Hitachi Content Platform Anywhere Enterprise

v8.0

Portal Installation Guide for ESXi

This document describes how to install and configure an HCP Anywhere Enterprise Portal in a Vmware ESXi environment.

MK-HCPAE000-03
December 2023

Contents

Preface

About this document

This book describes how to install and initial configuration of an Hitachi Content Platform Anywhere Enterprise Portal in a VMware ESXi environment.

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 personnel who will install an HCP Anywhere Enterprise Portal.

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. Planning Your Installation

HCP Anywhere Enterprise Portal is a scalable cloud service delivery platform that you install at your own data center or in a cloud environment and use to create, deliver and manage cloud storage applications, including a Global File System, file access via stubbing/caching, backup, and mobile collaboration. HCP Anywhere Enterprise Portal is compatible with cloud storage infrastructure from multiple vendors and cloud storage providers such as AWS, Azure, and Google Cloud Platform.

HCP Anywhere Enterprise Portal facilitates access to cloud storage services; handles data protection and file sync & share services; used for provisioning and monitoring global file services. This is the beating heart of the system and is the component that will run in the customer's Datacenter or VPC. The portal ensures data consistency, maintains version history, and facilitates file sharing among users, regardless of their access method. Both global source-based deduplication and data compression are used to ensure that only incremental data changes are transferred for storage in the cloud, and that data blocks are stored only once. This dramatically reduces storage capacity needs and overall network traffic. You extend the global file system to users, via HCP Anywhere Enterprise Edge Filers, HCP Anywhere Enterprise Drive Share (Agents), and HCP Anywhere Enterprise Drive Connect. The portal ensures data consistency, maintains version history, and facilitates file sharing among users, regardless of their access method. Both global source-based deduplication and data compression are used to ensure that only incremental data changes are transferred for storage in the cloud, and that data blocks are stored only once. This dramatically reduces storage capacity needs and overall network traffic.

HCP Anywhere Enterprise Portal enables you to create one or more tenants, called Team, or Virtual, Portals. These tenants are accessed by end-users and management staff via web-based interfaces. HCP Anywhere Enterprise Edge Filers and endpoint HCP Anywhere Enterprise Agents are centrally managed from HCP Anywhere Enterprise Portal using a single web-based console. Template-based management, centralized monitoring, customized alerting and remote software and firmware upgrade capabilities make it easy to manage gateways of various types and sizes as well as individual endpoints – up to hundreds of thousands of connected devices – with no need for on-site IT presence in remote locations.

Together, these components allow Hitachi Vantara to offer true global file services: files are centrally stored and protected, while users can easily access them everywhere. On top of the all-in-one global namespace/file system approach, Hitachi Vantara allows its customers to achieve the following goals:

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

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

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

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

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

Planning Your Installation

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

- **Main database**. Only one server can host the main database. The server that hosts the main database is called the primary server.
- **Database replication server**. A passive database service set to replicate the primary server. During server installation, you can turn on the replication service and select the primary server from which to replicate.
- **Application server**. This service accepts connections and handles requests from Web and CTTP clients. Application servers are added to the cluster to increase client handling capacity. Any servers that are enabled as application servers automatically balance the connected clients between them, allowing for maximized capacity and availability.

  Note: CTTP clients are HCP Anywhere Enterprise Edge Filers and Agents that communicate with the HCP Anywhere Enterprise Portal application server using a proprietary secure, WAN optimized transport protocol.
- **Messaging server**. This server enables sending notifications from the portal to various consumers, for example the Varonis Data Security Platform, which is a connector running on top of the HCP Anywhere Enterprise Messaging Service. In production environments that use the messaging service, the HCP Anywhere Enterprise Portal must include three application servers defined as messaging servers.
- **Document preview server**. This server is used to process document preview requests. The document preview server supports high availability. You can install one or more servers, in order to ensure uninterrupted document preview generation and redundancy in the event of a server failure.

By default, the first installed server is the primary server, hosting the main database and application server. You can install any number of additional servers. The same procedure is used to install all the server instances.

Scalability, Sizing, and Load Balancing

HCP Anywhere Enterprise Portal is horizontally scalable. Additional servers can be added:

- As application servers, to increase client handling capacity. Any servers that are enabled as application servers automatically balance the connected clients between them, allowing for maximized capacity and availability. The number of application servers deployed depends on

the use case:
    - ROBO (remote office, branch office) use case – The users connect to the local HCP Anywhere Enterprise Edge Filers, each edge filer connection to a virtual portal is one connection, even if there are thousands of users connected to each edge filer. You require one application server for every 100 edge filers.
    - FSS (file sync and share) use case – The users connect directly to a virtual portal. You require one application server for every 10,000 users and a minimum of one virtual portal for every 100,000 users.
- As messaging servers, to enable sending notifications from the portal to various consumers, for example the Varonis Data Security Platform, which is a connector running on top of the HCP Anywhere Enterprise Messaging Service. In production environments that use the messaging service, the HCP Anywhere Enterprise Portal must include three application servers defined as messaging servers.
- As document preview servers. The document preview servers supports high availability. You can install one or more servers, in order to ensure uninterrupted document preview generation and redundancy in the event of a server failure.

Data Replication and Failover

The main database is stateful and contains critical data. You must replicate all such servers to maintain the availability of critical data. The application service is stateless, and therefore, any dedicated application servers do not require replication or backup. Failover between application servers is automatic.

Replicating the database is described as part of the installation for a HCP Anywhere Enterprise Portal.

HCP Anywhere Enterprise Portal includes a built-in replication function for achieving higher level of availability. Replication can be achieved using other platform dependent replication methods (such as SAN or VMWare-level replication).

SECURITY

All internal communication between HCP Anywhere Enterprise Portal servers is authenticated to prevent unauthorized access. Nevertheless, to follow the defense in-depth security philosophy, the primary database server, which stores sensitive data, should be placed in its own firewalled, isolated network, and only the application servers should be allowed to face the Internet.

REQUIREMENTS

The HCP Anywhere Enterprise Portal image, obtainable from Hitachi Vantara support. The HCP Anywhere Enterprise Portal can be managed in VMware vCenter and in VMware vCloud Director.

HCP Anywhere Enterprise Portal must be installed on a machine that meets the following requirements:

- VMware ESXi 6.7U1 or later. Hitachi Vantara recommends 7.0.x and later as VMware has announced that version 6.7U1 has reached the end of life.
- **Production Deployment Blueprint**
  A minimal production installation of HCP Anywhere Enterprise Portal comprises of four 64-bit virtual machines: Two database servers (primary and secondary) and two application servers. The minimum two application servers are required for high availability and load balancing.
  If the HCP Anywhere Enterprise Messaging service is deployed, the minimal production installation comprises of five 64-bit virtual machines: Two database servers (primary and secondary), and three application servers that also function as messaging servers.
  For more details about the HCP Anywhere Enterprise Messaging service, see Managing the HCP Anywhere Enterprise Messaging Service.
  Additional application servers may be deployed for further load balancing.
  Note: Three, and only three application servers function as messaging servers. Any additional servers function purely as application servers for load balancing.
  Optionally, one or more preview servers can be deployed for document previews.
  The following table details the requirements per HCP Anywhere Enterprise Portal Server in a production environment.

Server	Minimum Requirements	Notes
Primary Database Server	8 vCPU, 32GB RAM, 100GB data pool (SSD), 200GB archive pool (Magnetic)	The data pool should have at least 2000 IOPS and should be sized around 1% of the expected global file system size. The archive pool size should be double that of the data pool.
Secondary, Replication, Database	The replication database server must have the same configuration as the primary database server.	–
Application Server	4 vCPU, 16GB RAM, 100GB data pool (Magnetic) **or**, with the HCP Anywhere Enterprise Messaging service: 4 vCPU, 32GB RAM, 250GB data pool (Magnetic)	An application server can handle up 10,000 clients. When the number of expected clients will be near 10,000, 8 vCPUs and an additional 16GB is recommended (32GB without the HCP Anywhere Enterprise Messaging service and 48GB with the HCP Anywhere Enterprise Messaging service).
Preview Server	4 vCPU, 16GB RAM, 60GB data pool (SSD)	–

Note: All resources allocated to a server must be dedicated to that server and not shared with other servers. You must not run non-HCP Anywhere Enterprise applications on any of the HCP Anywhere Enterprise Portal servers.
Hitachi Vantara recommends seeking guidance from Hitachi Vantara support for a more accurate estimation of the required sizing.

- **Test Deployment Blueprint**
  The following table details the minimal requirements in a test configuration, with a single 64-bit virtual machine deployment.

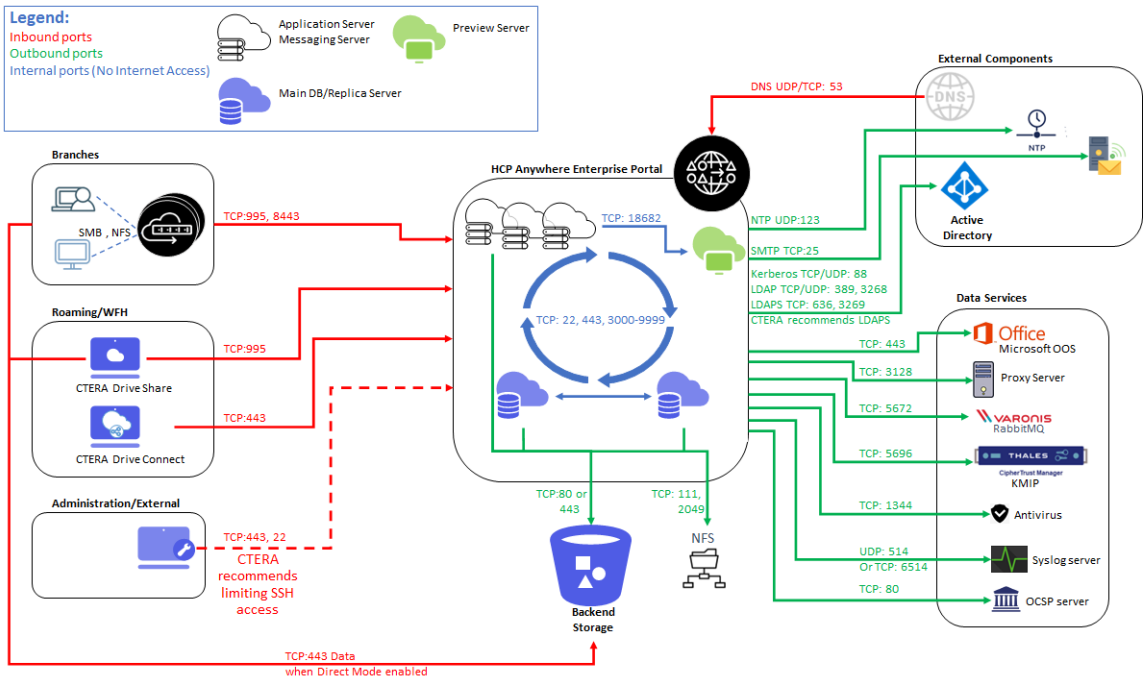
  Warning: Do not use this setup for production.

  If the HCP Anywhere Enterprise Messaging service will not be part of the test deployment:
  - Single server, 2 vCPU, 8GB RAM, 100GB SSD storage.

  If the HCP Anywhere Enterprise Messaging service will be part of the test deployment:
  - Single server, 4 vCPU, 24GB RAM, 250GB SSD storage.
- **Other requirements**
  - Access from the virtual machine to a Storage Area Network (SAN) or directly attached hard drive.
  - Specific ports must be open. For details, see Port Requirements.
  - A DNS name for the HCP Anywhere Enterprise Portal installation. This can be changed after the installation.
  - An ICAP Server and license if the antivirus feature will be used.
  - An SMTP mail server address and port for sending notifications.

Port Requirements

To allow access to and from the Internet on the firewall on each machine that will operate as an application server or database server, ensure the relevant network ports are open. In addition, portal servers communicate with each other over specific ports. These ports also need to be opened but do not need Internet access.


Legend:
Inbound ports
Outbound ports
Internal ports (No Internet Access)
Application Server
Messaging Server
Preview Server
Main DB/Replica Server
External Components
DNS UDP/TCP: 53
DNS
NTP
Active Directory
Branches
SMB , NFS
TCP:995, 8443
HCP Anywhere Enterprise Portal
TCP: 18682
NTP UDP:123
SMTP TCP:25
Kerberos TCP/UDP: 88
LDAP TCP/UDP: 389, 3268
LDAPS TCP: 636, 3269
CTERA recommends LDAPS
TCP: 22, 443, 3000-9999
Data Services
Roaming/WFH
CTERA Drive Share
TCP:995
CTERA Drive Connect
TCP:443
TCP: 443
Office
Microsoft OOS
TCP: 3128
Proxy Server
TCP: 5672
RabbitMQ
TCP: 5696
KMIP
TCP: 1344
Antivirus
UDP: 514
Or TCP: 6514
Syslog server
TCP: 80
OCSP server
Administration/External
TCP:443, 22
CTERA recommends limiting SSH access
TCP:80 or 443
TCP: 111, 2049
NFS
Backend Storage
TCP:443 Data
when Direct Mode enabled

Inbound Ports

Port	Protocol	Notes
22	TCP	SSH. Hitachi Vantara recommends limiting SSH access to specific IP addresses that may require access to the HCP Anywhere Enterprise application servers, for example to perform scheduled maintenance and support related work.
53	UDP	DNS resolution server (If portal internal DNS server is registered in DNS)
80	TCP	HTTP (redirects to port 443)
443	TCP	HTTPS
995	TCP	CTTP protocol communications with HCP Anywhere Enterprise Edge Filers and agents. For details about CTTP, see What is the CTTP Transport Protocol
8443	TCP	Communications with HCP Anywhere Enterprise Edge Filers for log collection

Outbound Ports

Port	Protocol	Notes
25	TCP	Default SMTP port. This port can be configured on the SMTP server and specified in the portal Web interface
80	TCP	HTTP
88	TCP & UDP	If Kerberos is used
111	TCP	NFS, only required if NFS storage is used
123	UDP	NTP (Network Time Protocol)
389	TCP & UDP	LDAP/LDAP GC (Global Catalog)
443	TCP	HTTPS
514	UDP	Default Syslog port. This port can be configured on the Syslog server
636	TCP	LDAP and LDAP GC with TLS (Hitachi Vantara recommends using LDAPS and LDAPS GC instead of LDAP and LDAP GC)
1344	TCP	If using an antivirus server
2049	TCP	NFS, only required if NFS storage is used
3128	TCP	Default Proxy server port, only required if a proxy server is defined in the global administration, where a different port can be configured
3268	TCP & UDP	LDAP/LDAP GC (Global Catalog)
3269	TCP	LDAPS and LDAPS GC (Hitachi Vantara recommends using LDAPS and LDAPS GC instead of LDAP and LDAP GC)
5672	TCP	Only required when using the Varonis service. The default port for RabitMQ. This port can be configured in Varonis Data Security Platform
5696	TCP	Only required when using the Key Management service to connect to the Key Management Interoperability Protocol (KMIP) server
6514	TDP	Default Syslog port over TCP/TLS, can be configured on the Syslog server

Additional Ports Not Requiring Internet Access

The following ports must be opened between the HCP Anywhere Enterprise Portal servers.

