is connected to and install this download. Alternatively, you can install firmware updates manually.

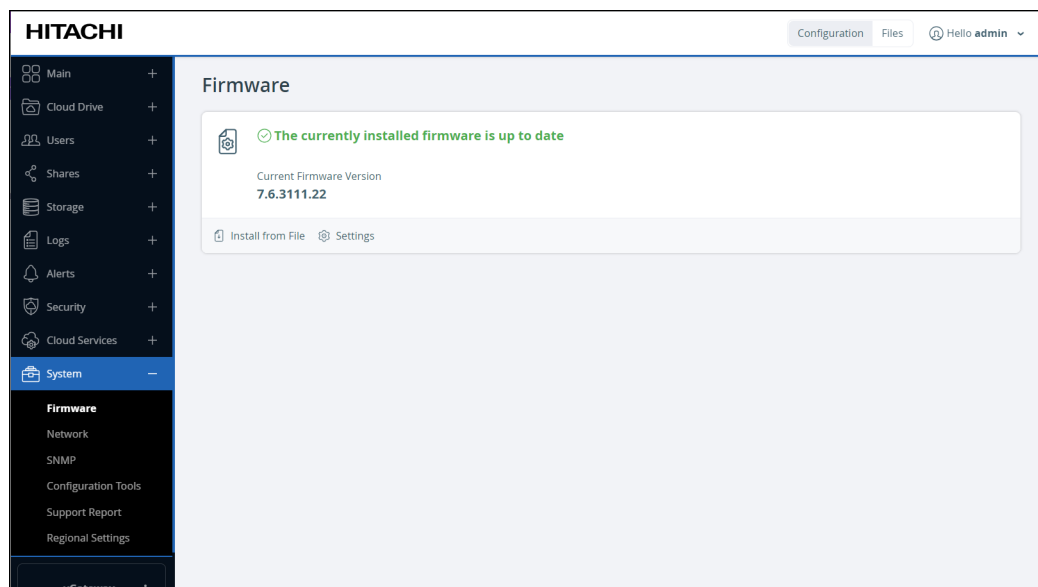
**Note:** The recommended method to update the HCP Anywhere Enterprise Edge Filer firmware is by pushing new firmware from the HCP Anywhere Enterprise Portal. For details refer to the HCP Anywhere Enterprise Portal documentation.

After an upgrade, the previous version is saved. When starting up the HCP Anywhere Enterprise Edge Filer the new version is selected and after a couple of seconds, it is started. If you need to revert to the previous version, during the startup, when both versions are displayed, select the previous version.

## Configuring Automatic Firmware Updates

**To configure automatic firmware updates:**

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



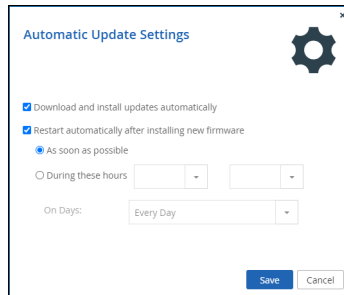
The following information can be displayed:

- Whether the current firmware is the latest version or not.
- The available newer version if there is one.
- The most recent available firmware version from the HCP Anywhere Enterprise Portal firmware repository.
- The progress of an upgrade. This information is displayed if firmware has been

downloaded, and Download and install updates automatically has been set in the **Automatic Update Settings** window.

2. Click Settings.

The **Automatic Update Settings** window is displayed.



3. To specify that the HCP Anywhere Enterprise Edge Filer should download and install firmware updates automatically, click **Download and install updates automatically**.

If you do not select this option, you must perform firmware updates manually, as described in [Manually Upgrading the Firmware](#).

