Hitachi Content Platform Anywhere Enterprise

v7.5 1159.35.1

Portal Release Notes

This document describes features, licensing information, and known issues for the 7.5 1159.35.1 release of HCP Anywhere Enterprise Portal.

RN-HCPAE000-02
November 2023

© 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.

Contents

Preface 4
About this document 4
Document conventions 4
Intended audience 4
Accessing product downloads 4
Getting Help 4

Chapter 1. Hitachi Content Platform Anywhere Enterprise Portal Version 7.5.1159.35.1. 5

LICENSING HCP Anywhere Enterprise PORTAL 5
Installing or Upgrading HCP Anywhere Enterprise Portal 5
Active Directory Running on Windows 2003 5
Upgrading the HCP Anywhere Enterprise Portal 5
Checking the HCP Anywhere Enterprise Portal Cloud File System (FSCK) 6
Major New Features in 7.5.1159.35.1 6
New Storage Node: HCP Hitachi Vantara (S3) 6
Adding a Global Administrator From Active Directory 7
What's New In the Portal Image 14
New Software Features 14
Resolved Software Issues 15
Known Issues 16

Preface

About this document

This book describes the latest release of the HCP Anywhere Enterprise Portal.

Document conventions

This document uses the following typographic convention:

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

Intended audience

This document is intended for HCP Anywhere Enterprise administrators.

Accessing product downloads

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

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

Getting Help

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

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

Chapter 1. Hitachi Content Platform Anywhere Enterprise Portal Version 7.5.1159.35.1

Hitachi Content Platform Anywhere Enterprise Portal 7.5.1159.35.1 requires portal image 7.5.1159.35.1

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

LICENSING HCP Anywhere Enterprise PORTAL

You cannot upgrade to HCP Anywhere Enterprise Portal version 7.5.x without a valid license that has not expired. When the portal license is about to expire, notifications appear in the portal user interface and the administrator can contact Hitachi Vantara for a license renewal. Additionally, emails are sent to the administrator.

Installing or Upgrading HCP Anywhere Enterprise Portal

For installation details, including ports that must be open, refer to the installation guide for your platform.

Active Directory Running on Windows 2003

Support for the weak encryption mode used by Active Directory on Windows Server 2003 is not supported by default. When using HCP Anywhere Enterprise Portal and Active Directory on Windows Server 2003, `set /settings/defaultPortalSettings/activeDirectorySettings/legacyActiveDirectorySupport true`. The default is `false`.

Set true to enable support for the encryption mode used by Active Directory on Windows Server 2003. This setting is false by default.

Upgrading the HCP Anywhere Enterprise Portal

The HCP Anywhere Enterprise Portal image and software on all portal servers can be upgraded as described in *Upgrading a HCP Anywhere Enterprise Portal* in the installation guide for your platform. You must upgrade both the portal image to the latest portal image as well as the portal software. After upgrading the portal image, you must reboot every server in the HCP Anywhere Enterprise Portal environment.

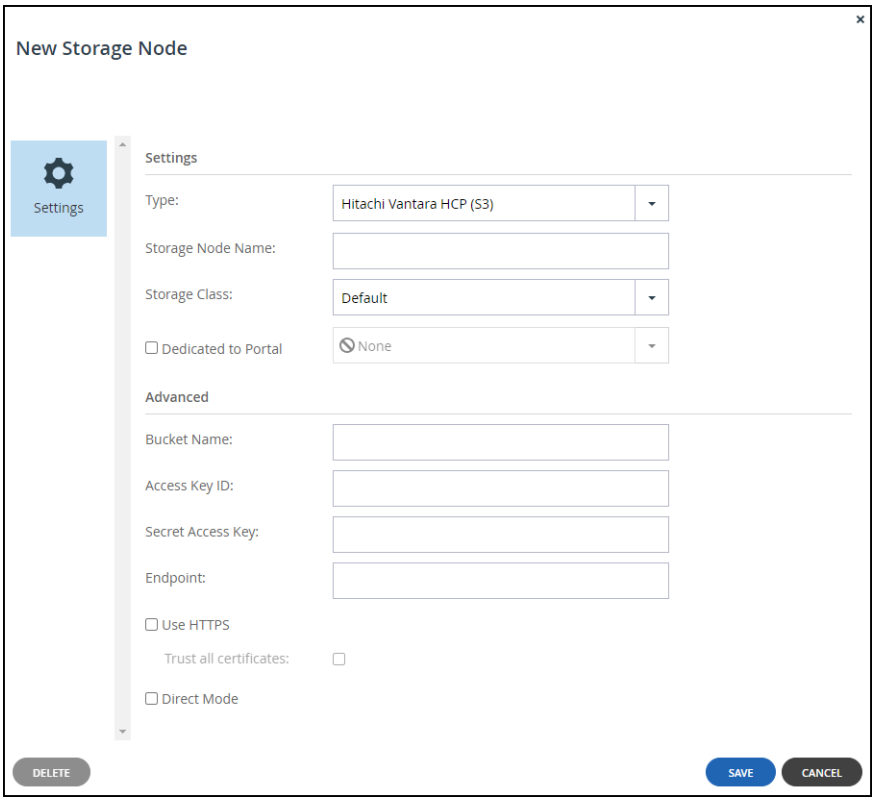
Checking the HCP Anywhere Enterprise Portal Cloud File System (FSCK)