Port	Protocol	Notes
22, 443	TCP	Internal communication between HCP Anywhere Enterprise Portal servers
3000-9999	TCP	Internal communication between HCP Anywhere Enterprise Portal servers
18682	TCP	Only required when a Preview server is used

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

Chapter 2. Installing HCP Anywhere Enterprise Portal Instances

Creating a HCP Anywhere Enterprise Portal

Contact Hitachi Vantara and request the latest ESXi HCP Anywhere Enterprise Portal OVA file.

Note: The following procedure uses the vSphere Client. You can also use the vSphere Host Client. When using the vSphere Host Client, because the OVA file is larger than 2GB, you must unpack the OVA file, which includes the OVF file, VMDK and MF files. Use the OVF and VMDK files to deploy the HCP Anywhere Enterprise Portal.
For the primary database server and secondary, replication, server, the HCP Anywhere Enterprise Portal instance is created with a fixed size data pool. If you require a larger data pool, which should be approximately 1% of the expected global file system size, you can extend the data pool.

To create the HCP Anywhere Enterprise Portal instance:

Note: The following procedure is based on vSphere Client 7.0.3. The order of actions might be different in different versions.

1. In the vSphere Client console click **File > Deploy OVF Template**.
2. The **Deploy OVF Template** wizard is displayed.
3. Browse to the HCP Anywhere Enterprise Portal OVA file and choose it.
4. Click **NEXT**.
5. Continue through the wizard specifying the following information, as required for your configuration:
   - A name to identify the HCP Anywhere Enterprise Portal in vCenter.
   - The location for the HCP Anywhere Enterprise Portal: either a datacenter or a folder in a datacenter.
   - The compute resource to run the HCP Anywhere Enterprise Portal.
6. Click **NEXT** to review the configuration details.

   Note: Click **Ignore** in the warning to be able to proceed.
7. Click **NEXT**.
8. Select the virtual disk format for the HCP Anywhere Enterprise Portal software and the storage to use for this software. Refer to VMware documentation for a full explanation of the disk provisioning formats. For **Select virtual disk format** select either **Thick Provision Lazy Zeroed** or **Thick Provision Eager Zeroed** according to your preference.
   - **Thick Provision Lazy Zeroed** – Creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine. Using the default flat virtual disk format does not zero out or eliminate the possibility of recovering deleted files or restoring old data that might be present on this allocated space.
   - **Thick Provision Eager Zeroed** – Creates a virtual disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data remaining on the physical device is zeroed out when the virtual disk is created. It might take much longer to create disks in this format than to create

lazy zeroed disks.

9. Click **NEXT**.
10. Select the **Destination Network** that the HCP Anywhere Enterprise Portal will use.
11. Click **NEXT** to review the configuration before creating the VM and then click **FINISH**.

    The HCP Anywhere Enterprise Portal is created and powered off.
12. For the primary database server and secondary, replication, server, right-click the VM in the navigation page and choose **Edit Settings**.

    The **Hard disk 2** and **Hard disk 3** entries together make up the data pool.

    a) Click **ADD NEW DEVICE > Hard Disk**.
    A new hard disk is added to the list of hard disks.

    b) Enter a size for the new hard disk.

    Note: The minimum archive pool should be 200GB but it should be sized around 2% of the expected global file system size.

    c) Expand the New Hard disk item and for Location browse to a the datastore you want for the archive pool.

    d) Select the disk to use for the archive pool.

    e) Click **OK**.
13. Power on the HCP Anywhere Enterprise Portal virtual machine.
14. For the primary database server and the secondary, replication, servers, continue with Logging in to the Server to Create the Archive Pool.

Logging in to the Server to Create the Archive Pool

You need to create an archive pool on the primary database server, and when PostgreSQL streaming replication is required, also on the secondary, replication, server.

To log in to the HCP Anywhere Enterprise Portal server:

- Log in as **root**, using SSH or through the console.
  The default password is `%1Change:Me0`.

You are prompted to change the password on your first login.

To create the archive pool:

1. Log in as `root`, using SSH or through the console.
2. Run `fdisk -l` to identify the disk to use for the archive pool.
3. Run the following command to create the archive pool: `portal-storage-util.sh create_db_archive_pool` *Device*

   where *Device* is the Device name of the disk to use for the archive pool.
   For example: portal-storage-util.sh create_db_archive_pool sdd

   Note: When using NFS storage, before you can create the database archive pool, you have to disable the root squashing security setting for NFS export while setting up the database replication. In the NFS implementation use the `disable root squash` setting. After disabling root squash, run the following command to create the database archive pool: `portal-storage-util.sh create_db_archive_pool -nfs <NFS_IP>:/export/db_archive_dir`
   where *NFS_IP* is the IP address of the NFS mount point.
   Hitachi Vantara recommends re-enabling root squash for the NFS export after the

database replication is set up and verified to be working.

4. Start HCP Anywhere Enterprise Portal services, by running the following command:
   `portal-manage.sh start`

Configuring Network Settings

By default, the HCP Anywhere Enterprise Portal server obtains an IP address using DHCP. In a production environment it is recommended to use a static IP address. Also when your infrastructure includes more than one network, you have to configure HCP Anywhere Enterprise Portal for the appropriate network. You configure network settings by using **nmtui**, the built-in network manager.

To use nmtui:

1. Log in as `root`, using SSH or through the console.
2. Run the following command: `nmtui`

   The **NetworkManager TUI** screen is displayed.
3. Use your keyboard arrows or the **TAB** key to navigate between options.

Changing the HCP Anywhere Enterprise Portal Server's Hostname

To change the HCP Anywhere Enterprise Portal server's hostname:

1. In nmtui, navigate to **Set system hostname** and press **Enter**.
   The **Set Hostname** screen opens, displaying the current HCP Anywhere Enterprise Portal hostname.
2. In the field provided, enter the server hostname.
3. Navigate to **OK** and press **Enter**.

   A confirmation message is displayed.
4. Press **Enter**.

   The new hostname is configured.
5. Navigate to **Quit** and press **Enter** to exit nmtui.
6. You need to reboot the system for the change to take effect. You can reboot the system by entering the command: `reboot`

Configuring a Network Interface

Listing Network Interfaces

To list all network interfaces:

- Run the following command: `ifconfig`

Configuring a Static IP Address for a Network Interface

To configure a static IP address for a network interface:

1. In nmtui, navigate to **Edit a connection** and press **Enter**.
   The following window opens, displaying all network adapters attached to the HCP Anywhere Enterprise Portal server.
2. Navigate to the network adapter for which you want to set a static IP address and press **Enter**.

   The **Edit connection** window is displayed.

3. Navigate to **Automatic** next to **IPv4 CONFIGURATION**, press **Enter**, and then select **Manual**.
4. Navigate to **Show** next to **IPv4 CONFIGURATION** and press **Enter**.

   Additional fields are displayed.
5. Navigate to **Add** next to **Addresses** and press **Enter**.
6. Type the static IP address.

   To specify a subnet mask, use the classless inter-domain routing (CIDR) notation. For example:
   - To set a class C subnet mask [255.255.255.0], use: *IP_Address*/24, for example, 192.168.93.204/24
   - To set a class B subnet mask [255.255.0.0], use: *IP_Address*/16, for example, 192.168.93.204/16

   You can refer to the following link for a full IPv4 CIDR reference: https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing#IPv4_CIDR_blocks
7. To configure a default gateway for the current network interface, navigate to **Gateway**, and then type the IP address of the default gateway.
8. To configure a DNS server, navigate to **Add** next to **DNS servers**, press **Enter**, and then enter the IP address of the DNS server.

   Note: You can add multiple DNS servers if desired, by repeating this step.
9. Navigate to **OK** and press **Enter**.
10. Navigate to **Quit** and press **Enter** to exit nmtui.
11. Restart the network service by typing the command: `service network restart`

Your changes take effect.

Enabling DHCP for a Network Interface

If you want to use DHCP, for example, for a demo, and you are configured to use a static IP, you can change to DHCP using nmtui.

To enable DHCP for a network interface:

1. In nmtui, navigate to **Edit a connection** and press **Enter**.
   A screen opens, displaying all network adapters attached to the HCP Anywhere Enterprise Portal server.
2. Navigate to the network adapter for which you want to enable DHCP, and then press **Enter**.

   The **Edit connection** screen is displayed.
3. Navigate to **Manual** next to **IPv4 CONFIGURATION**, press **Enter**, and then select **Automatic**.
4. Navigate to **OK** and press **Enter**.
5. Navigate to **Quit** and press **Enter** to exit nmtui.
6. Restart the network service, by entering the command: `service network restart`

Your changes take effect.

Deactivating a Network Interface

To deactivate a network interface:

1. In nmtui, navigate to **Activate a connection** and press **Enter**.
   A screen opens, displaying all network adapters attached to the HCP Anywhere Enterprise Portal server.

Note: An asterisk (*) to the left of a network adapter's name indicates that the network adapter is activated.

2. Navigate to the activated network adapter you want to deactivate, a network adapter with an asterisk, and press **Enter**.
3. Navigate to **Quit** and press **Enter** to exit nmtui.

The network adapter is deactivated.

Activating a Network Interface

To activate a network interface:

1. In nmtui, navigate to **Activate a connection** and press **Enter**.
2. Navigate to the deactivated network adapter you want to activate, a network adapter without an asterisk, and press **Enter**.
3. Navigate to **Quit** and press **Enter** to exit nmtui.

The network adapter is activated.

The asterisk (*) to the left of a network adapter's name indicates that the network adapter is activated.

Configuring Static Routes

To configure a static route for a network interface:

1. In nmtui, navigate to **Edit a connection** and press **Enter**.
2. Navigate to the network interface for which you want to set a static route and press **Enter**.
   The **Edit connection** screen is displayed.
3. Navigate to **Show** next to **IPv4 CONFIGURATION** and press Enter.
   Additional fields are displayed.
4. Navigate to **Edit** next to **Routing** and press **Enter**.
5. Navigate to **Add** and press **Enter**.
6. In the fields provided, type the network destination/prefix, the next hop, and the route metric.
   Note: To add another static route, navigate to **Add** and press **Enter**, and then specify the route details.
   To remove an existing route, navigate to **Remove** next to the static route you want to remove and press **Enter**.
7. When done configuring static routes, navigate to **OK** and press **Enter**.
8. Navigate to **OK** and press **Enter**.
9. Navigate to **Quit** and press **Enter** to exit nmtui.
10. Restart the network service, by running the following command: `service network restart`
    Your changes take effect.
11. To view the list of static routes, run the following command: `netstat -rn`

Configuring a Default Gateway

To set a default gateway for the HCP Anywhere Enterprise Portal server:

1. Log in as root over SSH or through the console to the HCP Anywhere Enterprise Portal.
2. Run the following command:

   `echo "GATEWAY=`*`default_gateway_ip_address`*`" > /etc/sysconfig/network`

   Where *default_gateway_ip_address* is your default gateway IP address.
   For example: `echo "GATEWAY=192.168.90.1" > /etc/sysconfig/network`
3. Restart the network service, by running the following command: `service network restart`

   Your changes take effect.

Additional Installation Instructions for Customers Without Internet Access

The HCP Anywhere Enterprise Portal image requires packages for syslog functionality for offline servers. During a HCP Anywhere Enterprise Portal image installation, these packages are downloaded from the Internet and automatically installed. If you do not have access to the Internet, you can install these packages manually, using the archive file provided with the image installation file.

To install the syslog functionality archive:

1. Install the HCP Anywhere Enterprise Portal image with the latest image file, as described above, prior to running the setup wizard.
2. Get the archive file, **exported_images.tar.gz**, from Hitachi Vantara support and copy it to a local folder on the HCP Anywhere Enterprise Portal machine.
3. Run the following on all servers (including main, Replica, DB, and Preview servers):

   `portal-syslog-client load_images `*`images_archive_path`*

   where *images_archive_path* is the path to the local folder where you copied the archive file.
4. Run the setup wizard.

Troubleshooting

If the setup wizard was run prior to loading the new packages, an error message is generated. To resolve it, run the CLI `portal-syslog-client load_images `*`images_archive_path`* and restart all servers.

Note: If you do not run the CLI command, the syslog functionality will not work and an error message is generated. For these reasons it is recommended to run the command, however if you don't, apart from the error message, there is no impact on HCP Anywhere Enterprise Portals where syslog functionality is not used.

Chapter 3. Configuring the Primary Server

Configuring the primary server is a one-time operation, the first time you access the HCP Anywhere Enterprise Portal.

Note: All HCP Anywhere Enterprise Portal servers must not run other services. By default, HCP Anywhere Enterprise portal servers are application servers.

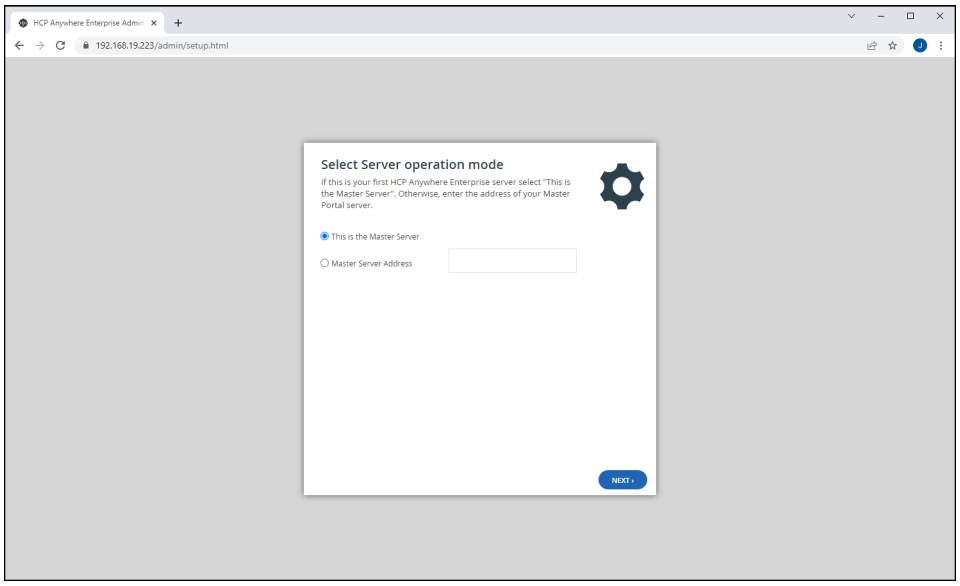
If you are installing an additional server, proceed directly with Installing Additional HCP Anywhere Enterprise Portal Servers.

