Administrator Guide

Guide Version 1.18

Copyright

Acknowledgments

Hypori uses open source and copyrighted third-party software as part of its Virtual Mobile Infrastructure product. Copyright information, licensing agreements, and general acknowledgments for third-party software usage are listed in separate documents, which are available on request. Contact your Hypori representative for more information.

Contents

Chapter 1. Overview of the Hypori Halo System

The Hypori Halo system is a Virtual Mobile Infrastructure (VMI) platform. Users running the Hypori Halo Client app on their mobile devices access their virtual workspace running in the Hypori Halo environment. The virtual workspace runs on the Android operating system and supports PKI credential-based multi-factor authentication. The virtual workspace leverages FIPS 140-2 crypto and TLS 1.2 encryption protocols to communicate securely with the Hypori Halo Client app.

The Hypori Halo system is composed of:

- **Client:** The app installed on the user's mobile device, which communicates with the virtual workspace on the Hypori Halo environment using secure, encrypted protocols.
- **Virtual Workspace:** The virtual mobile device component within the Hypori Halo environment. It hosts the apps that run on the secure server.
- **Environment:** The server clusters that host the Hypori Halo virtual workspaces.
- **Admin Console:** A web application to monitor and manage an expanded feature set within a designated Hypori Halo environment.
- **User Management Console:** A web application to manage users within a designated Hypori Halo environment.

Chapter 2. Getting Started

Welcome to the *Hypori Halo Administrator's Guide*. The Hypori Halo Admin Console is a full-featured, web-based UI allowing you to create and manage domains, manage users and their roles as well as designate both Client and Virtual Workspace policy for your users.

Browser Requirements

You can access Hypori Halo web applications using the following browsers:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Import the Client Certificate

Important:
You will need the default admin-level username and password to continue. If you do not have your admin-level username or password, contact Product Support *(on page 6)* for assistance.

Hypori Halo authenticates you by checking that you have the correct client certificate installed on your computer. You must import this certificate before you access the Hypori Halo Admin Console.

To import your certificate:

1. On your computer, disable all VPN's.
2. Using your browser, select the link sent to you by your Hypori Halo administrator.
3. At the login page, enter the User ID and password given to you by your Hypori Halo administrator.
4. At the bottom of the web page, click **Advanced** and then click **Download PKCS12 File**.
5. Install the .p12 certificate on your system. We have provided you generic Windows and Mac instructions below, but certificate installation steps may vary depending on your operating system and browser.

- **If installing on a Windows PC:**
    a. Double-click the downloaded .p12 file to open the Certificate Import Wizard
    b. Current User should be selected. Click **Next**.
    c. Leave the default selections selected. Click **Next**.
    d. Enter the password for the private key, then click **Next**.
    e. The Automatically select option should be selected. Click **Next**.
    f. Click **Finish**.
- **If installing on a Mac:**

> **Tip:**
> This procedure works best using Safari or Chrome.

    a. Double-click the downloaded .p12 file.
    b. Enter the Mac's admin password and the account's password when prompted.
    If you receive an error saying "System root does not have access to this certificate" perform these steps:
        i. Drag and drop the certificate into Keychain Access app under the login tab, located on the left side of the screen.
        ii. Double-click the cert entry, then select **Trust** from the drop-down list.
        iii. Select **Always Trust** as the default option at the top to update all the settings at once.
        iv. Go back and click the drop-down arrow for the entry, then double-click the **privatekey** entry.
        v. Change the selection to **Allow all apps to access** then click **Save Changes**.
        vi. Enter the Mac's admin password when prompted.
        vii. Close all open browser windows.
        If using Firefox, you must import the certificate into the browser itself by performing these additional steps: (skip the bullets below if using Safari or Chrome)
            - Open the browser. Click the hamburger menu ☰ in the upper right corner, then click **Preferences**.
            - Use the search bar to look for 'Certificates'.
            - Click **View Certificates**.
            - Click the **Your Certificates** tab.
            - Click **Import** (at the bottom), then select the certificate you installed from the Downloads folder.
            - Enter the account password when prompted.

Logging on to the Hypori Halo Admin Console

Before you log on to the Hypori Halo Admin Console, be sure you have imported the client certificate. See Import the Client Certificate *(on page 2)*.

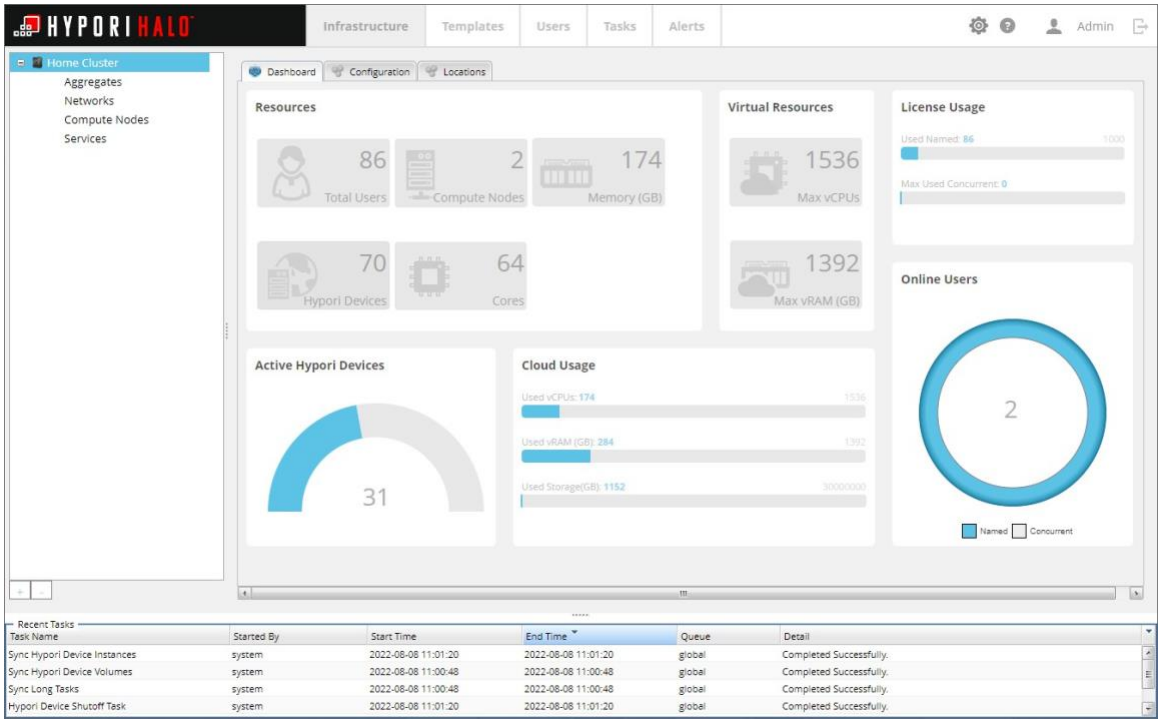
Note:
You must be on the management network to access the Hypori Halo Admin Console.

To access the Admin Console:

1. Open a web browser.
2. Enter the designated Admin Console URL into your browser.
3. Confirm your certificate.

Tip:
If your browser gives you the option to remember this decision, you should do so. Otherwise, you may be prompted for the certificate the next time you log in.

Hypori Halo Admin Console Layout



Menu

The menu is at the top of the Hypori Halo Admin Console, within the Hypori Halo banner. It is available regardless of which page you are viewing.

Infrastructure

Use the Infrastructure page to manage your server cluster.

Templates

Use the Templates page to manage virtual workspace templates, images, apps, and flavors used in the server cluster.

Users

Use the Users page to add and manage users and their virtual workspaces.

Tasks

Use the Tasks page to view the server's task history, ordered by task start time.

Alerts

Use the Alerts page to view server alerts generated by the server cluster.

Settings icon

Clicking the Settings icon allows you to configure the device whitelist, view/update licensing information, configure SMTP settings, and view/update external naming.

Help

Clicking the Help button accesses product documentation, software version information, and the Hypori Halo support site.

Logout

Clicking the Logout button initiates the log out process. In the Logout confirmation box, click **Yes** to log out of the Admin Console.