In order to check the consistency between the HCP Anywhere Enterprise Portal database and the actual data in the storage node, HCP Anywhere Enterprise Portal has a utility, FSCK, similar to the Linux FSCK utility. HCP Anywhere Enterprise Portal FSCK **must** be run only with approval from Hitachi Vantara support.

Major New Features in 7.5.1159.35.1

New Storage Node: HCP Hitachi Vantara (S3)

A new storage node is available: HCP Hitachi Vantara (S3). The minimum version of Hitachi Vantara HCP (S3) supported by HCP Anywhere Enterprise Portal is version 9.6.1.3.



The specific fields for HCP Hitachi Vantara (S3):

Bucket Name – A unique name for the S3 bucket that you want to add as a storage node.
Access Key ID – The S3 access key ID.
Secret Access Key – The S3 secret access key.
Endpoint – The endpoint name of the S3 service. The port for the endpoint can be customized by adding the port after the URL, using a colon (:) separator. The default port is 80.
Use HTTPS – Use HTTPS to connect with the storage node.

Trust all certificates – Do not validate the certificate of the object storage. Normally this is unchecked.
Direct Mode – Data is uploaded and downloaded directly to and from the storage node and not via the portal. If direct mode is defined for the storage node, Hitachi Vantara recommends setting the deduplication method to fixed blocks and keeping the default 4MB fixed block size. Once **Direct Mode** is set, the **Use HTTPS** option is also checked and cannot be unchecked.

Adding a Global Administrator From Active Directory

HCP Anywhere Enterprise Portal can be integrated with Microsoft Active Directory. If you are integrating the HCP Anywhere Enterprise Portal with Active Directory, make sure the ports described in the planning part of the HCP Anywhere Enterprise Portal installation guide are opened.

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

Note: Global Administrators must have an email address, as well as a first and last name, defined in Active Directory. Users without one of these attributes cannot log in to the portal and will cause synchronization to fail.
Login using SAML, LDAPS or Kerberos to validate the global administrator is not supported.
Nested groups are not supported by default since supporting nested groups has a performance impact. If you need support for nested groups, contact Hitachi Vantara support.

After users are fetched, they can be viewed in the HCP Anywhere Enterprise Portal.

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

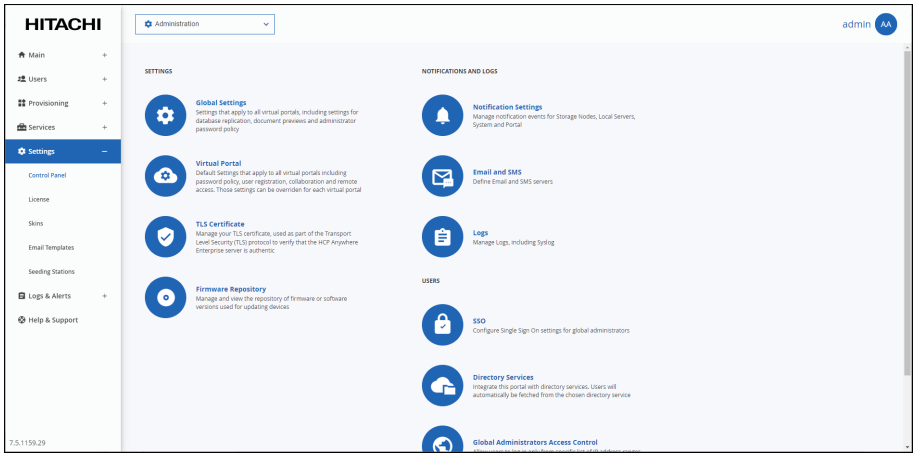
Integrating HCP Anywhere Enterprise Portal with Active Directory