PERFORMING INITIAL HCP ANYWHERE ENTERPRISE PORTAL SETUP

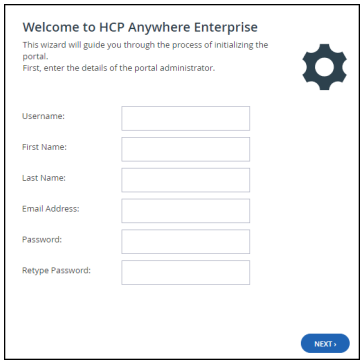
This procedure is performed only once, on the primary server.

To perform initial HCP Anywhere Enterprise Portal setup of the primary server:

1. Using a Web browser, browse to the HCP Anywhere Enterprise Portal, via the IP address or DNS.
   The **Setup** wizard opens, displaying the **Select Server operation mode** window.



2. Choose **This is the Master Server**.
3. Click **NEXT**.
   The **License Agreement** dialog box is displayed.
4. Read the agreement and then click **I Accept** and then click **NEXT**.
   The database is initialized and then the **Welcome to HCP Anywhere Enterprise Portal** window box is displayed.

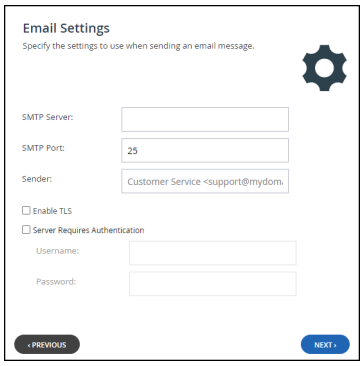


5. Complete the fields as follows:

   Username – The name for your HCP Anywhere Enterprise Portal administrator account.
   First Name – The first name of the administrator.
   Last Name – The last name of the administrator.
   Email Address – The email address of the administrator for notifications.
   Password – The password administrator will use to access the HCP Anywhere Enterprise Portal.
   Retype Password – The password.

6. Click **NEXT**.

   The **Email Settings** window is displayed.



7. Complete the fields as follows:

   SMTP Server – The outgoing mail server address for sending email messages from HCP Anywhere Enterprise Portal to users.
   SMTP Port – The port number for sending email messages from HCP Anywhere Enterprise Portal to users. This port is usually TCP 25.
   Sender – The email address that should appear in the From field of notifications.
   Enable TLS – Select this option to use Transport Layer Security (TLS) encryption for sending email messages from HCP Anywhere Enterprise Portal to users.
   Server requires authentication – Select this option if the SMTP server requires authentication.

   User Name – Type the user name that HCP Anywhere Enterprise Portal should use when authenticating to the SMTP server.
   Password – Type the password that HCP Anywhere Enterprise Portal should use when authenticating to the SMTP server.

   Warning: The username and password you specified for the HCP Anywhere Enterprise Portal administrator are sent to the email address using the information

specified here. If the address is incorrect, the email will not arrive and if you have not recorded the administrator username and password details and they are forgotten, you will not be able to access the HCP Anywhere Enterprise Portal.

8. Click **NEXT**.

   The **DNS Domain** window is displayed.

9. In the **DNS Suffix** field, type the DNS suffix to append to each virtual portal's name, in order to create the virtual portal's DNS name.

   For example, if a virtual portal's name is *myportal*, and the DNS suffix is *example.com*, then the virtual portal's DNS name is *myportal.example.com*.

   Note: You can change the DNS domain in the HCP Anywhere Enterprise Portal user interface, in **Settings > Global Settings**.

10. Click **NEXT**.

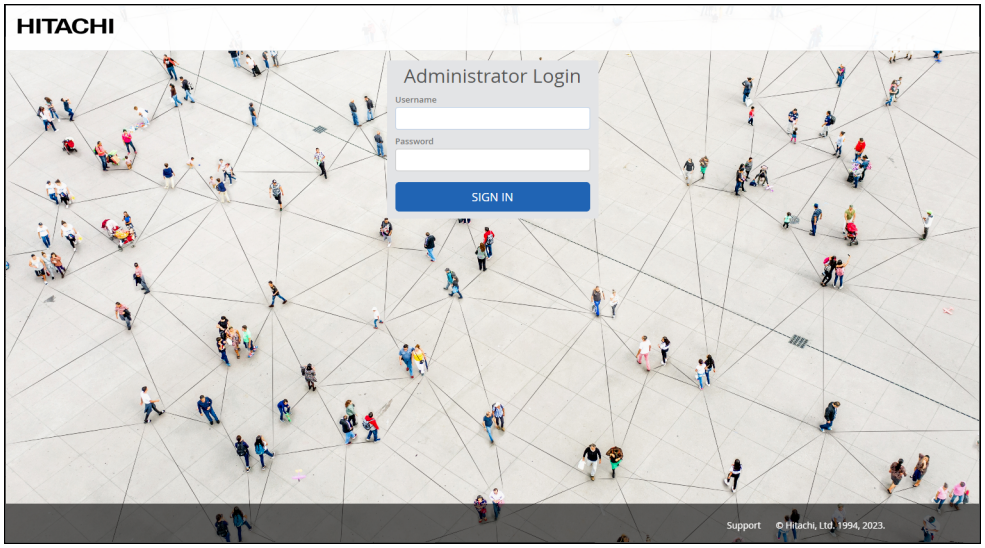
    The **Wizard Completed** window is displayed.

11. Click **FINISH**.

    The data is saved and a success message is displayed.

12. Click **OK**.

    HCP Anywhere Enterprise Portal opens, displaying the **Administrator Login** page.



13. Enter the user name and password you specified in step **5** and click **SIGN IN**.

The portal opens, displaying the **Main > Dashboard** page. By default, HCP Anywhere Enterprise Portal creates a team portal called *portal*. For information about how to rename, view and edit this portal, or create additional team portals, see the *Hitachi Content Platform Anywhere Enterprise Portal Team Administration Guide*.

Warning: The initial setup includes initializing the PostgreSQL database used by the HCP Anywhere Enterprise Portal. The database must be backed up. Backing up the database is described in Backing Up the HCP Anywhere Enterprise Portal Database.

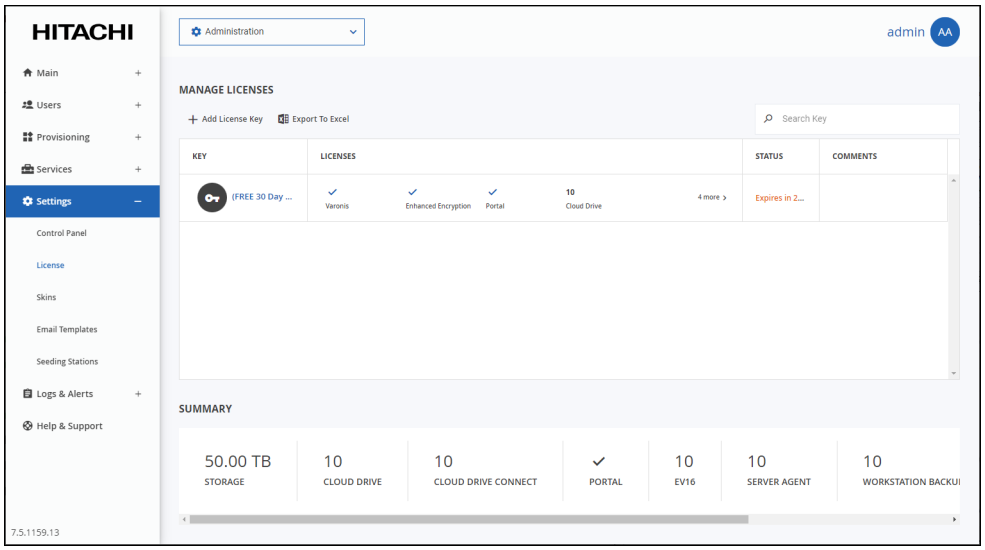
Installing the HCP Anywhere Enterprise Portal License

The HCP Anywhere Enterprise Portal includes a trial license for 30 days. Install the permanent license using the following procedure.

To install a license:

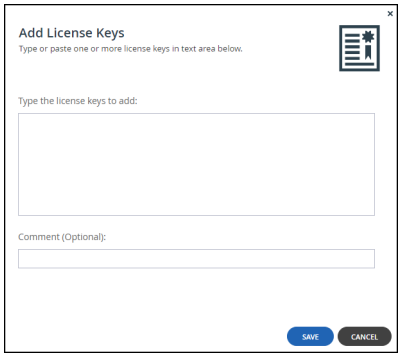
1. In the HCP Anywhere Enterprise Portal **Administrator Login** page, sign in as a global administrator.
2. In the global administration view, select **Settings > License** in the navigation pane.

   The **MANAGE LICENSES** page is displayed.



3. Click **Add license key**.

   The **Add License Keys** dialog box opens.



4. Copy the license key you received from Hitachi Vantara, and paste it into the text box.

   The system verifies and activates the license key by contacting the Hitachi Vantara Activation service. When the license key is activated, it is associated with this installation of HCP Anywhere Enterprise Portal.
5. Optionally add a comment In the **Comment** field.

   The comment is displayed in the **License** page. You can use this comment to document the purchase order number associated with the license, and the like.
6. Click **SAVE**.

Installing a TLS Certificate

Perform the following steps to install a certificate on HCP Anywhere Enterprise Portal:

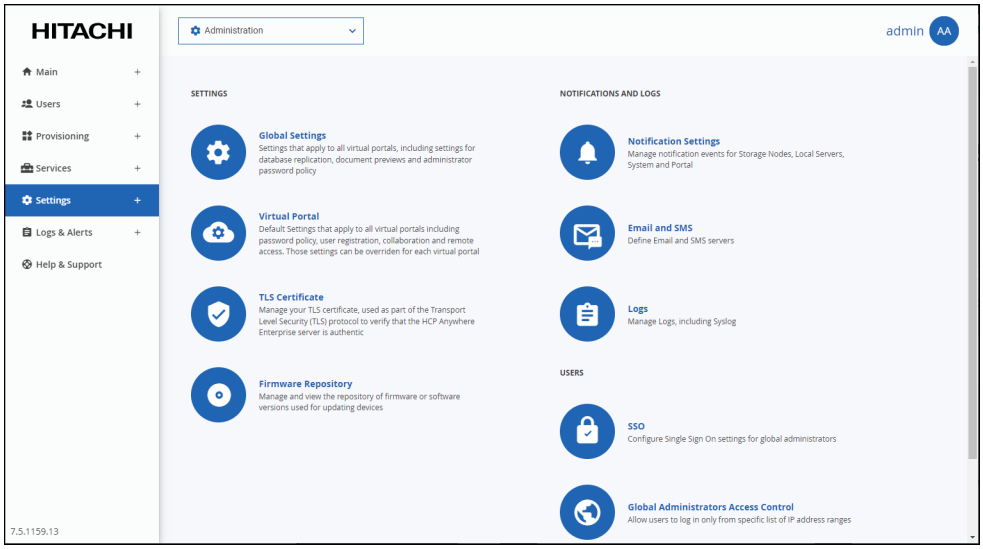
1. Note the HCP Anywhere Enterprise Portal DNS Suffix
2. Obtain a TLS Certificate
3. Generate a Certificate Signing Request
4. Sign the Certificate Request
5. Validate and Prepare Certificates for Upload
6. Install the Signed Certificate on HCP Anywhere Enterprise Portal

Note the HCP Anywhere Enterprise Portal DNS Suffix

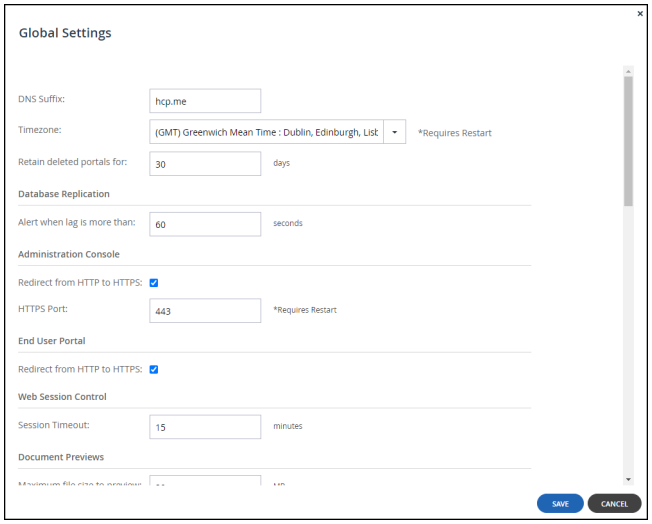
You need the HCP Anywhere Enterprise Portal's DNS suffix for use in later steps.

To view the HCP Anywhere Enterprise Portal DNS suffix:

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



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



3. Note the HCP Anywhere Enterprise Portal DNS Suffix in the **DNS Suffix** field.

Obtain a TLS Certificate

It is necessary to obtain a valid certificate signed either by a well-known certificate authority, such as GoDaddy, or by your own internal certificate authority.

The TLS certificate can be either of the following:

- **A wildcard certificate**
  A wildcard TLS certificate secures your website URL and an unlimited number of its subdomains. For example, a single wildcard certificate for *.hcp.com can secure both `company01.hcp.com` and `company02.hcp.com`, which may be for virtual portals *company01* and *company02*.

A wildcard certificate is mandatory if you plan for your service to consist of more than one virtual portal.

- **A domain certificate**
  A domain certificate secures a single domain or subdomain only. For example:
  `company01.hcp.com`
  This option is relevant if you are planning to provision a single virtual portal only.

Note: To obtain a self-signed certificate for testing and evaluation purposes only, contact Hitachi Vantara Support and specify the HCP Anywhere Enterprise Portal DNS suffix, see Note the Portal's DNS Suffix. Hitachi Vantara will generate a self-signed certificate for your DNS suffix and provide you with a ZIP file that you can upload to your HCP Anywhere Enterprise Portal environment.
HCP Anywhere Enterprise Portal also supports certificates with Subject Alternative Names: SAN certificates. This option enables you to secure multiple domain names with a single certificate.