Tabs

Some pages have tabs to help organize content. These tabs are at the top of the page, just under the Hypori Halo banner and menu. Select a tab to view its content.

Navigation Pane

The navigation pane, on the left side of some pages, provides hierarchical navigation within the page.

Recent Tasks Panel

The Recent Tasks panel at the bottom of the Admin Console shows a list of the tasks that have been executed by the Admin Console, sorted by event start time.

Product Support

For product support, contact us at: https://www.hypori.com/support/

Chapter 3. Server Clusters

The Hypori Halo servers host and store virtual workspace data. These servers are grouped in server clusters that have:

- A controller node that manages the compute nodes and storage nodes.
- Compute nodes that run the virtual workspaces.
- Storage nodes that provide access to remote storage, where virtual workspaces and their data can be stored to allow for high availability and disaster recovery.

Aggregates

An aggregate has one or more compute nodes that store their virtual workspace data on the remote storage server in their storage zone. The compute nodes access their data directly from the remote storage provider, coordinating access with the storage node.

Storage Zones

A server cluster has one or more storage zones. A storage zone has a remote storage server where virtual workspace data is stored and a storage node that enables access to the data. A storage zone stores data for one or more aggregates.

Managing Server Clusters

You can configure and manage the server clusters in your environment.

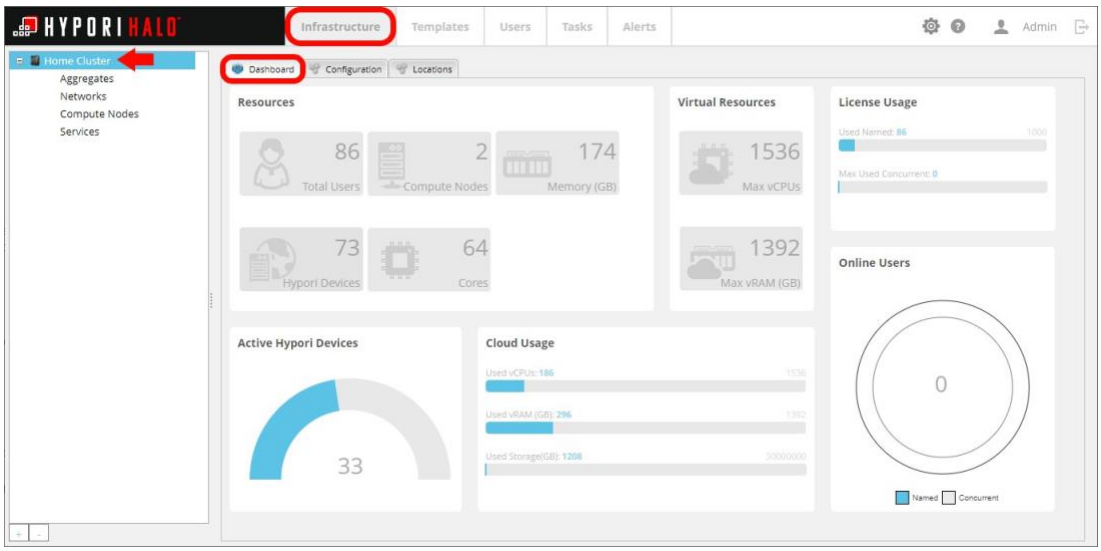
Important:
Provisioning additional server clusters should only be done with the assistance of Hypori Halo Support.

Viewing Server Cluster Dashboard Metrics

To view the metrics for a server cluster:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Infrastructure**.
3. In the navigation pane, select the server cluster.

4. Click the **Dashboard** tab.



The Dashboard page shows:

- **Resources**
  - **Total Users:** The number of users.
  - **Compute Nodes:** The number of compute nodes in the server cluster.
  - **Memory (GB):** The amount of available RAM for the server cluster.
  - **Hypori Devices:** The number of virtual workspaces in the server cluster.
  - **Cores:** The number of server cores in the server cluster.
- **Virtual Resources**
  - **Max vCPUs:** The maximum virtual CPU count for the server cluster.
  - **Max vRAM (GB):** The maximum virtual RAM (in GB) for the server cluster.
- **Active Hypori Devices:** The number of virtual workspaces currently running on the server cluster in relation to the total number of virtual workspaces provisioned.
- **Cloud Usage**
  - **Used vCPUs:** The number of virtual CPUs used in relation to the total number of virtual CPUs available.
  - **Used vRAM (GB):** The amount of virtual RAM (in GB) used in relation to the total amount of virtual RAM.
  - **Used Storage (GB):** The amount of storage (in GB) used in relation to the total amount of storage available.
- **License Usage**

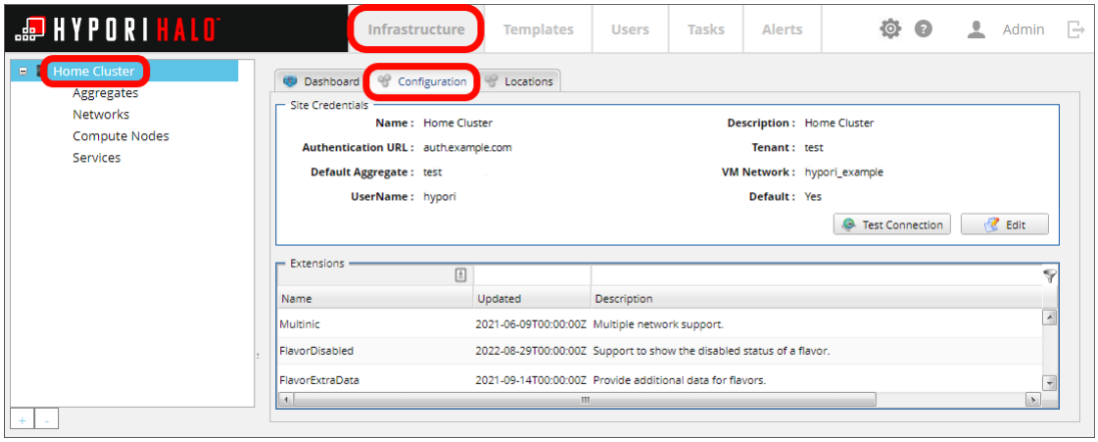
  - **Used Named:** The number of named user licenses in use in relation to the total number of named user licenses.
  - **Max Used Concurrent:** The maximum number of concurrent user licenses used from the available pool of licenses.
- **Online Users:** The number of users currently connected to their virtual workspaces, for each user license type.

Dashboard metrics are read-only, and they update automatically.

Viewing Server Cluster Details

To view the configuration settings for a server cluster:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Infrastructure**.
3. In the navigation pane, select the server cluster you want to view.
4. Click the **Configuration** tab.



The Configuration tab shows:

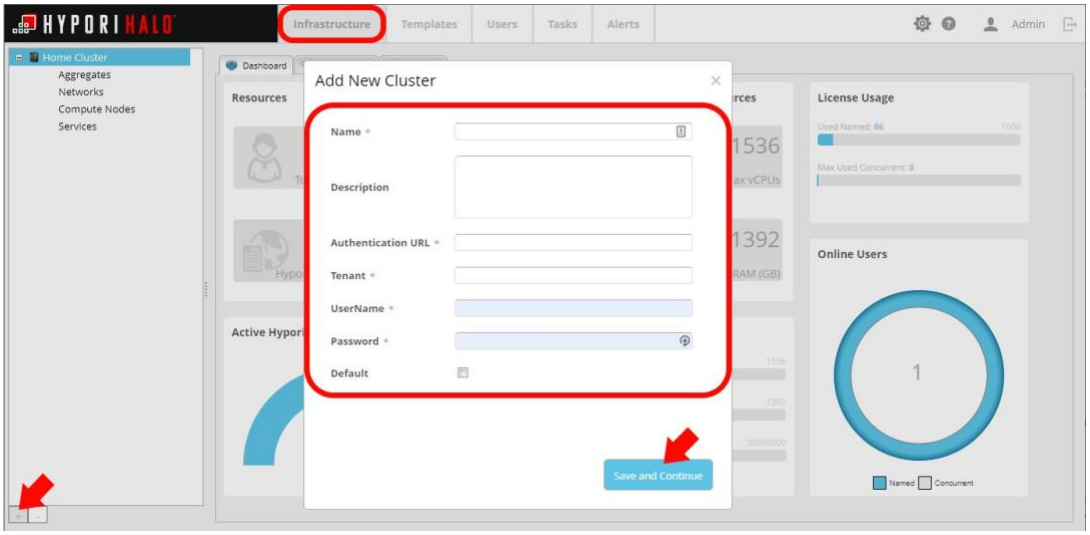
- **Name:** The name of the server cluster.
- **Description:** A brief description of the server cluster.
- **Authentication URL:** The URL for the controller node.
- **Tenant:** The tenant resource container within the compute node.
- **Default Aggregate:** The name of the aggregate to which new virtual workspaces are added by default.
- **VM Network:** The name of the enterprise network, which provides virtual workspaces with access to shared resources in your enterprise.