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

- LDAPS (TCP port 636) and Global Catalog TLS (TCP port 3269) ports must be opened.
- Domain controllers must have a domain controller certificate with the EKU (Enhanced Key Usage) Client Authentication/ServerAuthentication.
  a) On the domain controller, open the Certificates MMC and export the domain controller certificate into .cer format.
  b) Import the certificate on each HCP Anywhere Enterprise Portal application server:
  Log in to each HCP Anywhere Enterprise Portal application server using SSH and run the command: `portal-cert.sh import -f <certificate>.cer <Alias_Name>`
  where *certificate* is a name for the certificate and *Alias_Name* is a name you can use to identify the certificate.
  Note: You only need to import the certificate and not the whole certificate chain.
  c) After importing the certificate to each HCP Anywhere Enterprise Portal application server, run the command to start the portal: portal-manage.sh restart
  d) Follow the instructions in the **To set up defining an administrator from Active Directory:** procedure, below, checking Use TLS.
  e) Remove access to ports TCP 389 and TCP 3268.

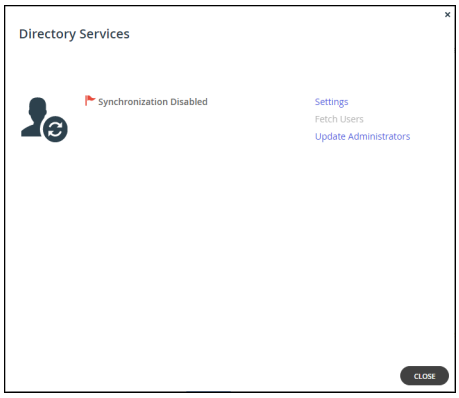
To set up defining an administrator from Active Directory:

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



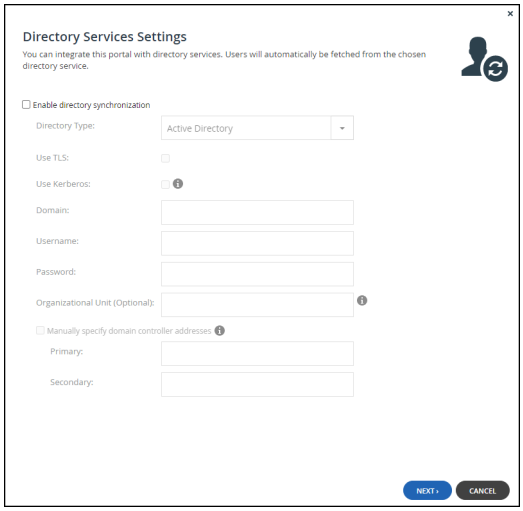
2. Select **Directory Services** under **USERS** in the **Control Panel** page.

   The **Directory Services** window is displayed.



3. Click **Settings** to set directory settings, including enabling connecting to a directory service. If you have already connected to a directory service, you can fetch all the users from the domain by clicking **Fetch Users**, as described in Manually Fetching Global Administrators From Active Directory.

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

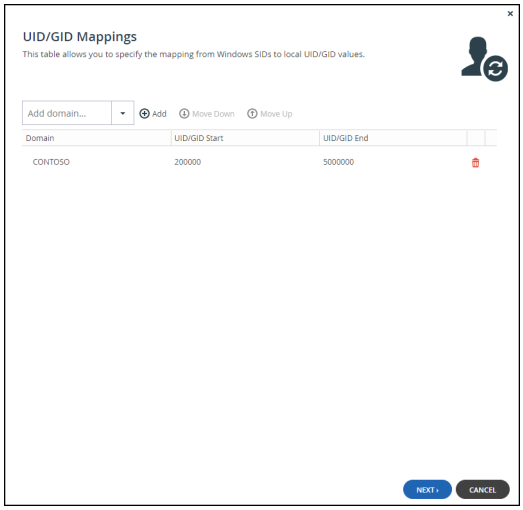


Enable Directory Synchronization – Enable integration with a directory domain.
Directory Type – Integration is with Active Directory.
Use TLS – Connect to the Active Directory domain using TLS.
Use Kerberos – Use the Kerberos protocol for authentication when communicating with the Active Directory domain. This is useful for achieving Single Sign-on (SSO) with Windows computers. If unchecked, NTLM is used.
Domain – The name of Active Directory domain with which you want to synchronize users.
Username – The name to use for authenticating to Active Directory.
Password – The password for authenticating to Active Directory.
Organizational Unit (Optional) – The name of the organizational unit within the Active Directory domain.
Manually specify domain controller addresses – The IP address of the Active Directory domain controllers. If unchecked, DNS is used to automatically find the domain controllers.