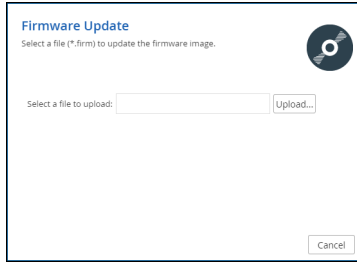
4. To specify that the HCP Anywhere Enterprise Edge Filer should automatically reboot after installing new firmware updates, do the following:
  - a) Click **Restart automatically after installing new firmware**.
  - b) Specify when automatic rebooting should occur, by doing one of the following:

To reboot as soon as possible after a firmware update, choose **As soon as possible**. In this case, the HCP Anywhere Enterprise Edge Filer will reboot as soon as it is recommended to do so. For example, the automatic reboot might be deferred, if the HCP Anywhere Enterprise Edge Filer is undergoing system maintenance that should not be interrupted.

To reboot only during specific hours, choose **During these hours**, then use the drop-down lists to specify the desired time range. If you do not enable automatic rebooting, then you will need to reboot the HCP Anywhere Enterprise Edge Filer as described in [Restarting the HCP Anywhere Enterprise Edge Filer](#), when this page indicates that a new update has been installed.
5. Click Save.

## Manually Upgrading the Firmware

1. In the **Configuration** view, select **System > Firmware** in the navigation pane. The **Firmware** page is displayed, showing the currently installed firmware version.
2. Either,
  - a) Click **Install from Portal** to install the latest version from the HCP Anywhere Enterprise Portal. **Install from Portal** is only available if the portal repository includes firmware to use.
  - b) Click **Yes**.Or,
  - a) Click **Install from File**. The **Firmware Update** window is displayed.



- b) Click **Upload** and browse to the required firmware (\*.firm) file.

The firmware file is uploaded. A progress bar displays the percentage upload.

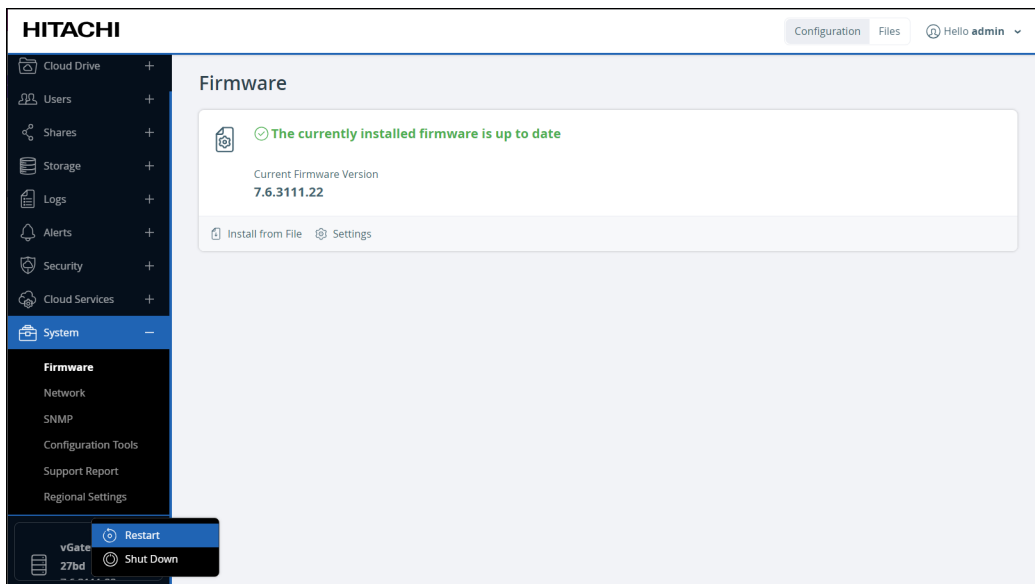
On completion, the HCP Anywhere Enterprise Edge Filer automatically reboots after a few minutes. The page displays the current firmware version until after the reboot, the new firmware version after the reboot, and the time until the reboot starts automatically.

## Restarting the HCP Anywhere Enterprise Edge Filer

If you are experiencing problems with the HCP Anywhere Enterprise Edge Filer, restarting it may solve the problems.