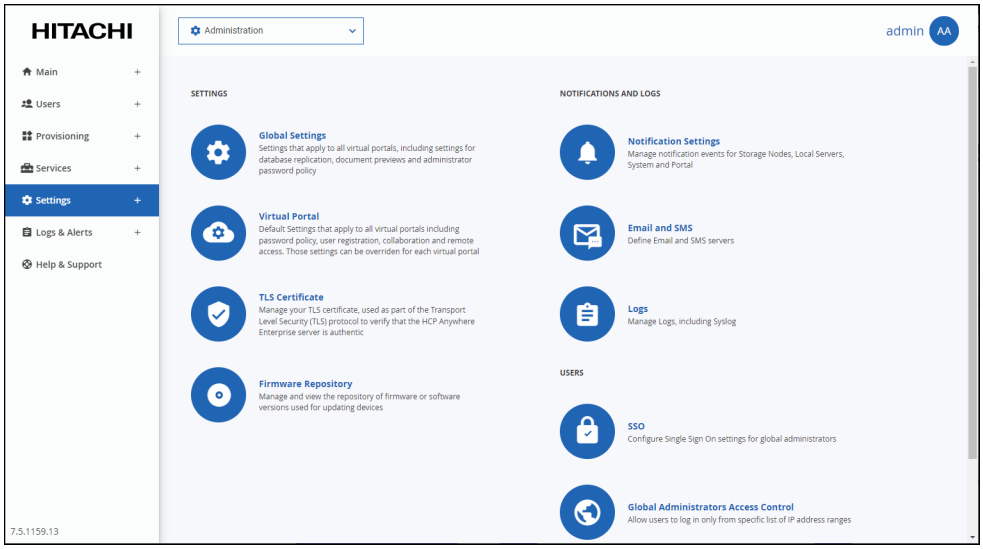
Generate a Certificate Signing Request

You need to generate a certificate signing request, CSR, for your domain. You can generate the CSR from within the HCP Anywhere Enterprise Portal or externally. If you generate the CSR externally, convert the private key file to RSA(PKCS1) format.

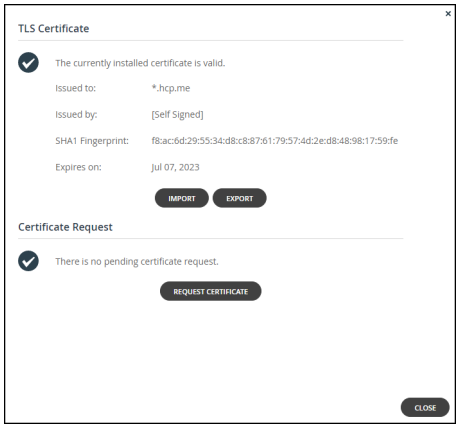
Warning: HCP Anywhere Enterprise Portal generates a built-in certificate that is not suitable for production. This certificate is valid for testing purposes only, as it is not signed by a well-known certificate authority.

To generate a certificate signing request for your domain:

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



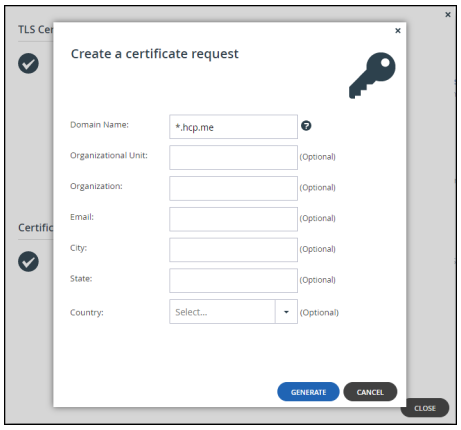
2. Select **LS Certificate** under **SETTINGS** in the **Control Panel** page.
   The **TLS Certificate** window is displayed.



Note: On installing the portal you have a trial license and self-signed certificate.

3. Click **REQUEST CERTIFICATE**.

   The **Create a Certificate Request** window is displayed.



4. In the Domain Name field, enter the domain name for which you want to request a certificate.

   The value entered must match the type of certificate you chose to use. For example, if you chose a wildcard certificate, the domain name might be `*.example.com`
   If you chose a domain certificate, the domain name might be `company01.example.com`, where *company01* is the name of your virtual portal.
   If multiple virtual portals are configured, each virtual portal has its own DNS name. In this case, the TLS certificate should be a wildcard certificate with an asterisk before the DNS suffix, for example, `*.example.com`
   If you have only one portal, and do not intended to configure multiple virtual portals, then use a regular TLS certificate and not a wildcard certificate.
   To request a certificate that specifies multiple alternative names, type the multiple names in this field, separated by semicolons (;). The certificate will include the `subjectAltName` certificate extension.

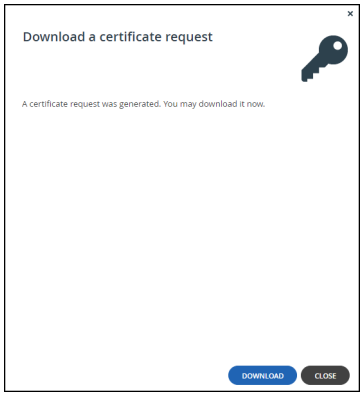
5. Optionally, specify the following:

   Organizational Unit – The name of your organizational unit.
   Organization – The name of your organization.
   Email – Your email address.
   City – Your city.
   State – Your state.

Country – Your country.

6. Click **GENERATE**.

   A key pair is generated and stored on the portal.
   The **Download a certificate request** screen is displayed.

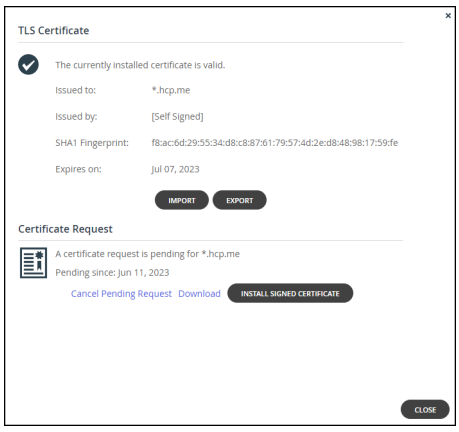


7. Click **DOWNLOAD**.

   The certificate request file *certificate.req* is downloaded to your computer.

8. Click **CLOSE**.

   The **Certificate Request** area of the **TLS Certificate** window indicates that the certificate request is pending.



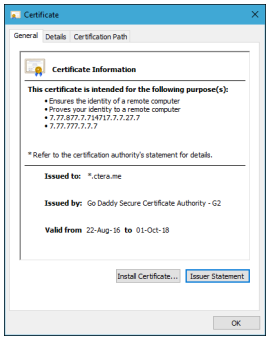
Warning: **When you generated the CSR, a private.key file was registered in the HCP Anywhere Enterprise Portal. If you now generate a new CSR, it will override the existing private.key file, and signing the old CSR will result in an error message indicating that the CSR does not match the private.key file. Therefore, do not generate a new CSR before installing the signed certificate.**

Sign the Certificate Request

To sign the certificate request:

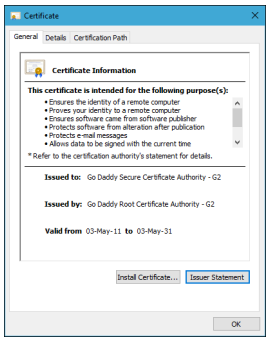
1. Send the `certificate.req` file you generated to your certificate authority for signing.
   If the request is successful, the certificate authority will send back an identity certificate that is digitally signed with the certificate authority's private key.
   Note: The certificate authority should return a base-64 encoded identity certificate.

2. Open the identity certificate and verify that the **Issued to** field includes the DNS suffix you provided upon creating the certificate request.



3. Build a certification chain from your identity certificate to your trusted root certificate.

   You need to obtain all of the intermediate certificates, as well as your root certificate authority's self-signed certificate.
   If you are using a well-known certificate authority, the intermediate certificates and the root certificate authority's self-signed certificate can be downloaded from your certificate authority website. If you are using your own internal certificate authority, contact the necessary entity to provide you with the required intermediate and self-signed certificate.
   In the above example, the certificate was issued by **Go Daddy Secure Certification Authority** to .hcp.me . To build the certification chain, obtain a certificate issued to **Go Daddy Secure Certification Authority**.



   To continue the certification chain, you must obtain a certificate issued to the same authority that the previous certificate was issued by. You continue the chain until the certification chain is complete, with the last certificate, which is a self-signed certificate, issued to and by the same entity.

Validate and Prepare Certificates for Upload

To validate and prepare certificates for upload:

1. Verify that none of the certificates in the certificate chain are corrupted or using invalid encoding.
   To do so, open each certificate in a program such as Notepad or Word, and verify that it contains the following:

```
-------- BEGIN CERTIFICATE -------
<CERTIFICATE CONTENT>
-------- END CERTIFICATE -------
```

2. Change the identity certificate issued to `*.hcp.me` to `certificate.crt`
3. Change the file extension of the other certificates in the certificate chain to `crt`

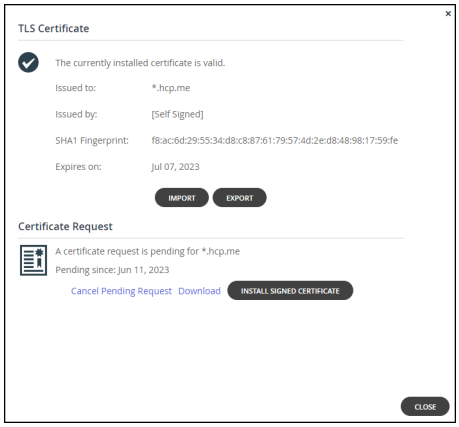
   For example, c`ertificate-name.crt`
4. Archive all of the certificates, the identity certificate, the intermediary certificates, and the root self-signed certificate, in a ZIP file called `certificate.zip`.

Install the Signed Certificate on HCP Anywhere Enterprise Portal

If you have a valid signed certificate, install it and replace the built-in certificate.

1. In the global administration view, select **Settings** in the navigation pane.
2. Select **TLS Certificate** under **SETTINGS** in the **Control Panel** page.

   The **TLS Certificate** window is displayed.

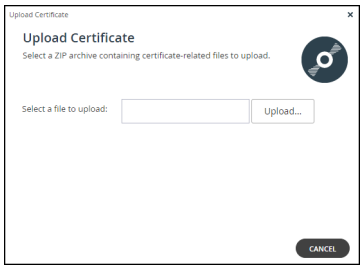


   The **Certificate Request** area of the TLS Certificate window indicates that the certificate request is pending.

   Note: To cancel a pending request, for example, to make changes to the current certificate request, click **Cancel Pending Request** and click **YES** in the confirmation window that is displayed.

   The pending certificate request is canceled.
3. Click **INSTALL SIGNED CERTIFICATE**.

   The **Upload Certificate** window is displayed.



   Click **Upload** and browse to the certificate.zip file you created. All the certificates in the certificate chain must be in the ZIP file in X.509 format, and each file must have a ".crt" extension.

   The certificate is installed on HCP Anywhere Enterprise Portal.
4. Click **FINISH**.
5. Restart all the HCP Anywhere Enterprise Portal servers via the **Main > Servers** page. See

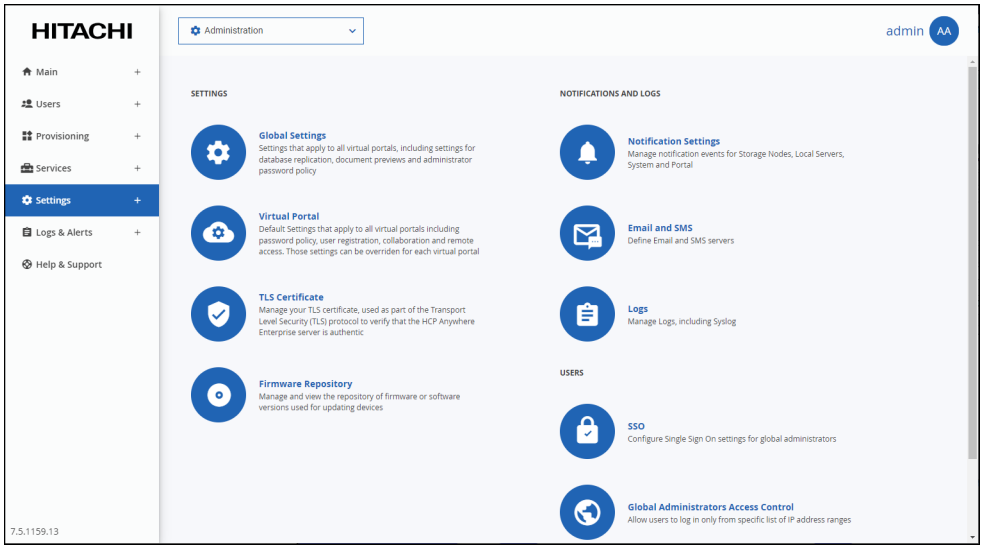
Restarting a Server from the User Interface. You can start the servers in any order.

6. Open the HCP Anywhere Enterprise Portal.
   If the certificate update was successful, there won't be any security exceptions.

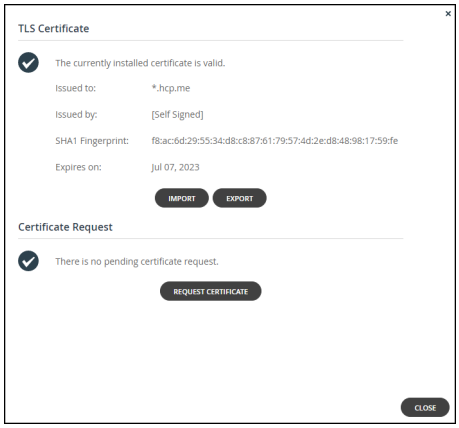
Importing a TLS Certificate

To import a TLS certificate:

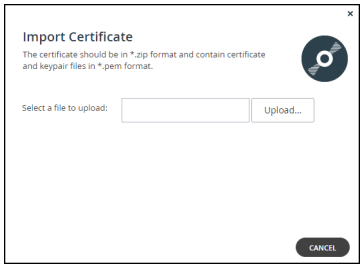
1. In the global administration view, select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.



2. Select **LS Certificate** under **SETTINGS** in the **Control Panel** page.
   The **TLS Certificate** window is displayed.



3. Click **IMPORT**.
   The **Import Certificate** window is displayed.



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

Creating DNS Records

The HCP Anywhere Enterprise Portal includes a built-in DNS server. This server automatically resolves the domain names of all the defined virtual portals, as well as names of devices using the remote access service. In order for this DNS server to work, you must register it using an NS (Name Server) record on your DNS server.

The procedure used for configuring the DNS for remote access depends on the whether you have purchased a dedicated domain (the DNS suffix includes only records for the HCP Anywhere Enterprise Portal) or not (the DNS suffix includes records that are unrelated to the HCP Anywhere Enterprise Portal).