- Primary – The address of the primary domain controller.
- Secondary – The address of the secondary domain controller.

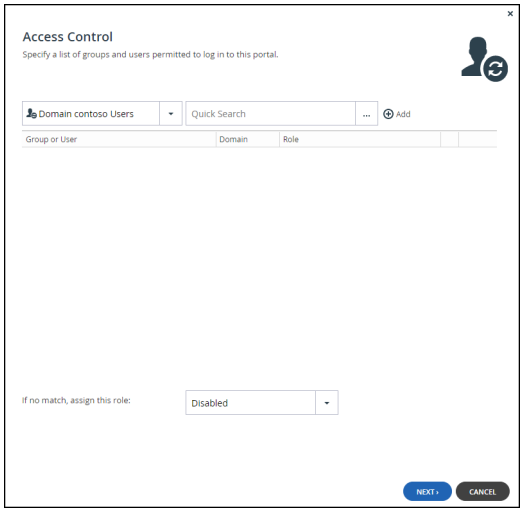
4. Click **NEXT**.

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



5. To add the other Active Directory domains in the tree/forest, do the following for each one:
   a) Select the user to add to the group and click **Add**.
   In the **Add domain** field, enter the Active Directory domain name, or select it from the drop-down list and click **Add**.
   The domain is added.
   In the **UID/GID Start** field enter the starting number in the range of portal user and group IDs (UID/GID) to assign to users and user groups from this Active Directory domain.
   In the **UID/GID End** field enter the ending number in the range of portal user and group IDs (UID/GID) to assign to users and user groups from this Active Directory domain.
   b) You can re-order the list of added domains by selecting a domain and clicking **Move Up** or **Move Down**.
   The order in which domains are displayed represents the order in which the domains are displayed in lists throughout the portal interface.
6. Click **NEXT**.

   The **Access Control** window is displayed.



7. Add each global administrator allowed to access the portal:
   a) In the drop-down list, select one of the following:
   Domain Users – Search the users defined in directory service.
   Domain Groups – Search the user groups defined in directory service.
   b) Select the user or user group from the drop-down list or in the **Quick Search** field, enter a string that is displayed anywhere within the name of the user or user group you want to add.
   c) Select the user or group and click **Add**.
   The user or user group is added to the list of users and user groups with access to the portal.
8. To remove a user or group, select the row and click .

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

   Disabled – The user account is disabled. The user cannot access the end user portal view.
   Read/Write Administrator – The user can access the end user portal view as an administrator with read-write permissions.
   Read Only Administrator – The user can access the end user portal view as an administrator

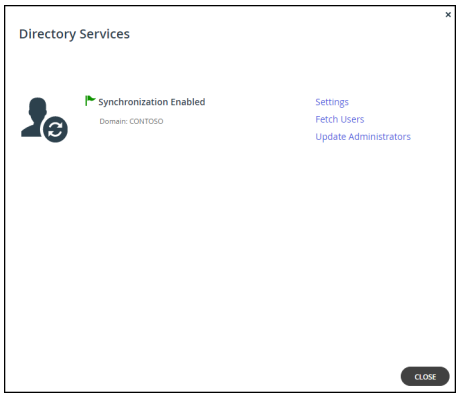
with read-only permissions.
Support – The administrator has read/write access to devices, user accounts, folders, and folder groups, and read-only access to all other settings in the HCP Anywhere Enterprise Portal.

10. To assign a role for a global administrator with no match in the access control list, select the user role from the **If no match, assign this role** drop-down list: **Disabled**, **Read/Write Administrator**, **Read Only Administrator**.
11. Click **NEXT**.

    The **Wizard Completed** window is displayed.
12. Click **FINISH**.