- **UserName:** The username for the controller node.
- **Default:** Whether this is the server cluster to which new virtual workspaces are added by default.

Adding Server Clusters

To add a server cluster:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Infrastructure**.
3. At the bottom of the navigation pane, click the **add** (**+**) icon.
4. In the Add New Cluster box, provide the following information:
    - **Name:** The name of the server cluster.
    - **Description:** A brief description of the server cluster.
    - **Authentication URL:** The URL for the controller node.
    - **Tenant:** The tenant resource container within the compute node.
    - **UserName:** The username for the controller node.
    - **Password:** The password for the controller node.
    - **Default:** Whether this is the server cluster to which new virtual workspaces are added by default.



5. Click **Save and Continue**.
6. On the next screen, provide the following information:

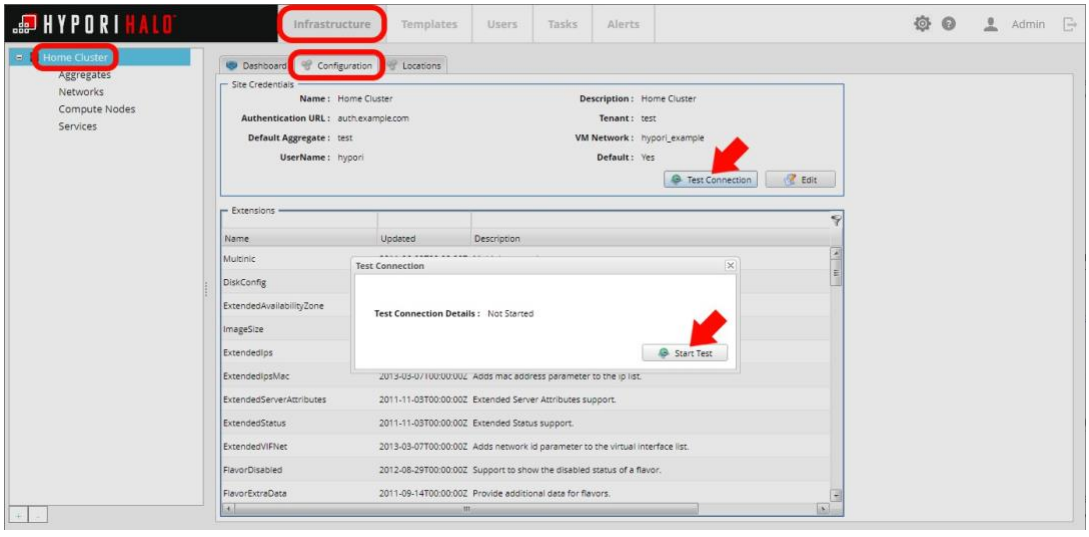
- **VM Network:** The name of the enterprise network, which provides virtual workspaces with access to shared resources in your enterprise.
- **Default Aggregate:** The name of the aggregate to which new virtual workspaces are added by default.

7. Click **Apply** to save the configuration settings.

Editing Server Clusters

To edit the configuration for an existing server cluster:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Infrastructure**.
3. In the navigation pane, select the server cluster you want to edit.
4. Click the **Configuration** tab.
5. In the Site Credentials area, click **Edit**.
6. In the Update Cluster box, modify the following information as necessary:
    - **Name:** The name of the server cluster.
    - **Description:** A brief description of the server cluster.
    - **Authentication URL:** The URL for the controller node.
    - **Tenant:** The tenant resource container within the compute node.
    - **UserName:** The username for the controller node.
    - **Password:** The password for the controller node.
    - **Default:** Whether this is the server cluster to which new virtual workspaces are added by default.



7. Click **Save and Continue**.
8. On the next screen, edit the following information as needed:

- **VM Network:** The name of the enterprise network, which provides virtual workspaces with access to shared resources in your enterprise.
- **Default Aggregate:** The name of the aggregate to which new virtual workspaces are added by default.

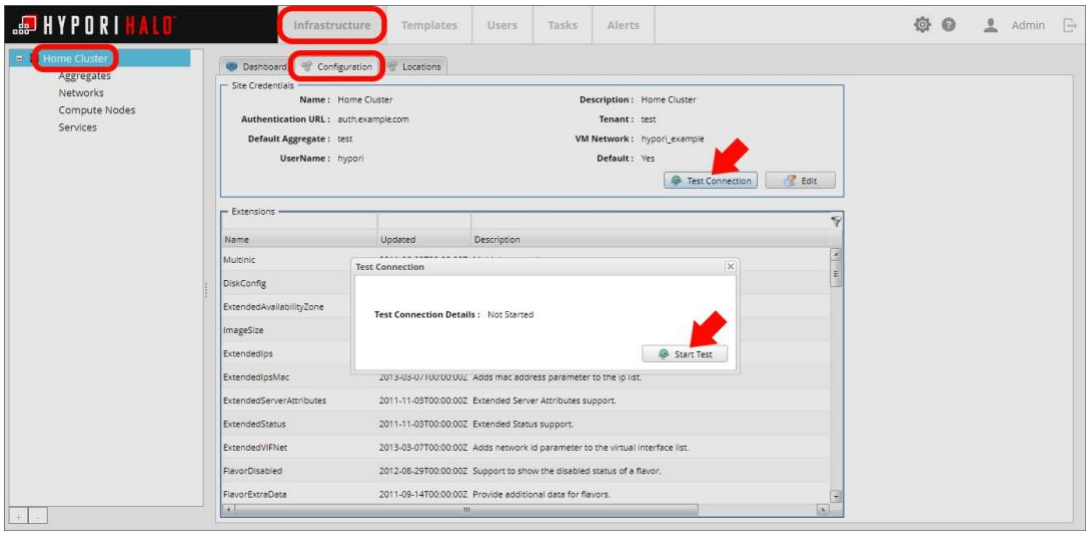
9. Click **Apply** to save the modified configuration settings.

Testing Server Cluster Connections

To test a server cluster connection:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Infrastructure**.
3. In the navigation pane, select the server cluster you want to test.
4. Click the **Configuration** tab.
5. In the Site Credentials area, click **Test Connection** to open the Test Connection box.
6. Click **Start Test**.

   If the test does not complete successfully, click **Re-run Test**. If the test fails again, clear the box, and check your connection settings.