If you have a dedicated domain:

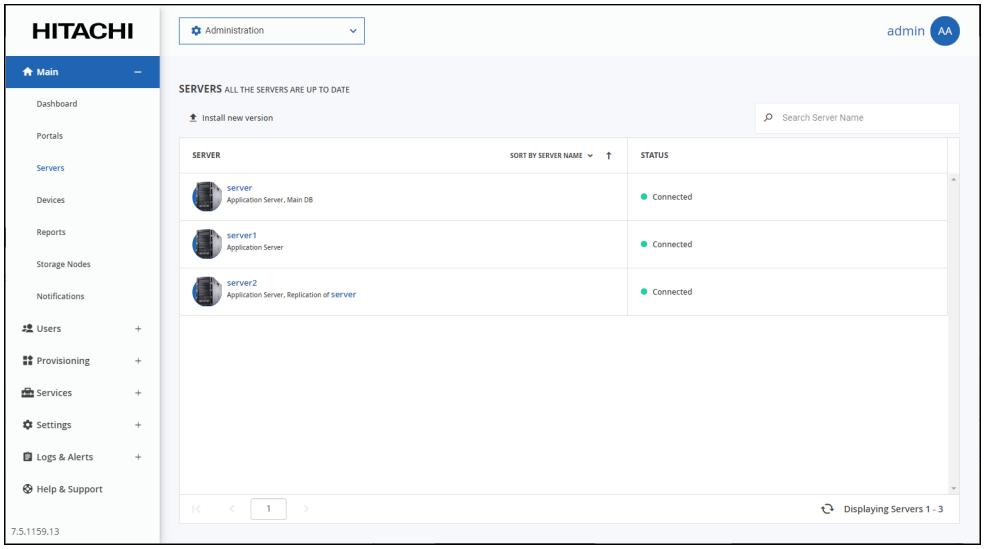
- If you have a dedicated domain for the HCP Anywhere Enterprise Portal – no servers other than the HCP Anywhere Enterprise Portal – then the NS record can be created just once, in that zone.
  For example, for a DNS suffix called *storage.example.com* and two HCP Anywhere Enterprise Portal servers with IPs 123.168.0.3 (primary) and 123.168.0.4 (secondary), you would register:
  ```
  A          srv1.example.com          192.168.10.3
  A          srv2.example.com          192.168.10.4
  ```
  Next, you would create an NS record for each server to the zone *storage.example.com*:
  ```
  NS       storage.example.com       srv1.example.com
  NS       storage.example.com       srv2.example.com
  ```

Configuring a Public NAT Address

Immediately after deploying a HCP Anywhere Enterprise Portal instance, the HCP Anywhere Enterprise Portal server will respond to DNS requests with its private internal IP address. In order to make the HCP Anywhere Enterprise Portal available via the Internet, and to enable the HCP Anywhere Enterprise Portal to respond to DNS queries with the public IP address, you must configure the HCP Anywhere Enterprise Portal's public NAT address.

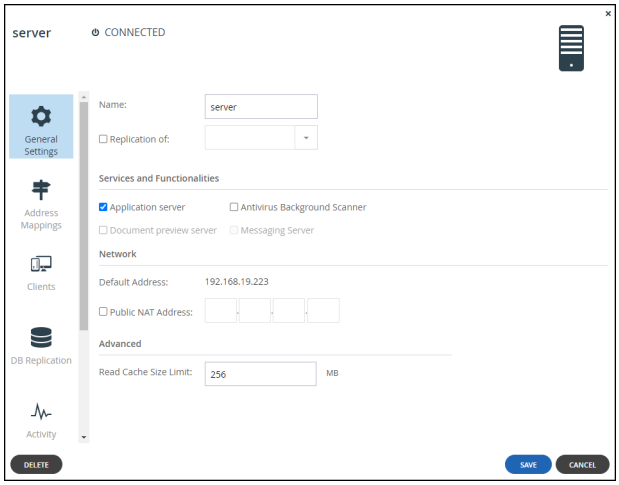
To configure a Public NAT address:

1. In the global administration view, select **Main > Servers** in the navigation pane.
   The **SERVERS** page is displayed, listing all the servers for the HCP Anywhere Enterprise Portal.



2. Click the server to edit.

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



3. Check **Public NAT Address** and enter public IP address.
4. Click **SAVE**.

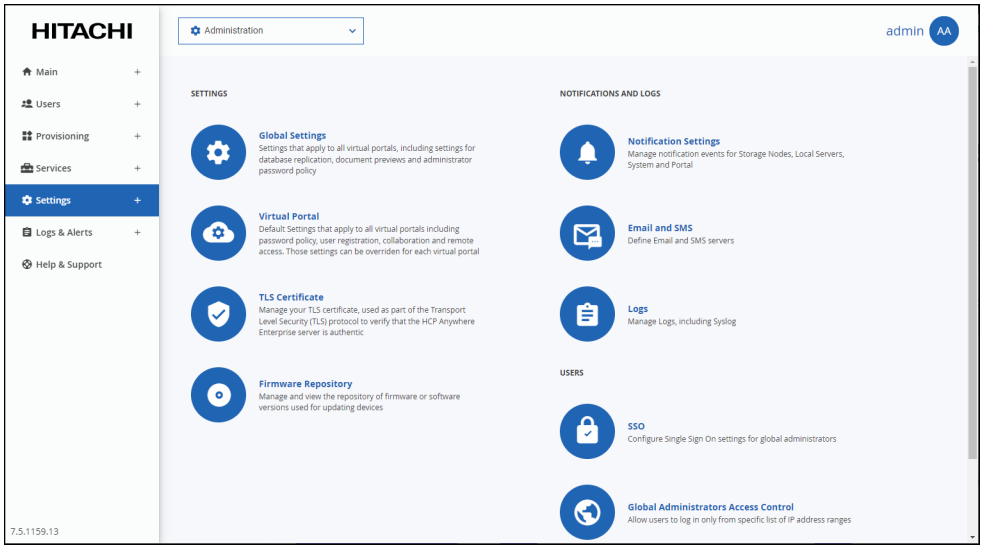
Setting Up the Time Zone and Configuring NTP

Note: HCP Anywhere Enterprise Portal is pre-configured with NTP servers. If you want to use different NTP servers, Hitachi Vantara provides the following procedures.

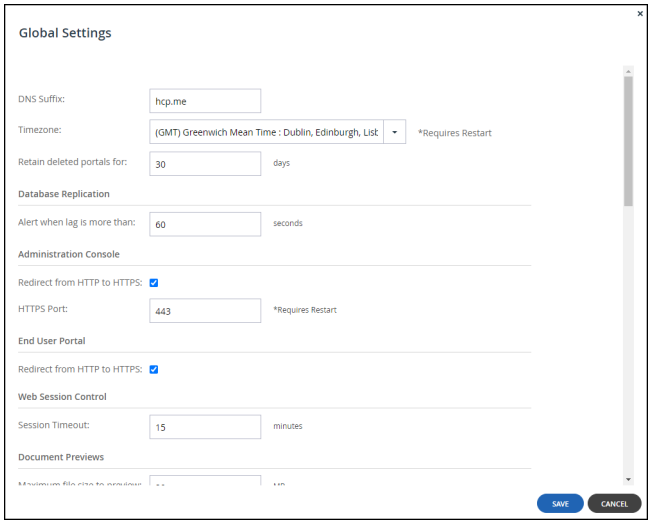
You can configure the time zone for the HCP Anywhere Enterprise Portal. If for whatever reason, the HCP Anywhere Enterprise Portal clock and HCP Anywhere Enterprise Edge Filer clocks are not synced, you can configure the HCP Anywhere Enterprise Portal NTP server, as described below.

To configure the HCP Anywhere Enterprise Portal server's time zone:

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



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



3. Select the correct time zone for the HCP Anywhere Enterprise Portal from the list.
4. Click **SAVE**.
5. Restart the server as described in Restarting a Server from the User Interface.

To configure NTP in the HCP Anywhere Enterprise Portal server:

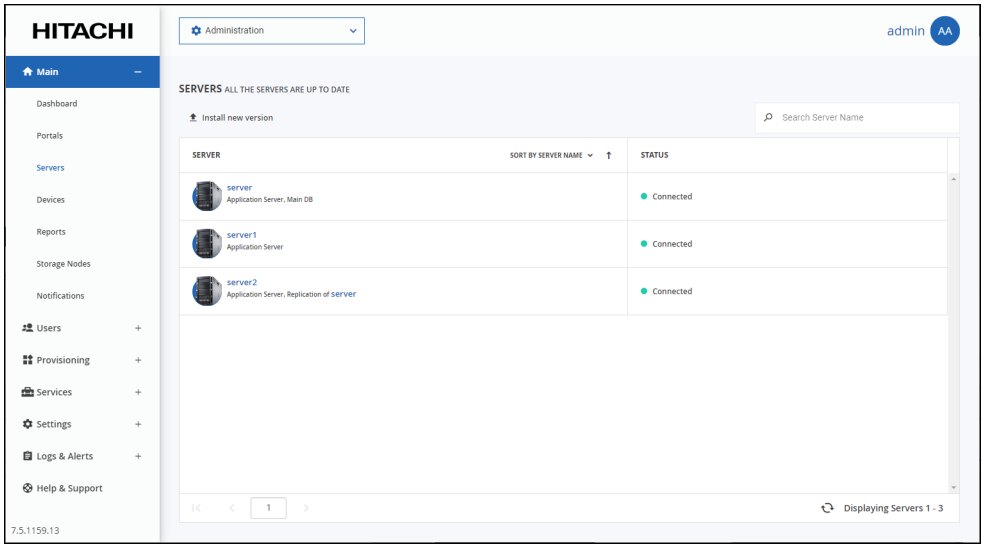
1. Log in as **root**, using SSH to the portal server.
2. Run the command to start the date service: `systemctl start ntpdate.service`
3. Run the command to start the NTP server: `ntpdate <time-server>`
4. Run the command to restart the date service: `systemctl restart ntpdate.service`

Restarting a Server from the User Interface

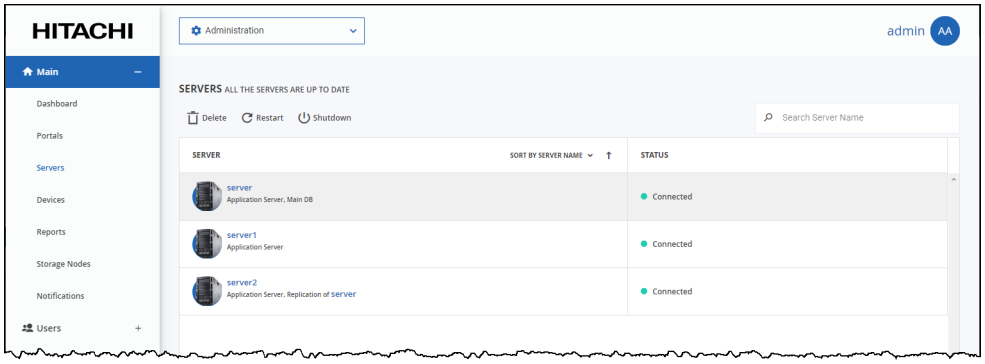
HCP Anywhere Enterprise Portal servers can be restarted from the HCP Anywhere Enterprise Portal user interface.

To restart a server:

1. In the global administration view, select **Main > Servers** in the navigation pane.
   The **SERVERS** page is displayed, listing all the servers for the HCP Anywhere Enterprise Portal.



2. Select the server to restart and click **Restart**.



   A confirmation window is displayed.
3. Click **RESTART** to confirm.

The server is restarted.

Chapter 4. Installing Additional HCP Anywhere Enterprise Portal Servers

All servers except the primary server are additional servers.

You install additional servers using the same procedure you used to install the primary server, except for the following:

- For messaging servers, you require 4 vCPU, 32GB RAM, and 250GB data pool (Magnetic).
- For a preview server, you require 4 vCPU, 16GB RAM,and 60GB data pool (SSD).
- For all other application servers, you require 4 vCPU, 16GB RAM, and 100GB data pool (Magnetic).

Installing an additional server involves installing a server as described in *Installing HCP Anywhere Enterprise Portal Instances* and then configuring it as an additional server.

By default, HCP Anywhere Enterprise portal servers are application servers running no other service.

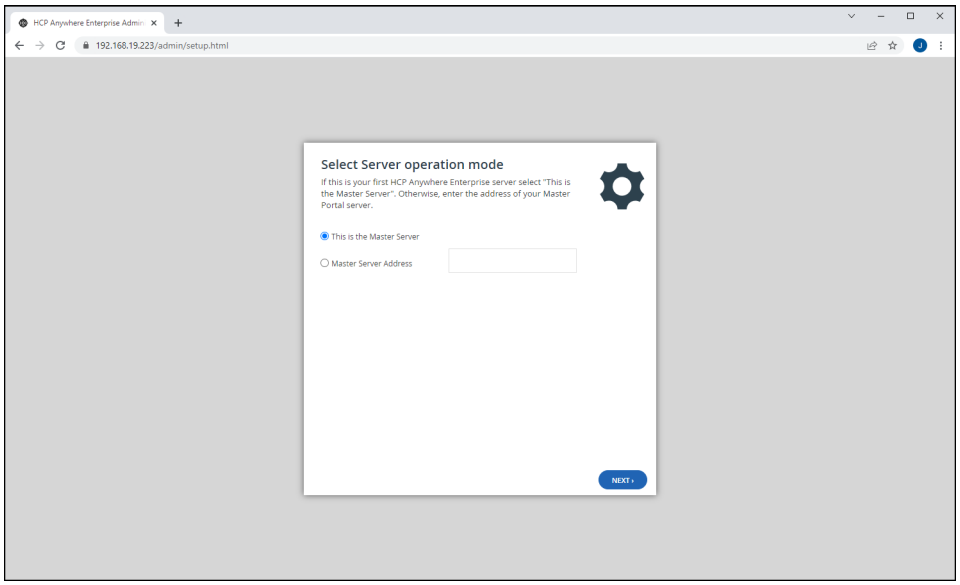
Following initial setup, you can enable or disable the application service through the HCP Anywhere Enterprise Portal web interface. For details, see the *Hitachi Content Platform Anywhere Enterprise Portal Global Administration Guide*.

Note: For document previews to work, you must install at least one document preview server.

To configure an additional server:

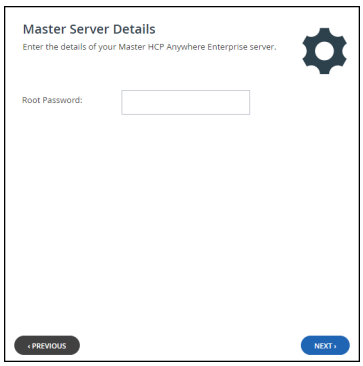
Note: If the HTTPS administration port was changed on the primary server, you must enable the relevant port on all servers.

1. Using a Web browser, browse to the new server, via the IP address or DNS.
   The **Setup** wizard opens, displaying the **Select Server operation mode** window.



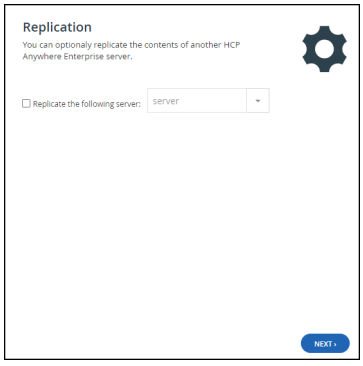
2. Choose **Master Server Address** and enter the address of the primary server.
3. Click **NEXT**.

   The **Master Server Details** window is displayed.



4. Enter the root password for the primary server. The default is `%1Change:Me0`, but this should have been changed on first access to the server.
5. Click **NEXT**.