### To restart the HCP Anywhere Enterprise Edge Filer via the user interface:

1. At the bottom of the navigation pane, next to the HCP Anywhere Enterprise Edge Filer name, click the three dots menu and then click **Restart**.



A confirmation message is displayed.

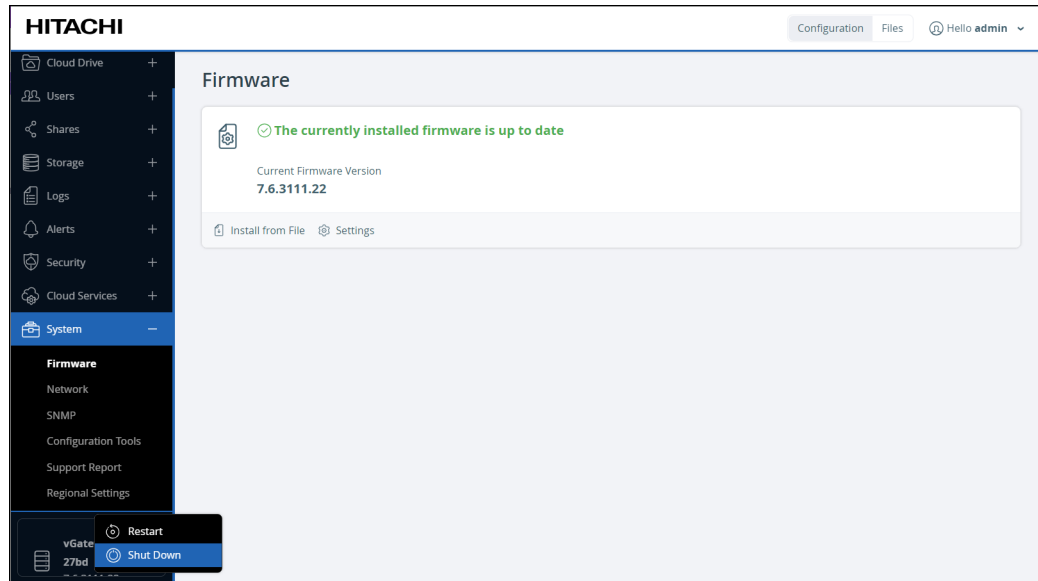
2. Click **Reboot**.

The HCP Anywhere Enterprise Edge Filer restarts.

# Shutting Down the HCP Anywhere Enterprise Edge Filer

**To shut down a HCP Anywhere Enterprise Edge Filer via the user interface:**

1. At the bottom of the navigation pane, next to the HCP Anywhere Enterprise Edge Filer name, click the three dots menu and then click **Shut Down**.



A confirmation message is displayed.

2. Click **Shut Down**.

The HCP Anywhere Enterprise Edge Filer shuts down.

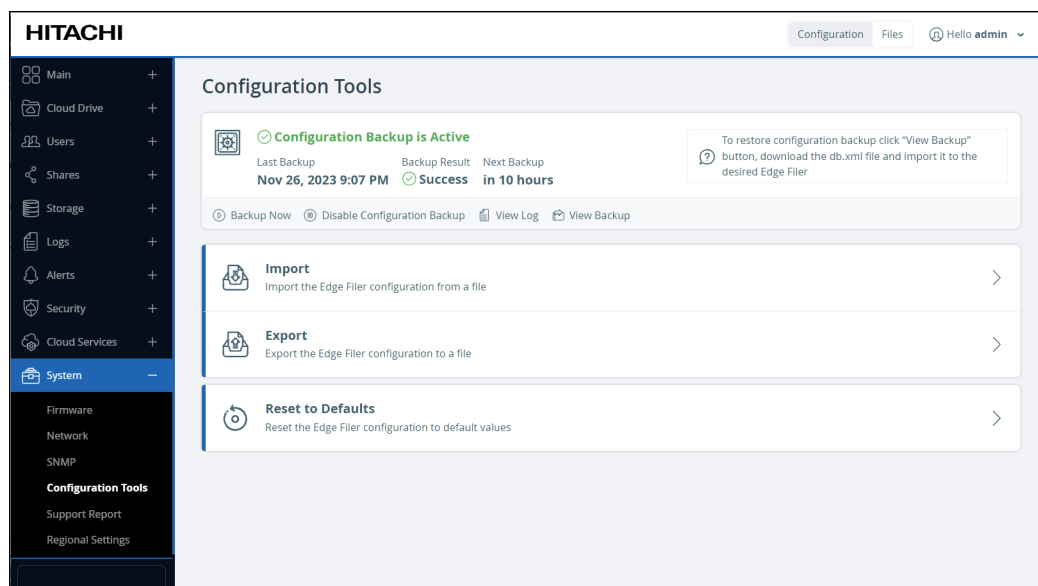
# Resetting a HCP Anywhere Enterprise Edge Filer to its Default Settings