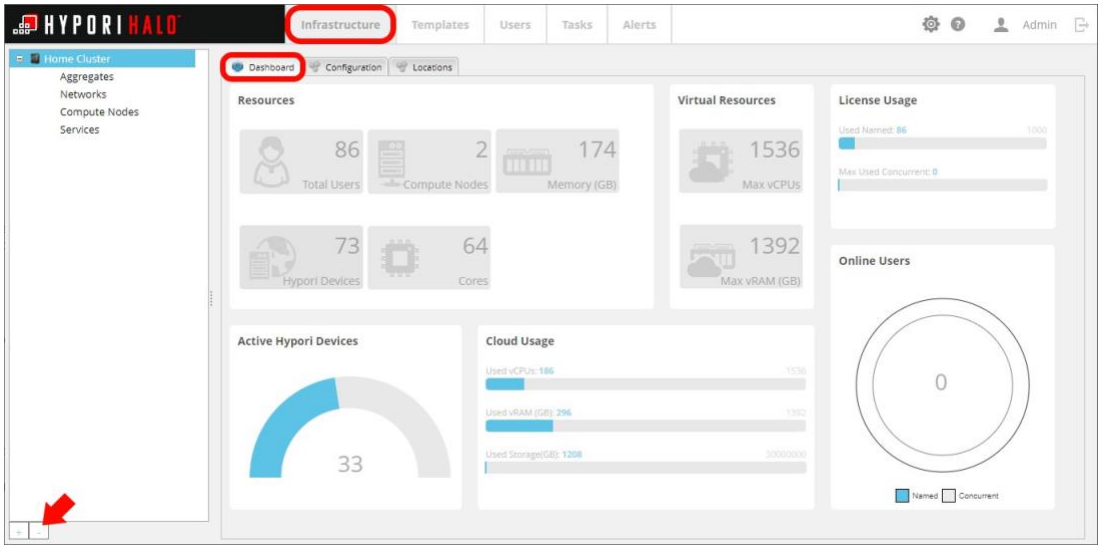


7. After the test completes successfully, click the ✕ in the upper right corner to clear the confirmation message.

Deleting Server Clusters

To delete a server cluster:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Infrastructure**.
3. In the navigation pane, select the server cluster to be deleted.
4. At the bottom of the navigation pane, click the **minus** (-) icon.



5. In the confirmation box, click **Yes**.

> **Tip:**
> You cannot delete a server cluster that is in use.

Managing Aggregates

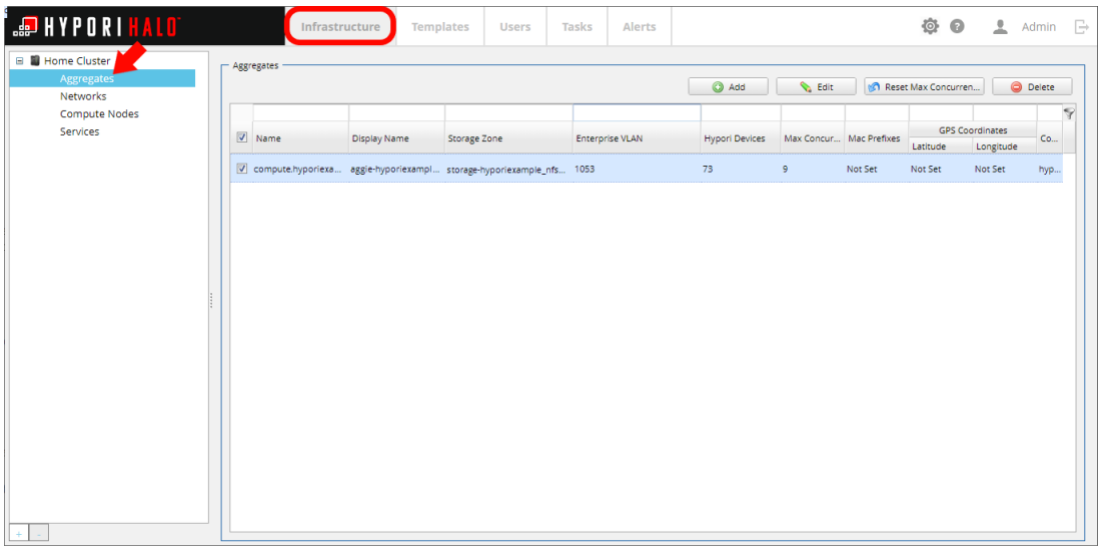
An aggregate distributes virtual workspaces across its compute nodes. Typically, the compute nodes in an aggregate are in close physical proximity to ensure that users who access their virtual workspaces associated with that aggregate have a similar experience.

Viewing Aggregates

To view the information about the aggregates in a server cluster:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Infrastructure**.

3. In the navigation pane, expand the server cluster and click **Aggregates**.



For each aggregate, the Aggregates screen shows:

- **Name:** The name of the aggregate.
- **Display Name:** The name by which the aggregate will be referenced in the Hypori Halo User Management Console. (HUMC)
- **Storage Zone:** The storage zone for the aggregate.
- **Enterprise VLAN:** The identifier for the logical network connecting the compute nodes to the virtual workspaces. Each Enterprise VLAN typically supports up to 500 virtual workspaces.
- **Hypori Devices:** The number of virtual workspaces hosted by the aggregate.
- **Max Concurrency:** The largest number of concurrently active users on this aggregate.
- **Mac Prefixes:** The prefix used for virtual workspaces in the aggregate. If not set, this value is set to `fa:16:3e`
- **GPS Coordinates:** The physical location of the aggregate.
- **Compute Nodes:** The compute nodes in the aggregate.

Creating Aggregates

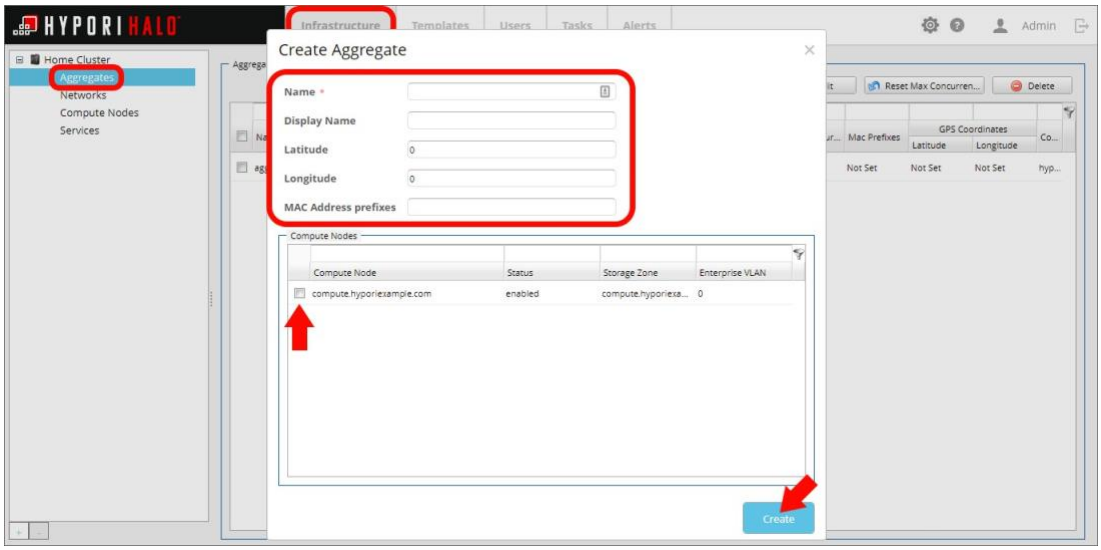
Before you create an aggregate, ensure that the compute nodes you want to include in the aggregate have been installed and share the same storage zone, which includes a remote storage server and storage node.

To create an aggregate:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Infrastructure**.

3. In the navigation pane, expand the server cluster and click **Aggregates**.
4. Click the **add** (+) icon.
5. In the Create Aggregate box, provide the following information:
    - **Name:** The name of the aggregate.
    - **Display Name:** The name by which the aggregate will be referenced in the Hypori Halo User Management Console. (HUMC)
    - **Latitude:** The latitude coordinate of the aggregate. If not set, this value is set to `0`.
    - **Longitude:** The longitude coordinate of the aggregate. If not set, this value is set to `0`.
    - **MAC Address prefixes:** The prefix used for virtual workspaces in the aggregate. If not specified, this value is set to `fa:16:3e`

> **Tip:**
> Latitude and Longitude are optional settings that are used as the default physical location when using apps in the virtual workspace. If a virtual workspace app requests a GPS location and there is not a GPS location available, this default will be provided to the app.



6. On the Compute Node list, ensure that only the compute nodes to be included in the aggregate are selected.
7. If you selected compute nodes using local storage, go to the next step. If you selected compute nodes with remote storage, click **Next** and select the storage node associated with your compute nodes.
8. Click **Create**.