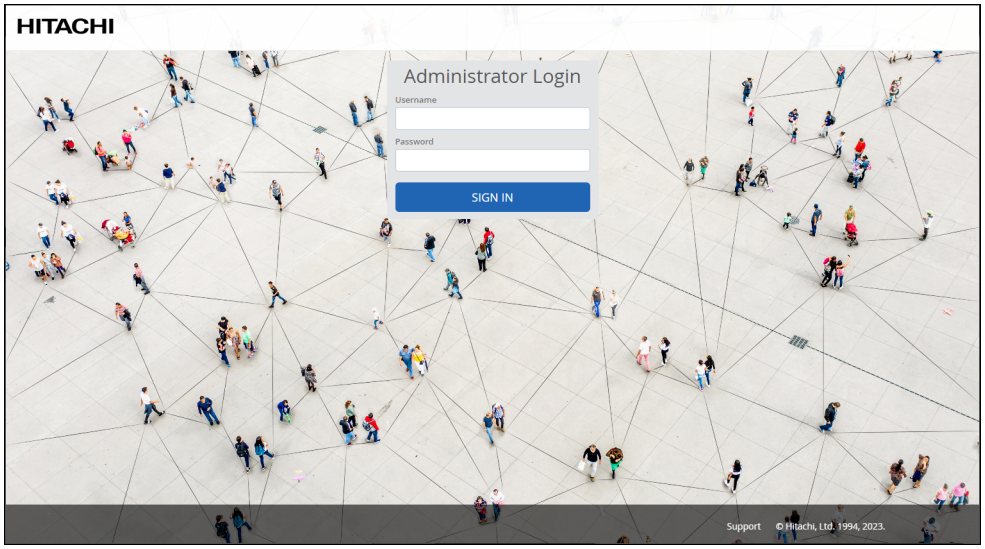
   The **Replication** window is displayed.



6. To configure this server as a replica of the main database, select the **Replicate the following server** check box, and then select the server you want to replicate in the drop-down list.
7. Click **NEXT**.

   The wizard completes and a success message is displayed.
8. Click **OK**.

   HCP Anywhere Enterprise Portal opens, displaying the **Administrator Login** page.

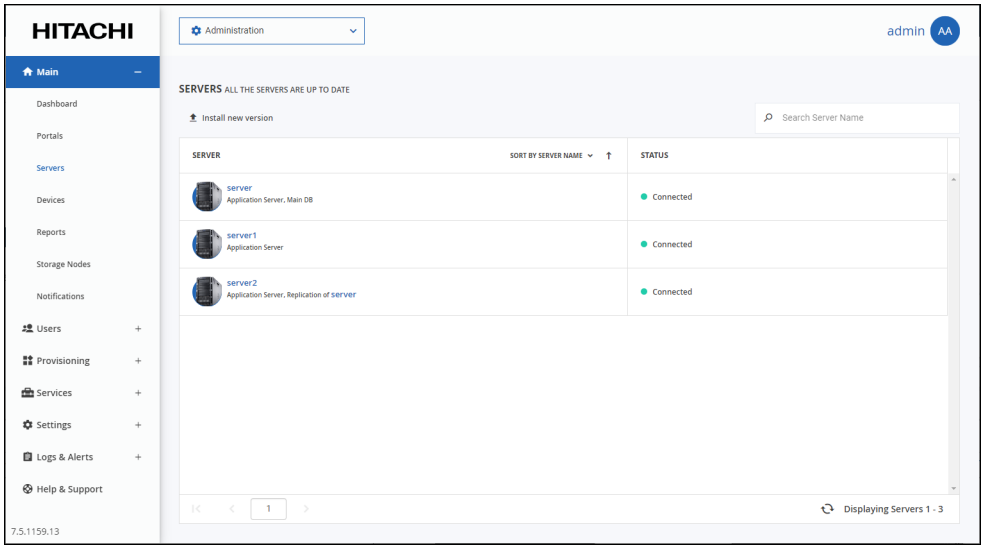


9. Enter the user name and password and click **SIGN IN**.

   The portal opens, displaying the **Main > Dashboard** page. By default, HCP Anywhere Enterprise Portal creates a team portal called *portal*. For information about how to rename, view and edit this portal, or create additional team or reseller portals, see the *Hitachi Content Platform Anywhere Enterprise Portal Global Administration Guide*.

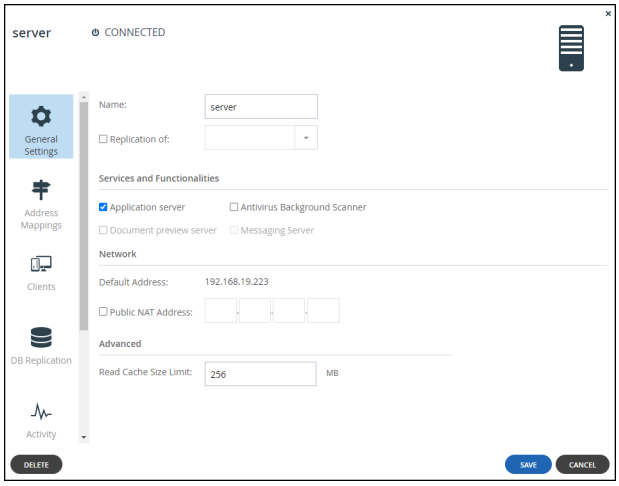
10. In the global administration view, select **Main > Servers** in the navigation pane.

    The **SERVERS** page is displayed, listing all the servers for the HCP Anywhere Enterprise Portal.



11. Click the server to edit.

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



12. Check the boxes of the services to be provided by this server, for example, as a document preview server.
13. Click **SAVE**.

Chapter 5. Configuring HCP Anywhere Enterprise Portal Database for Backup and Restore

In this chapter

Backing Up the HCP Anywhere Enterprise Portal

To back up the HCP Anywhere Enterprise Portal servers and storage you need to use third-party recovery tools.

For HCP Anywhere Enterprise Portal database backup, see Backing Up the HCP Anywhere Enterprise Portal Database.

Using third-party tools can result in a recovery after a disaster not being consistent with the database with the recovery being either older or newer than the database recovery.

If the portal recovery is older than the database, it will be missing some recent blocks. In this situation, you should rollback the database to an earlier point-in-time that matches the latest portal recovery.

If the portal recovery is newer than the database, since deleted blocks are kept for a minimum of 30 days and these blocks are never modified, as long as the database is no more than 30 days older, there will be no data loss.

Note: Running HCP Anywhere Enterprise FSCK is usually recommended following a disaster recovery. HCP Anywhere Enterprise FSCK must be run only with approval from Hitachi Vantara support.

Backing Up the HCP Anywhere Enterprise Portal Database

HCP Anywhere Enterprise Portal uses PostgreSQL to store metadata. This database must be backed up to ensure continued use of HCP Anywhere Enterprise Portal in order to ensure data and metadata persistence and consistency on the HCP Anywhere Enterprise platform, and to keep Recovery Time Objective (RTO) and Recovery Point Objective (RPO) values to a minimum.

Calculating the Minimum Space Required for the Database Backup

The archive pool must be at least double the data pool.

For example, if the primary database uses 1TB storage and a secondary, replication, database uses another 1TB, then each of these databases require 2TB for backup. The total storage must be at least 6TB: 1TB for the primary database, 1TB for the secondary database and 4TB for the primary and secondary backups (2TB for each backup).

See the following procedures:

Using PostgreSQL Continuous Archiving – HCP Anywhere Enterprise Portal uses PostgreSQL's built-in continuous archiving mechanism to enable you to roll back to an older version of the portal database.

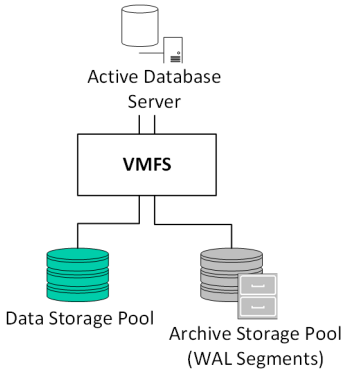
Using PostgreSQL Streaming Replication – Streaming replication enables the continuous streaming and replication from a primary database server to a secondary, replication, server.

Using PostgreSQL Continuous Archiving

HCP Anywhere Enterprise Portal uses PostgreSQL's built-in continuous archiving mechanism, known as Point-In-Time Recovery (PITR).

After backing up the database for the first time, the base backup, Incremental backups of the database are performed using Write Ahead Log (WAL) files, which include all the database transactions and changes. Running a base backup and incremental backups is non-disruptive: the database continues running, without losing any data.

The following diagram illustrates continuous archiving and point-in-time recovery:



Using WAL logs has the following major benefits:

- Ensures data integrity
- Significantly reduces the number of disk writes

Note: The HCP Anywhere Enterprise Portal database WAL files are located in $pgdatadir/pg_wal which is commonly called the WAL directory.
The WAL file size is 16MB. Once a WAL file reaches 16MB, a new WAL file is created.
The maximum number of WAL files stored in the WAL directory is 128. This means that the WAL directory size can reach 16 (MB) * 128 (files) = 2GB.
When the 128-file threshold is reached, WAL files are recycled.

The database base backup and WAL logs are compressed upon backup:

- The base backup is typically 20%-30% of the size of the original database size. By default, there are always two base backups in the archive pool so the archived base backups typically consume around 40%-60% of the original database size.
- An archived WAL file size is typically 20% the size of the original WAL file.

Configuring PostgreSQL Continuous Archiving

To configure PostgreSQL continuous archiving:

1. Using SSH, log in as `root` to your HCP Anywhere Enterprise Portal primary database server.
2. In the command line, enter the following command to configure the maximum number of days to keep the backups: `portal.sh configure-db-recovery backup-history-days`

   Where *backup-history-days* is the number of days you want to retain a base backup archive before a new one is created. For example, to retain an archive for seven days, run: `portal.sh configure-db-recovery 7`
   An initial base backup of the database is created and the next backup is scheduled based on the backup-history-days parameter. Starting from the second base backup, the first scheduled base backup, there is always two base backups in the archive pool. WAL files are created after the first base backup. When a scheduled base backup is performed, the new base backup replaces both the old base backup that exceeded the backup-history-days, as well as the WAL files created in the period of time between the old base backup and the new base backup.

   Warning: The minimum retention period recommended by Hitachi Vantara is 7 days. If you set the retention period to less than 7 days, you must also have a secondary backup method in order to protect the portal from disasters.

When the command finishes successfully a message is displayed, similar to the following:

```
NOTICE: pg_stop_backup complete, all required WAL segments have been
archived
Done
```

You can roll back to any older version of the database up until the previous base backup.

Note: You can change the backup-history-days parameter at a later date using the command `portal.sh set_archive_history_days history-days`

Rolling Back PostgreSQL Continuous Archiving to a Previous Point-in-Time

Note: Hitachi Vantara recommends reverting a database only with the help of Hitachi Vantara support.

After continuous archiving has been set up, you can roll back to an older version of the portal database.

Note: If the database has become corrupted and it is not just the data that you want to roll back, you need to revert the primary database to a snapshot.

To roll back PostgreSQL continuous archiving to a previous point in time:

1. Using SSH, log in as `root` to the HCP Anywhere Enterprise Portal primary database server.
2. In the command line, enter the following command to view the oldest time possible to roll back to: `portal.sh db-rollback -p`
3. Enter the following command to roll back to a point in time within the available backup range: `portal.sh db-rollback -r "point-in-time"`

   Where *point-in-time* is the desired point in time, in the format YYYY-MM-DD hh:mm:ss. For example: `portal.sh db-rollback -r "2023-11-06 00:23:21"`

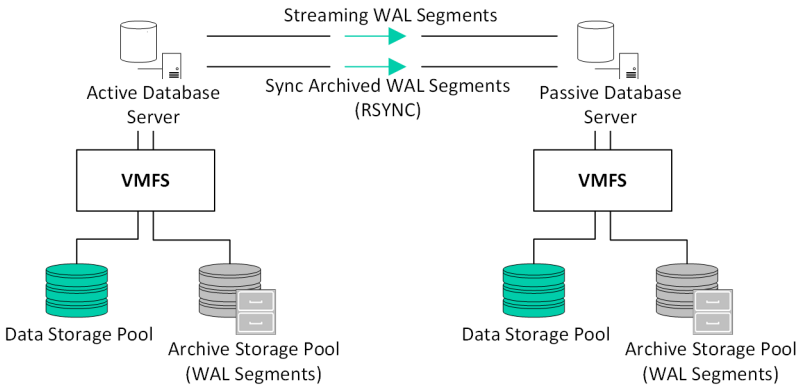
   Note: If the HCP Anywhere Enterprise Messaging service was setup after the rolled back point-in-time, the messaging service status will be grey, as if messaging is not configured, and all existing messaging data will be lost.
4. When rolling back a primary database server, from which a replication server is streaming,

described in Using PostgreSQL Streaming Replication, restart the HCP Anywhere Enterprise Portal on the secondary database server, the replicating server, by running: portal-manage.sh restart

Using PostgreSQL Streaming Replication

Streaming replication enables the continuous streaming and replication of WAL segments from the WAL directory and archived WAL segments from the primary database server to a secondary database server.

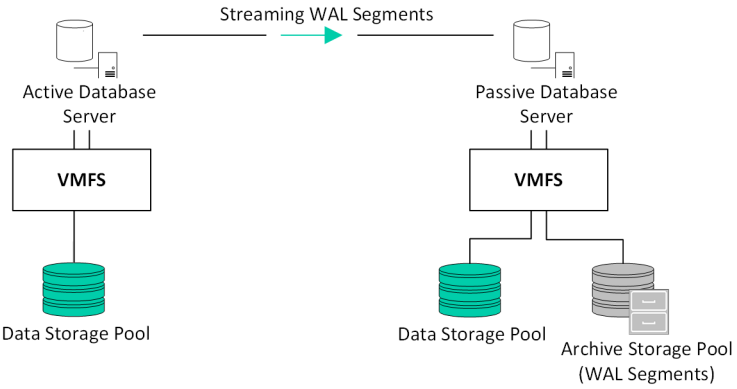
The following diagram illustrates streaming replication with continuous archiving and point-in-time recovery:



Note: Syncing archived WAL segments is done only on the first setup of the replica.

This process is complementary to configuring continuous archiving. It protects against failures occurring on the primary database server, by streaming the WAL directory and synchronizing the database's archived WAL logs to a secondary database server.

Note: You can also configure the replication so that the archive pool is on the passive, secondary, database and not the active database server with point-in-time recovery on the secondary.



Configuring PostgreSQL Streaming Replication

The secondary server continuously streams the primary server's WAL segments, and synchronizes the primary database server's archived WAL segments every 10 minutes. Streaming replication

traffic runs on TCP port 5432, which means you must open these ports for communication between the primary and secondary database servers. The secondary HCP Anywhere Enterprise Portal database server acts as a standby/passive server and cannot be used for load balancing purposes.