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

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



14. Click **CLOSE**.

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

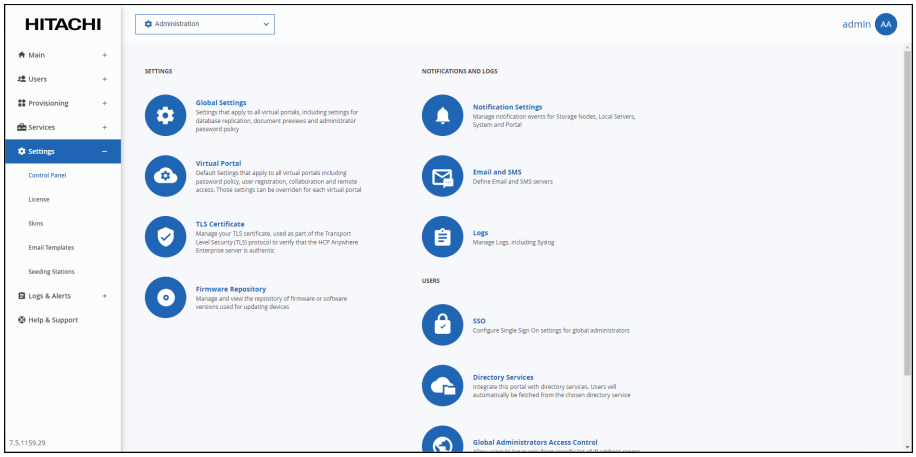
Manually Fetching Global Administrators From Active Directory

You can manually fetch user data from an integrated directory, after the connection with the directory service is established to immediately update data in the local user database, instead of waiting for HCP Anywhere Enterprise Portal to automatically fetch data at midnight.

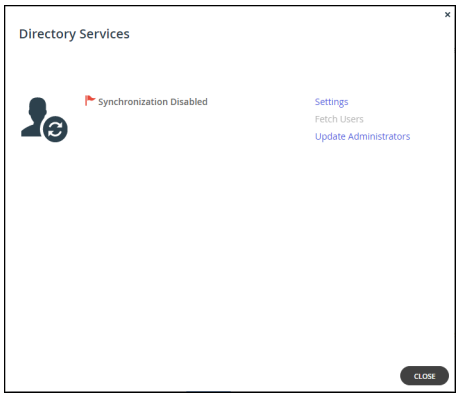
Note: If an administrator in Active Directory is disabled, manually fetching the user data immediately updates the portal users, instead of waiting until the portal automatically re-fetches all previously fetched directory users, every day at midnight.

To manually fetch user data:

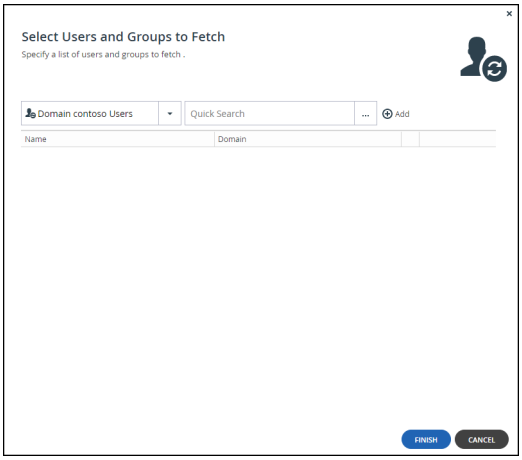
1. Select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.



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



3. Either,
   Click **Update Administrators**.
   Or,
   a) Click **Fetch Users**.
   The **Select Users and Groups to Fetch** window is displayed.



b) Add each global administrator allowed to access the portal:
In the drop-down list, select one of the following:
Domain Users – Search the users defined in directory service.
Domain Groups – Search the user groups defined in directory service.
Select the global administrator from the drop-down list or in the Quick Search field, enter a string that is displayed anywhere within the name of the user or user group you want to add.
Select the user or group and click **Add**.
The user or user group is added to the list of users and user groups to fetch.

c) Click **FINISH**.