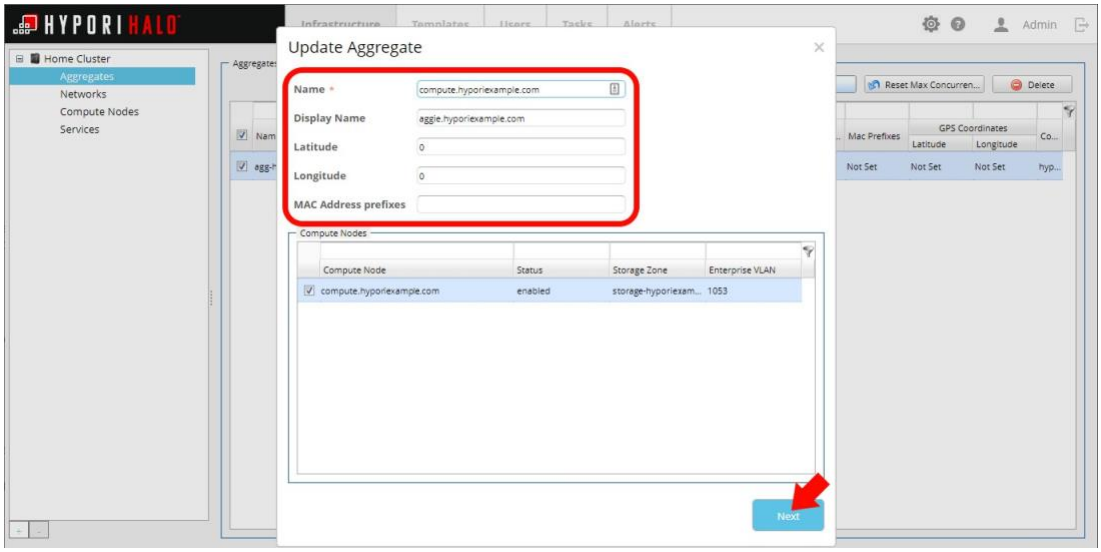
> **Note:**
> If the Create button is greyed out and not available, the storage node was not allocated. To resolve this situation:
>
> a. Uncomment **storage.example.com**.
>
> b. Delete the host.
>
> c. Re-run the `step2` script.

9. In the confirmation box, click **Yes**.

Editing Aggregates

To edit the properties for an aggregate:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Infrastructure**.
3. In the navigation pane, expand the server cluster then click **Aggregates**.
4. Check the box next to the aggregate you want to modify then click **Edit**.



5. In the Update Aggregate box, modify the following information as needed:
   - **Name:** The name of the aggregate.
   - **Display Name:** The name by which the aggregate will be referenced in the Hypori Halo User Management Console. (HUMC)
   - **Latitude:** The latitude coordinate of the aggregate. If not set, this value is set to `0`.
   - **Longitude:** The longitude coordinate of the aggregate. If not set, this value is set to `0`.
   - **MAC Address prefixes:** The prefix used for virtual workspaces in the aggregate. If not specified, this value is set to `fa:16:3e`

6. On the Compute Nodes list, ensure that only the compute nodes you want to include in the aggregate are selected.
7. Click **Next**.
8. In the **Storage Zone** list, update the storage node associated with your compute nodes, if necessary.
9. If your remote storage node is already setup for encryption, check the box next to **Storage Encrypted?**. This option notifies the virtual workspace that its storage is encrypted.

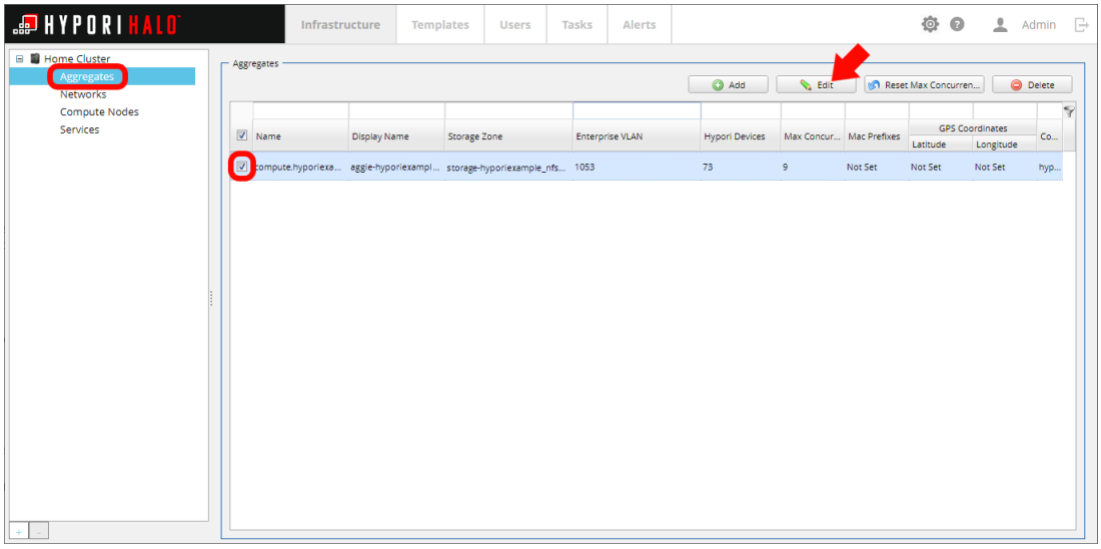
> **Important:**
> If you select **Storage Encrypted?** and the remote storage node is not setup for encryption, then the virtual workspace will behave as if it is performing encryption, but it will not actually be encrypted. For encryption to properly function, the remote storage node must be setup to encrypt before selecting **Storage Encrypted?**.

10. Click **Update**.

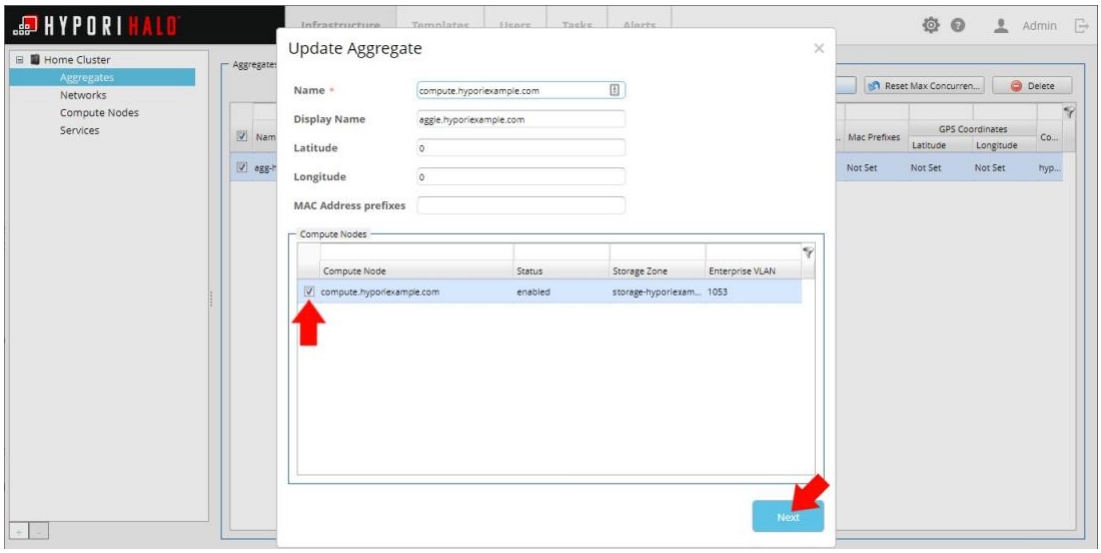
Enabling Encryption on Aggregates

To setup encryption for all workspaces on an aggregate:

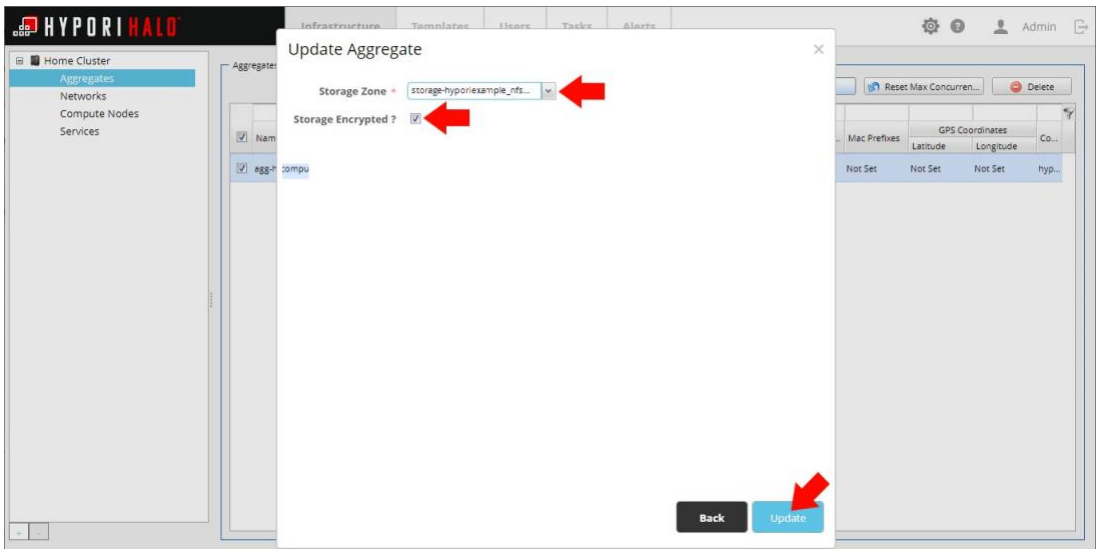
1. Open the Hypori Halo Admin Console.
2. In the menu, click **Infrastructure**.
3. In the navigation pane, expand the server cluster and click **Aggregates**.
4. Check the box next to the aggregate you want to modify then click **Edit**.



5. In the Update Aggregate box, under Compute Nodes, select the node that you want to enable encryption on, and then click **Next**.



6. Check the box next to **Storage Encrypted?** to enable encryption and then click **Update**.



Encryption will now be enabled for all virtual workspaces using the selected aggregate.

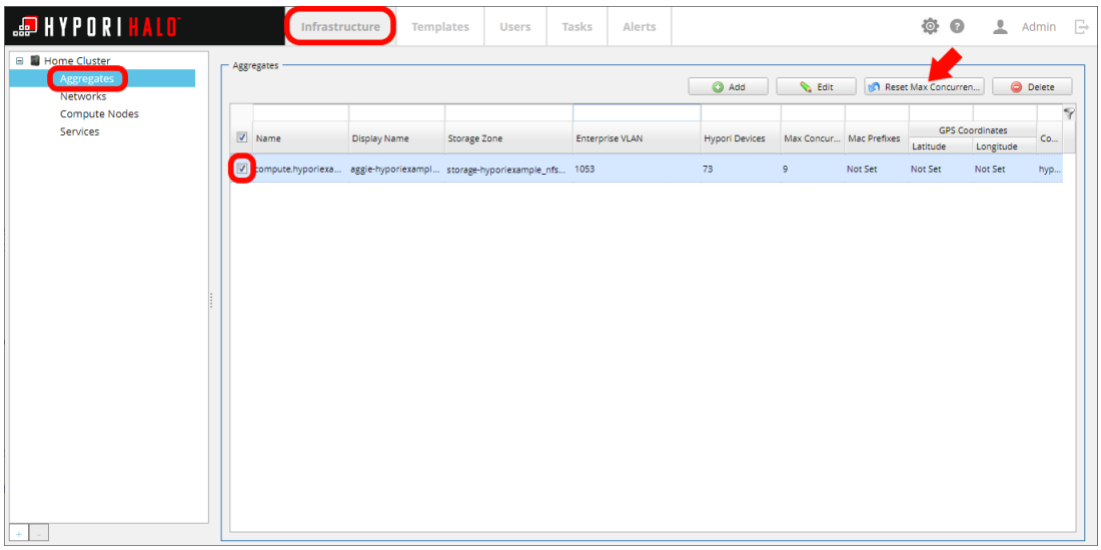
Resetting Max Concurrency for Aggregates

The Hypori Halo Admin Console tracks the largest number of concurrently active users on each aggregate. You can reset the max concurrency to clear this data and restart tracking.

To reset the max concurrency for an aggregate:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Infrastructure**.
3. In the navigation pane, expand the server cluster and click **Aggregates**.
4. Click **Reset Max Concurrency**.

5. In the confirmation box, click **Yes**.



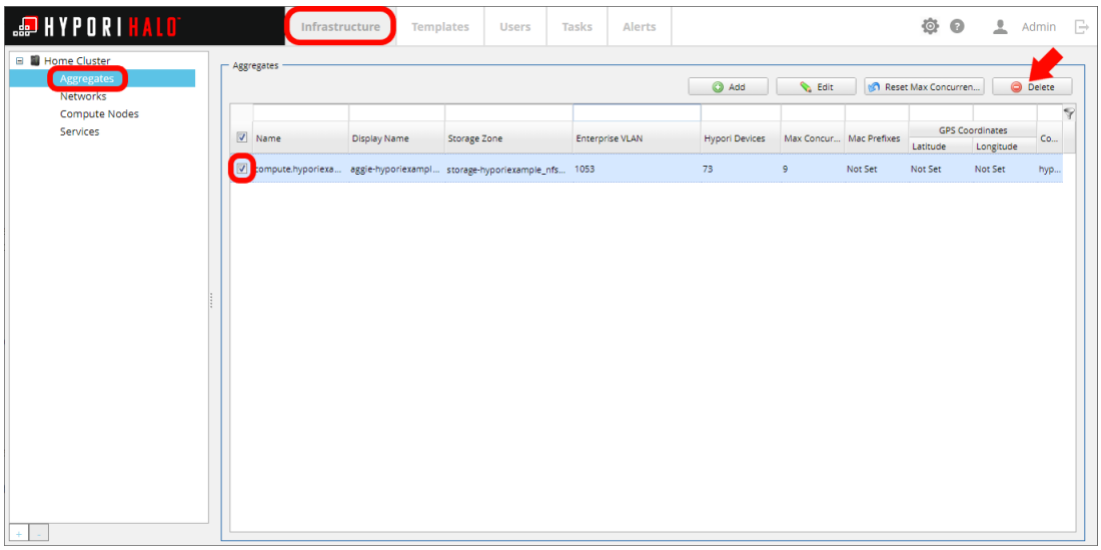
Deleting Aggregates

To delete an aggregate:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Infrastructure**.
3. In the navigation pane, expand the server cluster and click **Aggregates**.
4. Check the box next to the aggregate to be deleted.
5. Click **Delete**.

> **Tip:**
> You can also delete an aggregate by holding your cursor over the row in the table then clicking the **Delete Aggregate** icon.

6. In the confirmation box, click **Yes**.



Tip:

You cannot delete an aggregate that is in use.

Managing Compute Nodes

The Hypori Halo Admin Console allows you to perform management tasks on the compute nodes.

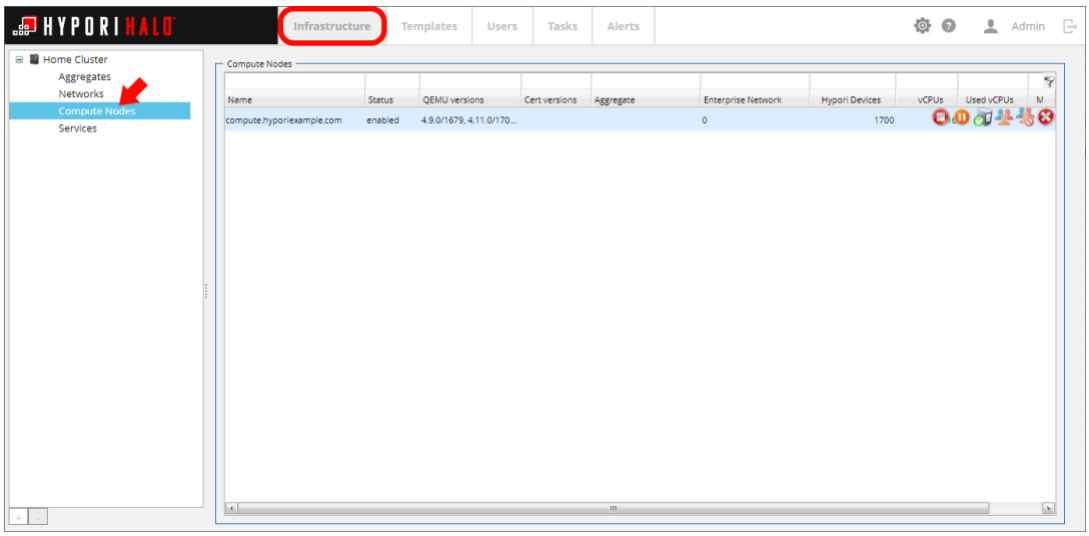
Each compute node is part of an aggregate. The compute nodes in an aggregate share a storage zone, including a storage node and its associated remote storage. The aggregate distributes virtual workspaces across its compute nodes.