You can reset the HCP Anywhere Enterprise Edge Filer to its factory default settings. This action does not reset the version, which is taken from the HCP Anywhere Enterprise Portal.

**Warning:** This action erases all of your passwords and settings, and you will need to reconfigure the HCP Anywhere Enterprise Edge Filer. To reconfigure, run the setup wizard, described in *Initial HCP Anywhere Enterprise Edge Filer Setup*, in the installation guide.

To reset the HCP Anywhere Enterprise Edge Filer to its default settings via the user interface:

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



2. Click **Reset to Defaults**.  
A confirmation message is displayed.
3. Click **Yes**.

The HCP Anywhere Enterprise Edge Filer is reset to its default settings, and the initial Login page is displayed.

To reconfigure the HCP Anywhere Enterprise Edge Filer, run the setup wizard, described in the *Initial HCP Anywhere Enterprise Edge Filer Setup*, in the installation guide.

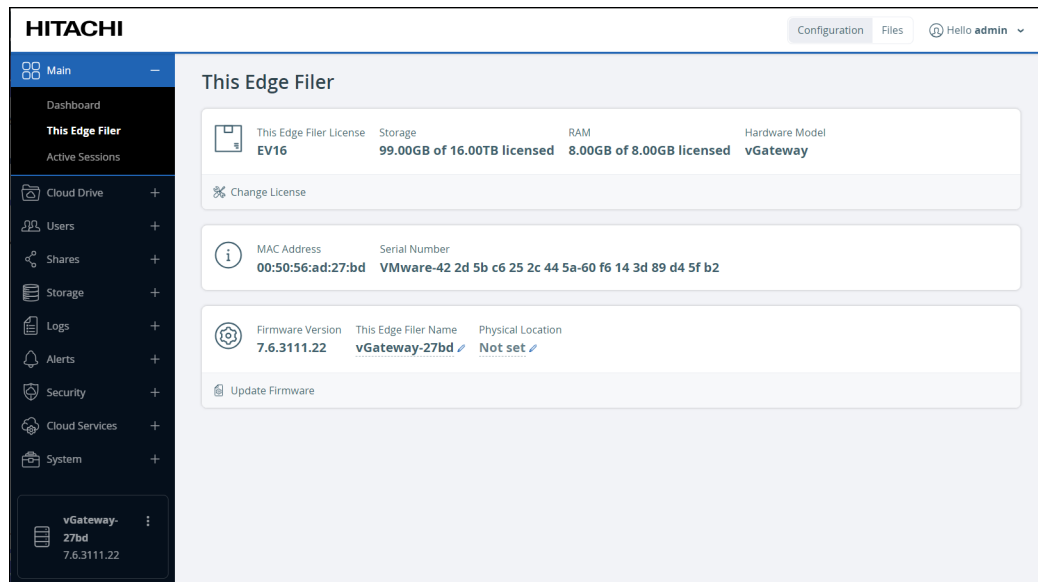


# Changing the HCP Anywhere Enterprise Edge Filer License

A HCP Anywhere Enterprise Edge Filer requires a license to operate, which it receives from HCP Anywhere Enterprise Portal. You can change the license to another license that is available in your HCP Anywhere Enterprise Portal account.