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

4. Click **CLOSE**.

What's New In the Portal Image

ID Number	Description
PIM-3277, PIM-3540, PIM-3684	The HCP Anywhere Enterprise Messaging service could not be configured when FIPS was set.
PIM-3510	The AWS Systems Manager Agent (SSM Agent) was upgraded to amazon-ssm-agent-3.1.1080.0-1.x86_64.
PIM-3559	Security has been strengthened.
PIM-3600	During and immediately after a resource spike, the local quota feature stopped working.
PIM-3606, PIM-3607, PIM-3608	To increase security (CESA-2023:4152, CESA-2023:3556) the bind-utils package, openSSH, and Python have been updated.
PIM-3689	In an environment with multiple servers, starting t he portal on some of the servers timed out.
PIM-3696	The Key Management service (KMIP) did not work with the latest 7.5.x version.
PIM-3749	To improve security, the following packages have been updated: bind-export-libs to 9.11.4-26.P2.el7_9.14 bind-export-libs to 3.10.0-1160.95.1.el7

New Software Features

ID Number	Description
SP-23023	The time to deploy a portal server has been improved.
SP-23153	The Access and System log information displayed were not fully SOCII compliant.
SP-23246, SP-23247	When the HCP Anywhere Enterprise Messaging service is used, each messaging server IP no longer needs to be included in the **No Proxy For** list when setting up a proxy server in **Global Settings**.
SP-23384, SP-23385	A new storage node is available: HCP Hitachi Vantara (S3). For details, see New Storage Node: HCP Hitachi Vantara (S3). For the list of other supported storage nodes, refer to the *Hitachi Content Platform Anywhere Enterprise Global Administration Guide*.
SP-23441, SP-23447	Global administrators can be defined in Active Directory, but there must always be at least one local global administrator. For details, see Adding a Global Administrator From Active Directory.

Resolved Software Issues

ID Number	Description
SP-23006	When the Edge Filer Syslog service displayed a warning, the global banner was not displayed properly and the syslog servers disappeared from the user interface.
SP-23143	The *Messaging Status Monitoring* background task failed.
SP-23145	The HCP Anywhere Enterprise Edge Filer continued to display a `No Storage Node available` status even when the storage node problem was resolved.
SP-23150, SP-23151	Deleting a cloud folder and then creating a new cloud folder with the deleted folder name caused the deleted folder to be immediately deleted from the trashcan.
SP-23245	An error message was mistakenly issued when disabling database replication.
SP-23256	An active directory user in a child domain could not log in to the portal using SSO.
SP-23325	After a consent banner was implemented logging on using SSO failed.
SP-23350	The current snapshot could be updated to a temp snapshot or previous snapshot.
SP-23356	Connecting to a share using SMB and attempting to retrieve files from a previous snapshot timed out.
SP-23387	A *Failed to update folder stats* error was issued on application servers.
SP-23425	Deleting and undeleting a folder that was defined in a zone caused the syncing of the folder to hang after upgrading an edge filer.
SP-23530	An edge filer that was removed from a zone could still sync folder metadata.
SP-23568	In rare scenarios, adding a user from Active Directory failed and the task to add users from Active Directory did not complete.
SP-23650	Upgrading a HCP Anywhere Enterprise Portal while migrating files to a HCP Anywhere Enterprise Edge Filer failed.
SP-23701	In an environment with zones, sometimes folders from a HCP Anywhere Enterprise Edge Filer with folders to sync, connected to the zone, were not synced.
SP-23731	A portal with FIPS enabled could not connect to Active Directory via TLS.
SP-23755	The HCP Anywhere Enterprise Messaging service and dependent services, such as local quota, could not be configured when FIPS was set.
SP-23776	The task to update accounts ran multiple times a day instead of once a day.
SP-23854	The Key Management service (KMIP) did not work after an upgrade.
SP-23868	In specific scenarios, Active Directory groups were not fetched to the portal.
SP-23889	The portal sent too many requests to the antivirus server in too short a time.
SP-23962	Files did not upload to the portal while FSCK was running.

Known Issues

ID Number	Description
SP-16614	Support users with the relevant permissions cannot create user groups, add or remove users in an existing group nor delete users.
SP-17928	After changing a plan name and applying it, the process shows that zero users are updated.
SP-21806	Setting a preview server fails initially but after approximately 60 seconds starts working.
SP-23792	A portal with FIPS enabled could not set a local quota.

Hitachi Vantara

Corporate Headquarters 2535 Augustine Drive
Santa Clara, CA 95054 USA www.HitachiVantara.com community.HitachiVantara.com

Regional Contact Information
Americas: +1 866 374 5822 or info@hitachivantara.com
Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@hitachivantara.com
Asia Pacific: +852 3189 7900 or info.marketing.apac@hitachivantara.com