Viewing Compute Nodes

To view information about the compute nodes associated with a server cluster:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Infrastructure**.

3. In the navigation pane, expand the server cluster and click **Compute Nodes**.



For each compute node, the page shows:

- **Name:** The name of the compute node.
- **Status:** Whether the compute node is enabled.
- **QEMU Versions:** The hosted virtual machine monitor version.
- **Cert Versions:** The certificate version.
- **Aggregate:** The name of the aggregate associated with the compute node.
- **Enterprise Network:**
- **Hypori Devices:** The number of virtual workspaces associated with the compute node.
- **vCPUs:** The number of virtual CPUs associated with the compute node.
- **Used vCPUs:** The number of virtual CPUs currently allocated to Hypori Devices.
- **Mem (MB):** The amount of RAM on the compute node.
- **Used Mem (MB):** The amount of RAM currently allocated to Hypori Devices.

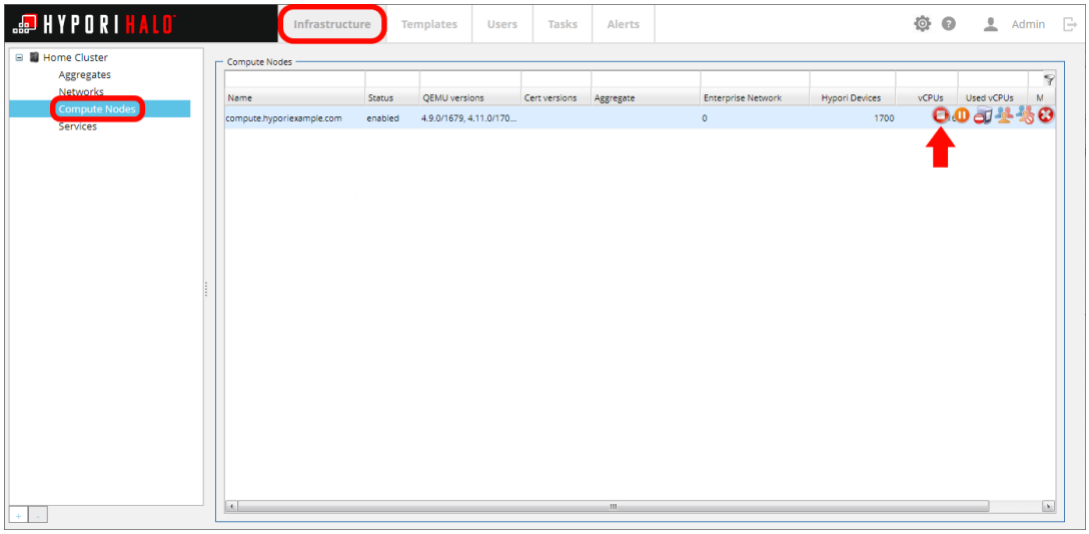
Tip:

The table displays an alert icon next to compute nodes with CPUs that do not meet hardware requirements. The performance of virtual workspaces using these compute nodes may be slower than expected. Hold your cursor over the alert to see the list of deficiencies.

Stopping All Virtual Workspaces on a Compute Node

To stop all virtual workspaces on a compute node:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Infrastructure**.
3. In the navigation pane, expand the server cluster and click **Compute Nodes**.
4. Hover your cursor over the compute node's entry and select the **Stop Hypori Devices** icon.



5. In the confirmation box, click **Yes**.

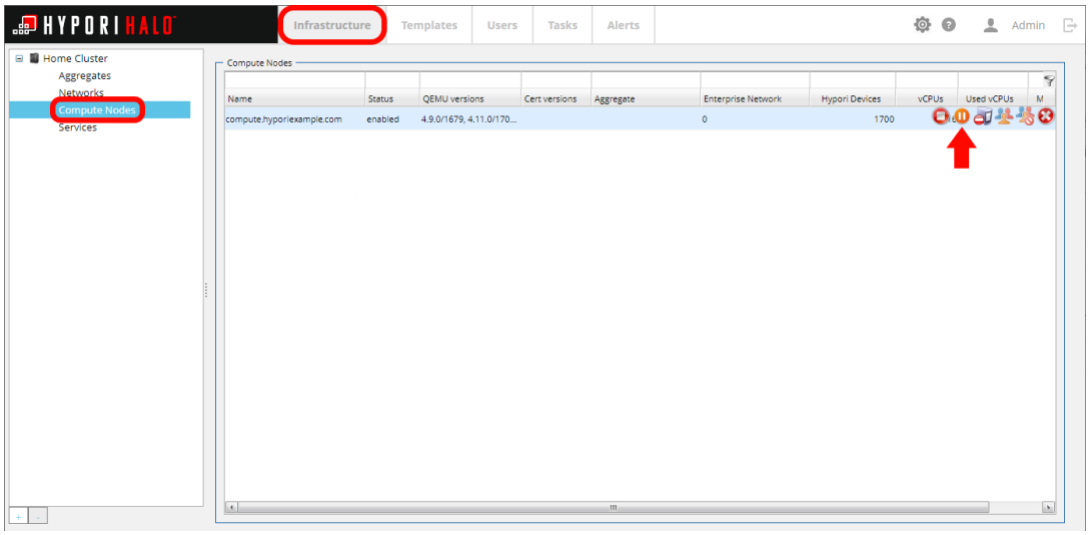
Note:

You can also stop specific virtual workspaces. See Stopping and Starting a Virtual Workspace *(on page 100)*.

Pausing All Virtual Workspaces on a Compute Node

To pause all virtual workspaces on a compute node:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Infrastructure**.
3. In the navigation pane, expand the server cluster and click **Compute Nodes**.
4. In the table, hover your cursor over the compute node.
5. Click the **Pause Hypori Devices** icon:



6. In the confirmation box, click **Yes**.

Note:

You can also pause specific virtual workspaces. See Pausing a Virtual Workspace *(on page 101)*.

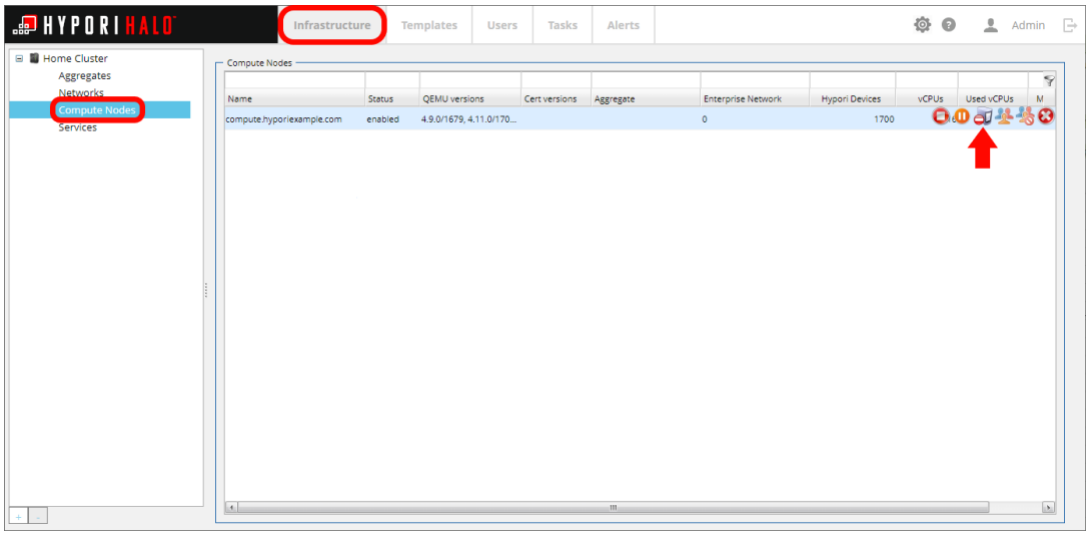
Disabling Compute Nodes

Tip:

After you disable a compute node, no virtual workspaces will be added to it.