## To change the HCP Anywhere Enterprise Edge Filer license:

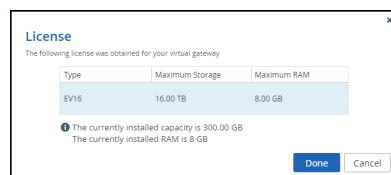
1. In the **Configuration** view, select **Main > This Edge Filer** in the navigation pane. The **This Edge Filer** page opens, displaying the HCP Anywhere Enterprise Edge Filer details.



2. In the license area click **Change License**.

The **Select License** window is displayed.

**Note:** When there is no choice, determined by the licenses available in the HCP Anywhere Enterprise Portal account, the current license is displayed. Click **Done** to exit the procedure.



3. Select the new license and click **Save**.

---


## Chapter 14. macOS: Accessing a HCP Anywhere Enterprise Edge Filer

When using a Mac computer to search for files in a share on the edge filer, you can search for these files using Mac Finder. Enabling file searches requires a file index. After indexing completes, you can search for files even when the HCP Anywhere Enterprise Edge Filer syncing is suspended. For details, see [macOS: Enabling Using Finder to Search in the HCP Anywhere Enterprise Edge Filer](#).

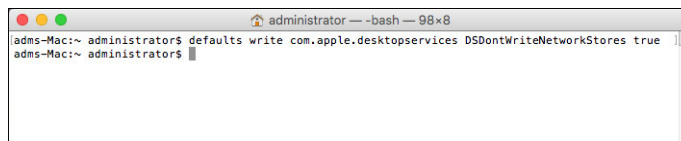
Before connecting a Mac computer to a HCP Anywhere Enterprise Edge Filer configured as a Caching Gateway, you have to configure the Mac computer:

- Hidden .DS\_Store files are not enabled.  
**Note:** Apple uses .DS\_Store files to store the custom attributes of folders. By default, Finder creates a .DS\_Store file in every folder that it accesses. Disabling the .DS\_Store setting is required when connected to the HCP Anywhere Enterprise Edge Filer.
- To display icons in Finder for stub files and folders.

### To configure the Mac computer when connecting to the HCP Anywhere Enterprise Edge Filer:

1. Update the Mac OS X to macOS 10.14 (Mojave) or higher.  
**Note:** You can check the version by right-clicking the Apple icon, , in the right of the menu bar and choosing **About This Mac** to display the version. If required, you can also update the software from this window.  
Hitachi Vantara recommends using either of the latest 2 versions of macOS.
2. Open the **Terminal** application, located under **Applications > Utilities**.
3. Execute the following command:

```
defaults write com.apple.desktopservices DSDontWriteNetworkStores true
```



4. Restart the Mac computer.

## Using HCP Anywhere Enterprise Cache Assist

HCP Anywhere Enterprise provides a macOS Finder extension, HCP Anywhere Enterprise Cache Assist, for enhanced display of cached network share for the purpose of providing a consistent user experience across any desktop and HCP Anywhere Enterprise Edge Filer.

For details about how to install and use HCP Anywhere Enterprise Cache Assist, see *Hitachi Content Platform Anywhere Enterprise Cache Assist*.

## Hitachi Vantara

Corporate Headquarters 2535 Augustine Drive  
Santa Clara, CA 95054 USA [www.HitachiVantara.com](http://www.HitachiVantara.com) [community.HitachiVantara.com](http://community.HitachiVantara.com)

### Regional Contact Information

Americas: +1 866 374 5822 or [info@hitachivantara.com](mailto:info@hitachivantara.com)

Europe, Middle East and Africa: +44 (0) 1753 618000 or [info.emea@hitachivantara.com](mailto:info.emea@hitachivantara.com)

Asia Pacific: +852 3189 7900 or [info.marketing.apac@hitachivantara.com](mailto:info.marketing.apac@hitachivantara.com)