Note: The allocated disk space for the PostgreSQL archive pool must be at least twice the size of the storage space allocated for the HCP Anywhere Enterprise Portal data pool, as described in Calculating the Minimum Space Required for the Database Backup.
The locations of the streaming and archived WAL segments are $pgdatadir/pg_wal and $DBarchive respectively.

To configure streaming replication:

1. Using SSH, log in as `root` to your HCP Anywhere Enterprise Portal secondary, replication, server.
2. Do one of the following:
   - If the secondary, replication, server has not been initialized, browse to the server's IP address or public DNS.
   - If the secondary, replication, server has been initialized but without replication, and you want to set it up as a replication server, open an SSH session to the HCP Anywhere Enterprise Portal secondary, replication, server, by running the following command:
     `portal-manage.sh resetdb`

     Warning: You must not run `portal-manage.sh resetdb` on the primary database server as this will delete all the data from the database.

   The **Setup** wizard opens, displaying the **Select Server operation mode** window.
3. Set the server as a replication of the primary database server.

   Note: After completing the setup wizard on an already initialized server, a new server entry is created representing the newly configured server. This makes the old server entry obsolete. You can remove the obsolete server entry by doing the following:

   a) Log in to the HCP Anywhere Enterprise Portal as a global administrator.
   b) In **Main > Servers** locate the obsolete server entry, displayed as *Not Connected*.
   c) Select the server and click **Delete**.
4. Log in as root to the HCP Anywhere Enterprise Portal replication server instead of the primary database server.

Failing Over PostgreSQL Streaming Replication to the Secondary Database Server

The secondary database acts as a passive database, meaning it can only process read requests. In the event that the primary database fails, you have to fail over to the secondary database server, making it active, in order to assure proper continuity of the platform.

Note: You can also switch between the primary and secondary database servers, making the secondary database server the primary database server and the primary database server a secondary server, when the primary database server is still up.

To failover to the secondary server:

1. Using SSH, log in as `root` to the HCP Anywhere Enterprise Portal secondary database server.
2. In the command line, enter the following command: `portal-failover.sh become_master`

The primary database server becomes the secondary server, and the secondary database server becomes the primary server.

Failing Back to the Primary Database Server

When the original primary server comes back online you can failback to it, to return to the original configuration.

To failback to the primary database server:

1. When the former primary database server is running again, using SSH, log in as root to the original primary database server.
2. In the command line, enter the following command: `portal-failover.sh become_master`

Log in to the portal as a global administrator and In the global administration view, select **Main > Servers** in the navigation pane and click the replication server name. Click **DB Replication** in the server window that is displayed and under **Database Replication** verify that the **Status** value is set to **OK**.

Note: If there is a mismatch between the requested WAL files and their location on the server the Status value can be set to Failed until the mismatch is resolved when the WAL file position reaches the location, which can take a few hours. Hitachi Vantara recommends the following manual procedure to resolve this issue:

a) Log in to the portal as a global administrator and In the global administration view, select **Main > Servers** in the navigation pane.
The **SERVERS** page is displayed, listing all the servers for the HCP Anywhere Enterprise Portal.

b) Click the replication server name and in the server window that is displayed, under **General Settings**, uncheck **Replication of**.

c) Click **SAVE**.

d) Click the replication server name again and in the server window that is displayed, under **General Settings**, recheck **Replication of**.

e) Click **SAVE**.
The replication process will reinitialize which can be monitored by clicking DB Replication in the server window and under Database Replication verify that the Status value is set to Reinitializing. After the replication has reinitialized, which can take some time, depending on the portal size and the amount of data to be replicated, and the Status value is set to OK.

Monitoring the Database Backup and Streaming Replication

You can monitor every database backup and replication component running on the server, including:

- Streaming replication
- Base backup
- WAL archive (continuous archive)

Monitoring Database Backup and Replication from the Notifications Pane

To monitor database backup and replication from the NOTIFICATIONS page:

- In the global administration view, select **Main > Notifications** in the navigation pane.
  The **NOTIFICATIONS** page is displayed.
  Any alerts related to database backup or streaming replication are displayed.

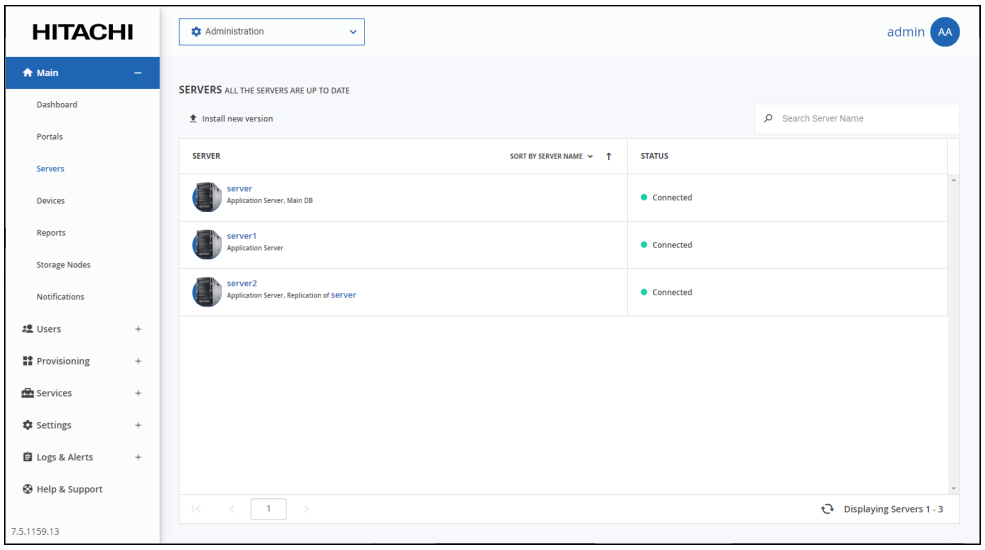
Monitoring Database Backup and Replication from the Server Task Manager

f streaming replication is set up, you can monitor it from the Server Task Manager. The HCP Anywhere Enterprise Portal runs a task every few minutes to verify that replication is working as expected. If any issues are detected, the task fails, and the HCP Anywhere Enterprise Portal displays an appropriate notification in the **NOTIFICATIONS** page, and also sends an email alert to the portal administrators.

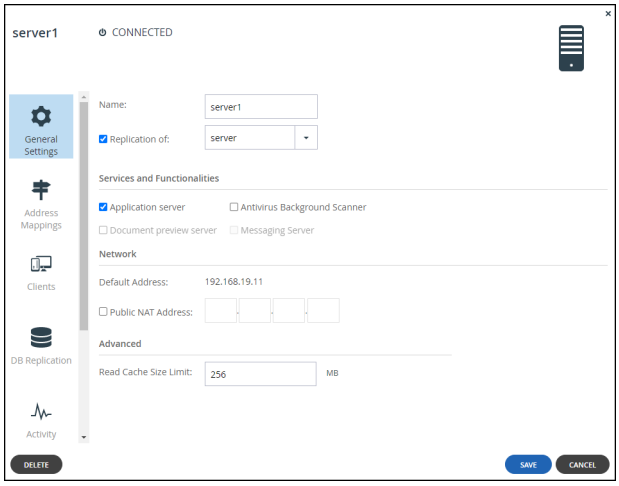
Note: The task runs the `portal.sh replication_status` command and analyzes the output. For more information see Monitoring Database Backup and Replication from the Server Console.

To monitor database backup and replication from the Server Task Manager:

1. In the global administration view, select **Main > Servers** in the navigation pane.
   The **SERVERS** page is displayed, listing all the servers for the HCP Anywhere Enterprise Portal.

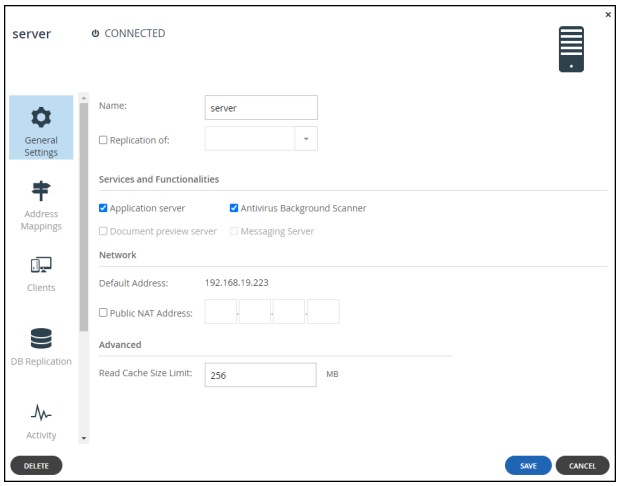


2. Click the replicating secondary server name.
   The server window is displayed with the server name as the window title.



3. Click the **DB Replication** option.

   The HCP Anywhere Enterprise Portal reports the status of its scheduled base backups and transaction log archiving process, as well as additional metrics to help detect when database replication falls behind due to lags in the process. In the event that replication falls behind, HCP Anywhere Enterprise Portal administrators are notified via email. The relevant email templates are *Replication setup failed* and *Replication has errors*.



Monitoring Database Backup and Replication from the Server Console

You can view the status of each database backup and replication component.

To monitor database backup and replication from the server console:

Note: This procedure can be performed on both the primary server and on secondary servers.

1. Using SSH, log in as `root` to the HCP Anywhere Enterprise Portal primary database server or secondary database server.
2. Run the following command: `portal.sh replication_status | json_reformat`

   The output is displayed in JSON format. For example:

   ```
   {
   ```

```
  "streaming_replication": {
    "status": "ok",
    "lastSuccess": "256KB"
  },
  "base_backup": {
    "status": "ok",
    "lastSuccess": "none"
  },
  "wal_archive": {
    "status": "failed",
    "lastSuccess": "3 hours"
  }
}
```

Both the primary and secondary servers have the same output structure. However, the fields have slightly different meanings:

Field	Primary Server	Secondary Server
streaming_replication		
status	Indicates whether a secondary server is streaming from the primary server: **ok** – Streaming replication is running. **failed** – Streaming replication failed. **not configured** – Streaming replication is not configured on this server.	Indicates whether this server is streaming from the primary server: **ok** – Streaming replication is running. **failed** – Streaming replication failed.
lastSuccess	The difference in size (in KB) between the last sent WAL segment and the secondary server's last checkpoint, a point in the WAL logs at which all data files have been written to the disk. In other words, the amount of data the primary database sent to the secondary database, which has not been processed by the secondary database.	The difference in size (in KB) between the last received WAL segment and the secondary server's last checkpoint, a point in the WAL logs at which all data files have been written to the disk. In other words, the amount of data the primary database sent to the secondary database, but which has not been processed by the secondary database. If the value is `none`, then the secondary database is up to date.
base_backup		
status	Indicates whether the last base backup was completed successfully: **ok** – Last base backup completed successfully. **failed** – Last base backup failed. **not configured** – Base backup is not configured for this server. This means that continuous archiving was not configured on the server.	Indicates whether the last base backup was completed successfully: **ok** – Last base backup completed successfully. **failed** – Last base backup failed.

Field	Primary Server	Secondary Server
lastSuccess	The last time a successful backup was run (in days). If the value is `none`, the `status` field is `ok`, and the last base backup was completed successfully.	
wal_archive		
status	Indicates whether a WAL was successfully archived in the past hour: **ok** – WAL directory was archived successfully in the past hour. **failed** – WAL directory was not archived in the past hour. This does not indicate a problem. You can change the status to `ok`, by running a manual command that forces archiving. For more information, contact Hitachi Vantara support. **not configured** – WAL archiving, that is continuous archiving, is not configured on this server. Archiving occurs after 16MB of data has been written or during a system restart.	Indicates whether a WAL was successfully synchronized in the past hour: **ok** – WAL directory was synchronized successfully in the past hour. **failed** – WAL directory was not synchronized in the past hour.
lastSuccess	The last time a WAL log was archived successfully (in hours). If the `status` field's value is `ok`, then `none` is output.	

3. Run the following command on the secondary server to view the secondary archive synchronization log: `portal-log.sh replication [-f]`

   Include the `-f` flag to display the log in the command window. Otherwise, the log is displayed in vim.

Reverting the Primary Database to a Snapshot

Note: Hitachi Vantara recommends reverting a database only with the help of Hitachi Vantara support.

When reverting a HCP Anywhere Enterprise Portal primary database to a previous snapshot, any files synced to the portal after the time of the snapshot **are missing in the HCP Anywhere Enterprise Portal**. This data is never synced to the portal when the devices are reconnected to the portal unless they physically existed on a device and not just as a stub file.

Note: Even though the data is no longer available, it will still be displayed as stub files on edge filers. You can use these stub files to identify the data that was added to the portal after the revert date. These files should be deleted from the edge filer. As long as the stub files exist on the edge filer, the sync status will indicate that there is a sync error.

You have to revert to a snapshot of the virtual machine when the actual database has become corrupted and not the data itself. If it is only the data that needs reverting to a previous point-in-time, rollback the database, as described in Rolling Back PostgreSQL Continuous Archiving to a Previous Point-in-Time. When you rollback the database to a previous point-in-time, after

continuous archiving has been set up, any files synced to the portal from the time of the database is rolled back to, to the present are synced when the devices are reconnected to the portal.

To ensure the portal and devices are synced after reverting to a snapshot:

Warning: This procedure must be performed immediately after reverting to the snapshot and before connecting any device to the portal.

1. Suspend syncing on all devices connected to the portal.
2. Roll back the HCP Anywhere Enterprise Portal primary database, as described in Rolling Back PostgreSQL Continuous Archiving to a Previous Point-in-Time.
3. Using SSH, log in as `root` to every HCP Anywhere Enterprise Portal application server except for the primary database server.
4. In the command line of every HCP Anywhere Enterprise Portal application server except for the primary database server, enter the following command to stop the server:
   `portal-manage.sh stop`
5. Using SSH, log in as root to the HCP Anywhere Enterprise Portal primary database server.
6. Enter the following command to change the Portal UUID: `change-portal-gvsn`
7. Restart all the application servers you stopped using the following command:
   `portal-manage.sh start`
8. Resume syncing on all devices connected to the portal.

Chapter 6. Additional Functionality for HCP Anywhere Enterprise Portal Servers

In this chapter

Enabling Federal Information Processing Standard (FIPS)

The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules. Setting the HCP Anywhere Enterprise Portal to be FIPS compliant requires a HCP Anywhere Enterprise Portal restart and impacts performance.

To change the HCP Anywhere Enterprise Portal to be FIPS compliant, contact Hitachi Vantara support.

Enabling/Disabling Remote Support

You can enable remote assistance by the Hitachi Vantara support team, by using the `portal-support.sh` script. This script adds a user called "support", which the Hitachi Vantara Support Team can uses to remotely access and log in to your HCP Anywhere Enterprise Portal.

To enable remote support:

1. Using SSH, log in as `root` to the HCP Anywhere Enterprise Portal primary server.
2. In the command line, enter the following command: `portal-support.sh enable`

The **support** user is created.

To disable remote support:

1. Using SSH, log in as root to your HCP Anywhere Enterprise Portal primary server.
2. In the command line, enter the following command: `portal-support.sh disable`

The **support** user is deleted.

Chapter 7. ESXi Specific Management

In this chapter

Load Balancing HCP Anywhere Enterprise Portal Servers

General Load Balancing Best Practices

- Probing to test tomcat reachability: Most load balancers have a health check/probing mechanism that checks for ports and services availability. The best scenario is to only use port tests that check if the port is available (checking ports 995 and 443). If a more accurate probing is required, use port 995 probe. With HTTPS use: *portalurl*/admin/startup.
- It is not recommended to use source NAT on the load balancer as this makes it hard to monitor and troubleshoot networking issues, since all the connections come to the tomcat servers from the same IP. This will also open the possibility that the HCP Anywhere Enterprise Portal will be locked due to too many retries if any user gets his password wrong 3 times and it will affect all users since this mechanism is based on IP.

Using F5 Load Balancer

Note: If you are not using F5 software for load balancing, the basic principles outlined here can still be applied.

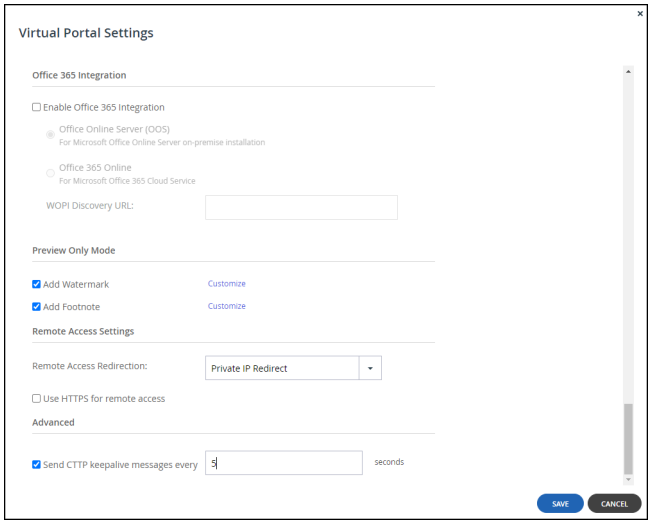
The following describes setting up load balancing based on F5 software. If your version of the F5 software is different to the version described below, contact Hitachi Vantara support for help with your configuration.

Note: Using F5 load balancing to perform SSL offloading requires the following configuration:

- Create an F5 iRule to add **Secure** and **HttpOnly** flags to the JSESSIONID cookie.
- Create an F5 iRule to add **HSTS** flags.
- Disable old insecure encryption algorithms like RC4.
- If F5 is configured to use TLS 1.0, you must change it.

The following best practices are recommended by Hitachi Vantara:

- Configure the **tcp** TCP protocol profile.
  - If **Idle Timeout** is configured, make sure the value is at least 5 minutes, 300 seconds, as HCP Anywhere Enterprise handles its own TCP sessions with keep alives.
  - If **Keep Alive Interval** is configured, make sure the value is greater than the value specified for **Send CTTP keepalive messages every** in the virtual HCP Anywhere Enterprise Portal settings. **Send CTTP keepalive messages every** prevents proxy or load balancer servers from preemptively terminating connection between a HCP Anywhere Enterprise Agent and the HCP Anywhere Enterprise Portal. Hitachi Vantara recommends setting **Send CTTP keepalive messages every** less than half the value specified for **Keep Alive Interval**.



- If **Zero window Timeout** is configured, make sure it is as high as possible. For example, 30000.
- Configure the **source_addr** Persistence profile.
- After setting the profiles, set up the load balancing for the HCP Anywhere Enterprise virtual servers.

Increasing the Data or Archive Pool Size

Note: Hitachi Vantara recommends changing the storage with the help of Hitachi Vantara Support.

To increase the storage:

1. For each HCP Anywhere Enterprise Portal instance you have installed, stop HCP Anywhere Enterprise services, by doing the following:
   a) Open an SSH session to the HCP Anywhere Enterprise Portal instance.
   b) Log in as `root` user.
   c) Run the command to stop the HCP Anywhere Enterprise Portal services:
   `portal-manage.sh stop`
2. In the vSphere Client console, right-click the HCP Anywhere Enterprise Portal virtual machine and click **Edit Settings**.
   The virtual machine settings are displayed.
3. In the **Virtual Hardware** tab, click select **Hard Disk** under **ADD NEW DEVICE**.
   A new hard disk is added to the settings.
4. Specify the disk size you want for the new disk.
5. Expand the **New Hard disk** item and for **Location** browse to the datastore you want to use for either the data pool or archive pool.
6. Select the disk to use.
7. Click **OK**.
   The new VMDK hard disk is added.
8. Log in as `root` over SSH to the HCP Anywhere Enterprise Portal server with the archive pool to increase.

9. Run the following command to identify the name of the device you attached: `fdisk -l`
10. Locate the device name according to its size and usage information.
11. Run the following command to extend the data pool: `portal-storage-util.sh extend_storage deviceName`

    where *deviceName* is the device name identified when you ran `fdisk -l`.
    Run the following command to extend the archive pool: `portal-storage-util.sh extend_db_archive_pool deviceName`
    where *deviceName* is the device name identified when you ran `fdisk -l`.
    For example: `portal-storage-util.sh extend_db_archive_pool sde`
12. For each HCP Anywhere Enterprise Portal instance, starting from the HCP Anywhere Enterprise Portal main database and proceeding to the application servers, start HCP Anywhere Enterprise Portal services.
    a) Log in as root user to each HCP Anywhere Enterprise Portal server over SSH.
    b) Run the following command to start the portal services: `portal-manage.sh start`

Protecting the HCP Anywhere Enterprise Portal Main Database Using vSphere HA

The HCP Anywhere Enterprise Portal platform must be protected from datacenter and virtualization host failure and maintain data integrity and business continuity. This can be achieved through HCP Anywhere Enterprise Portal's native, application level, database archiving and replication procedures but can also be managed at the ESXi layer.

To protect the HCP Anywhere Enterprise Portal platform from datacenter and virtualization host failure at the ESXi layer:

- vSphere HA Hardware and Software Requirements
- Configuring vSphere HA
- Testing vSphere HA Failover

vSphere HA Hardware and Software Requirements

Before starting to configure vSphere HA and protect the HCP Anywhere Enterprise Main Database VM, review VMware's vSphere HA Hardware and Software requirements. These requirements must be addressed prior to any configuration and VM deployments.

Configuring vSphere HA

Perform the following procedure to enable vSphere HA for your datacenter.

To configure vSphere HA:

1. Login in to your vCenter Server using vSphere client.
2. Right-click on the cluster you want to protect using vSphere HA on and click **Settings**.
3. Browse to **vSphere Availability** under **Services**.
4. Click **EDIT** for vSphere HA.

   The **Edit Cluster Settings** window is displayed.
5. Enable **vSphere HA**.

6. In the **Failures and responses** tab make sure that **Enable Host Monitoring** is on and set **Host Failure Response** to **Restart VMs**.
7. In the **Heartbeat Datastores** tab, select the shared datastores that will be used for vSphere HA.

   Note: You must select a minimum of two datastores. For automatic detection of accessible datastores, choose **Automatically select datastores accessible from the hosts**.
8. Click **OK**.

vSphere HA is now enabled on the cluster.

Once vSphere HA is enabled, using the dedicated, shared datastores, virtual machines deployed to hosts participating in your cluster are automatically protected.

Testing vSphere HA Failover

Virtual machines deployed to hosts participating in the vSphere HA-enabled cluster are protected.

To perform a failover test:

1. Deploy the HCP Anywhere Enterprise Portal Main Database VM to one of the hosts is the cluster with vSphere HA set.
2. Upload sample data to the HCP Anywhere Enterprise Global File System through HCP Anywhere Enterprise Portal's web application or via SMB using a HCP Anywhere Enterprise Edge Filer.
3. After successfully uploading files to the HCP Anywhere Enterprise Global File System, power off the vSphere host running the HCP Anywhere Enterprise Portal Main Database.

vSphere will provide an alert indicating that the failover process has started and will begin restarting the HCP Anywhere Enterprise Portal Main Database VM on a second host.

Upon completing the failover, vSphere will provide an alert indicating that the HCP Anywhere Enterprise Portal Main Database virtual machine is back up and running.

The failover and failback processes are performed automatically, requiring no manual intervention.

Chapter 8. Upgrading HCP Anywhere Enterprise Portal

The procedure to upgrade an existing HCP Anywhere Enterprise Portal installation is dependent on whether the upgrade involves upgrading the portal software or both the software and the portal image.

As a general rule, new releases include both image and software upgrades and Hitachi Vantara strongly recommends that you upgrade both. The release notes for each release specifies whether a portal image upgrade is required in addition to a portal software upgrade.

You can upgrade the software from within the portal user interface or via CLI (Upgrading the HCP Anywhere Enterprise Portal Software (Via the UI or CLI)) and the image via CLI (Upgrading the HCP Anywhere Enterprise Portal Image Via CLI).

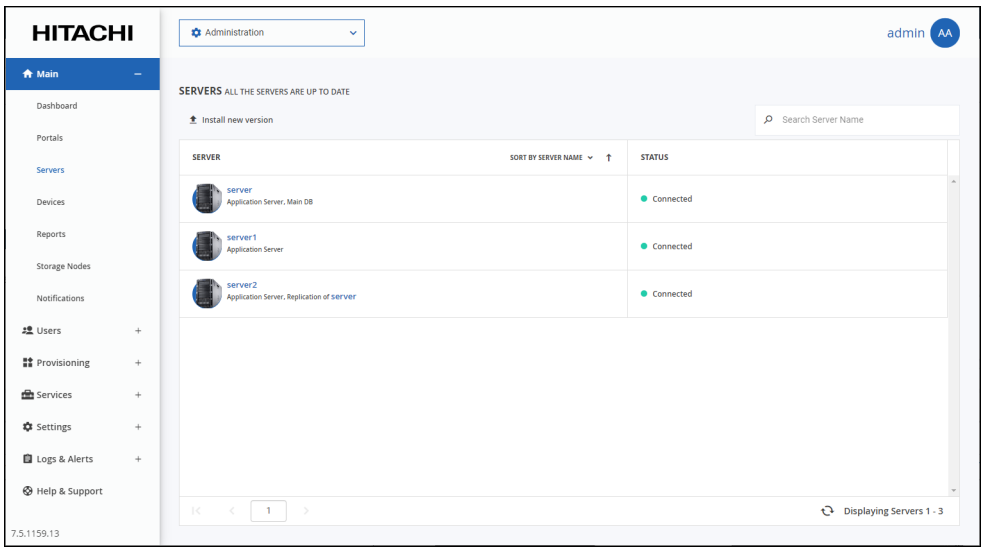
Hitachi Vantara recommends upgrading software and a new image with the help of Hitachi Vantara Support.

Upgrading the HCP Anywhere Enterprise Portal Software (Via the UI or CLI)

You can upgrade the HCP Anywhere Enterprise Portal software in the HCP Anywhere Enterprise Portal user interface or via the command line.

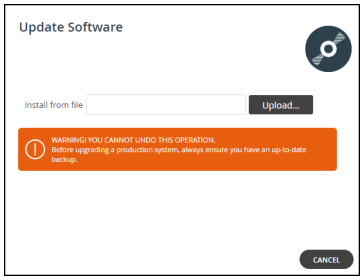
To upgrade the HCP Anywhere Enterprise Portal software via the portal user interface:

1. In the global administration view, select **Main > Servers** in the navigation pane.
   The **SERVERS** page is displayed, listing all the servers for the HCP Anywhere Enterprise Portal.



2. Click **Install new version**.

The **Update Software** window is displayed.



3. Upload the HCP Anywhere Enterprise Portal version provided by Hitachi Vantara.

   All servers in the HCP Anywhere Enterprise Portal installation are upgraded.

To upgrade the HCP Anywhere Enterprise Portal software via CLI:

1. Stop the HCP Anywhere Enterprise Portal servers.
   First stop all application and preview servers. Next stop the main database server and finally stop the replication database server, if available.
   a) Using SSH, log in as root to the HCP Anywhere Enterprise Portal server.
   b) Run the following command: `portal-manage.sh stop`
   Once services are stopped, the `Done` message is displayed on the screen.
2. When all servers are in a stop state, upgrade the primary database portal software.
   a) Using SSH, log in as root to the HCP Anywhere Enterprise Portal server.
   b) Upgrade the HCP Anywhere Enterprise Portal software: `portal-manage.sh upgrade` *`upgrade_file`*
   where *upgrade_file* is the software file provided by Hitachi Vantara.
3. Restart the primary database server: `portal-manage.sh start`
4. After the primary database server is running, using SSH, log in as root to the secondary HCP Anywhere Enterprise Portal servers.
5. Upgrade the HCP Anywhere Enterprise Portal software on each secondary HCP Anywhere Enterprise Portal server: `portal-manage.sh upgrade` *`upgrade_file`*
   where *upgrade_file* is the software file provided by Hitachi Vantara.
6. Restart the secondary HCP Anywhere Enterprise Portal servers.
   First start the replication database server, if available. Next, start the application and preview servers.
   a) Using SSH, log in as root to the HCP Anywhere Enterprise Portal server.
   b) Start the HCP Anywhere Enterprise Portal: `portal-manage.sh start`

Upgrading the HCP Anywhere Enterprise Portal Image Via CLI

When using CLI to upgrade the portal, you have to stop all the portal servers before upgrading the image.

To upgrade the HCP Anywhere Enterprise Portal image:

1. Stop the HCP Anywhere Enterprise Portal servers.
   First stop all application and preview servers. Next stop the main database server and finally stop the replication database server, if available.
   a) Using SSH, log in as root to the HCP Anywhere Enterprise Portal server.
   b) Run the following command: `portal-manage.sh stop`
   Once services are stopped, the `Done` message is displayed on the screen.
2. When all servers are in a stop state, upgrade the portal image.
   a) Using SSH, log in as root to the HCP Anywhere Enterprise Portal server.
   b) Copy the upgrade installer into the machine.
   c) Navigate to the location of the installer and run the following command:
   `tar xvf portal-installer-linux-7.0.xxx.tar.bz2`
   d) Navigate to the cd portal-installer-linux-`7.0`.xxx subdirectory and run the following command: `./install.sh -u`
3. Restart the servers.
   First start the main database server. Next start the replication database server, if available. Finally start the application and preview servers.
   a) Using SSH, log in as root to the HCP Anywhere Enterprise Portal server.
   b) Start the HCP Anywhere Enterprise Portal: `portal-manage.sh start`
   When the image kernel was also upgraded, an additional restart is also required to complete the kernel upgrade:
   Stop the portal: `portal-manage.sh stop`
   Start the portal: `portal-manage.sh start`
   Note: The additional stop and start commands above are mandatory in order to complete the kernel upgrade.

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