To disable a compute node:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Infrastructure**.
3. In the navigation pane, expand the server cluster and click **Compute Nodes**.
4. In the table, hover your cursor over the compute node.
5. Click the **Disable Host** icon:



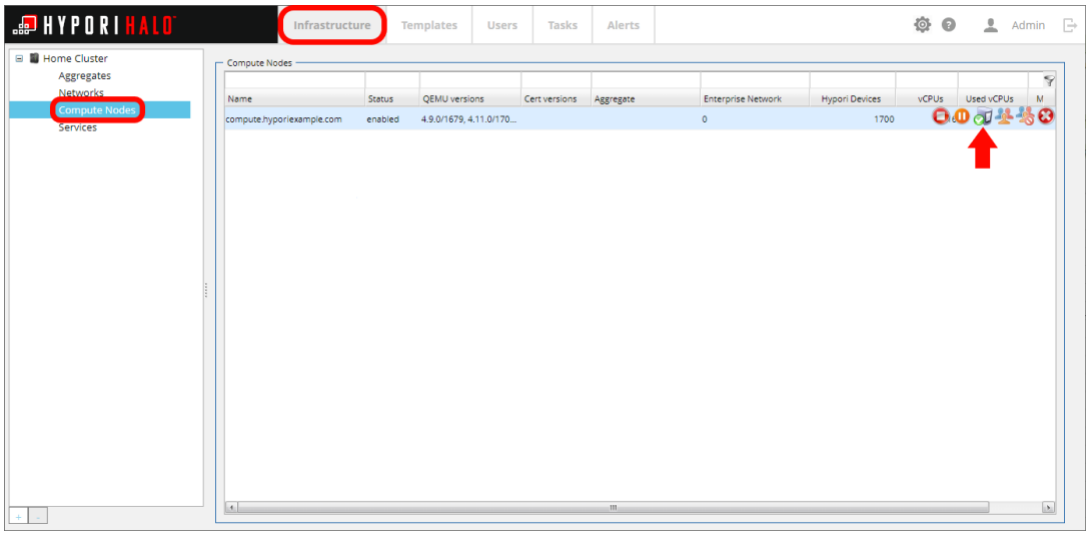
6. In the confirmation box, click **Yes**.

> **Important:**
> Disabling the compute node(s) in the Admin Console does not prevent users from connecting to their client and/or powering on their virtual workspaces on a "disabled" compute node. In addition, powering off the "disabled" compute node(s) could cause end users to see the following error:
>
> - VMAuthentication failed - Error 553 Server Error Aggregate <server_name> is currently down. Please ensure a nova-compute is up in the zone. Contact your Hypori Halo administrator for help.

Enabling Compute Nodes

To enable a compute node:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Infrastructure**.
3. In the navigation pane, expand the server cluster and click **Compute Nodes**.
4. In the table, hover your cursor over the compute node.
5. Click the **Enable Host** icon:



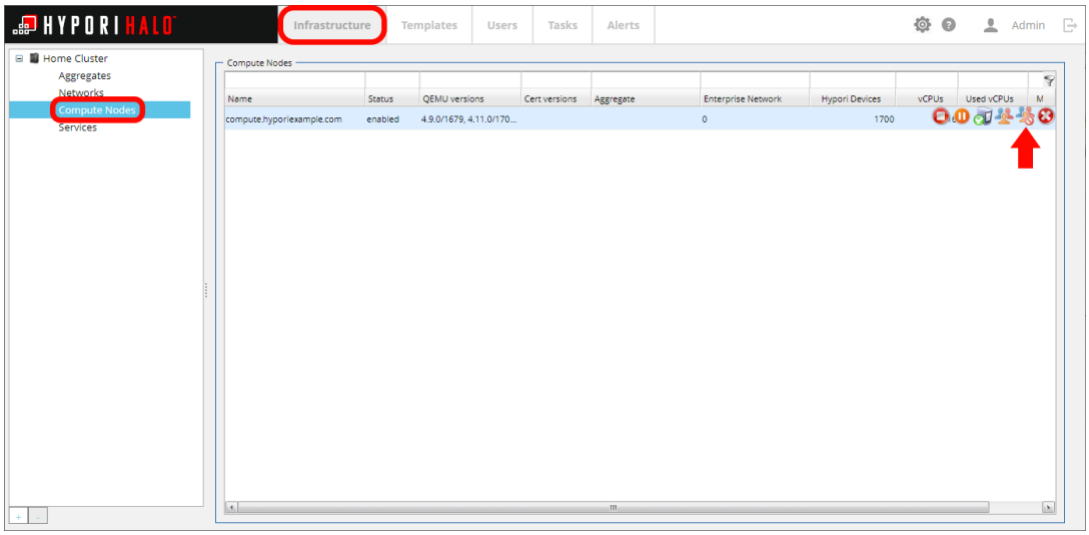
6. In the confirmation box, click **Yes**.

Disabling All User Accounts on a Compute Node

You can disable all user accounts on a compute node to prevent access to their virtual workspaces.

To disable all user accounts on a compute node:

1. In the menu, click **Infrastructure**.
2. In the navigation pane, expand the server cluster and click **Compute Nodes**.
3. In the table, hover your cursor over the compute node.
4. Click the **Disable Users on Host** icon:



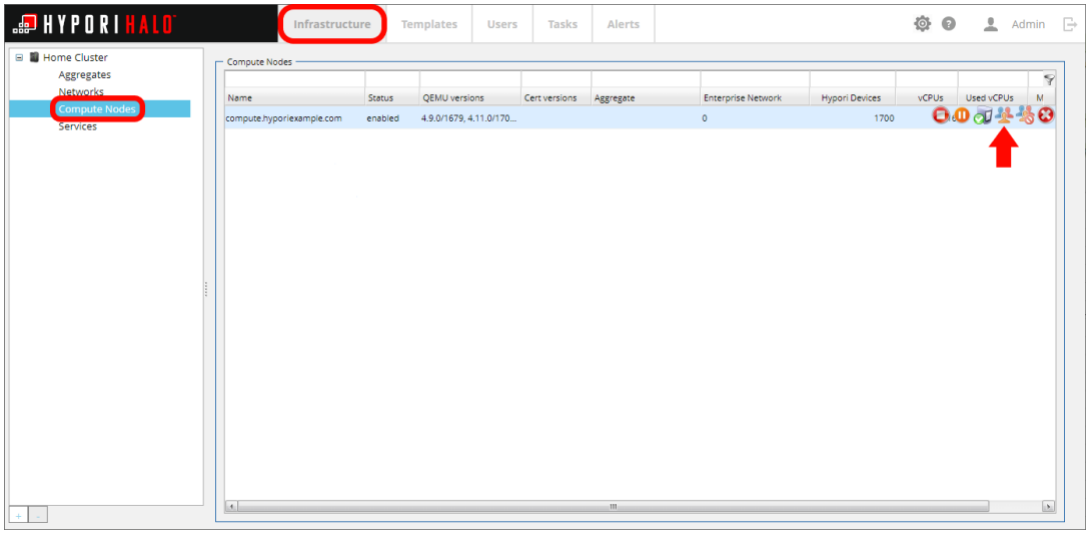
5. In the confirmation box, click **Yes**.
6. In the Disable Users box, type a message that will be shown when a user tries to access his or her virtual workspace and click **Apply**.

Note:
You can also disable select users. See Disabling Users *(on page 87)*.

Enabling All User Accounts on a Compute Node

To enable all user accounts on a compute node:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Infrastructure**.
3. In the navigation pane, expand the server cluster and click **Compute Nodes**.
4. In the table, hover your cursor over the compute node.
5. Click the **Enable Users on Host** icon:



6. In the confirmation box, click **Yes**.

Note:
You can also enable select users. See Enabling Users *(on page 88)*.

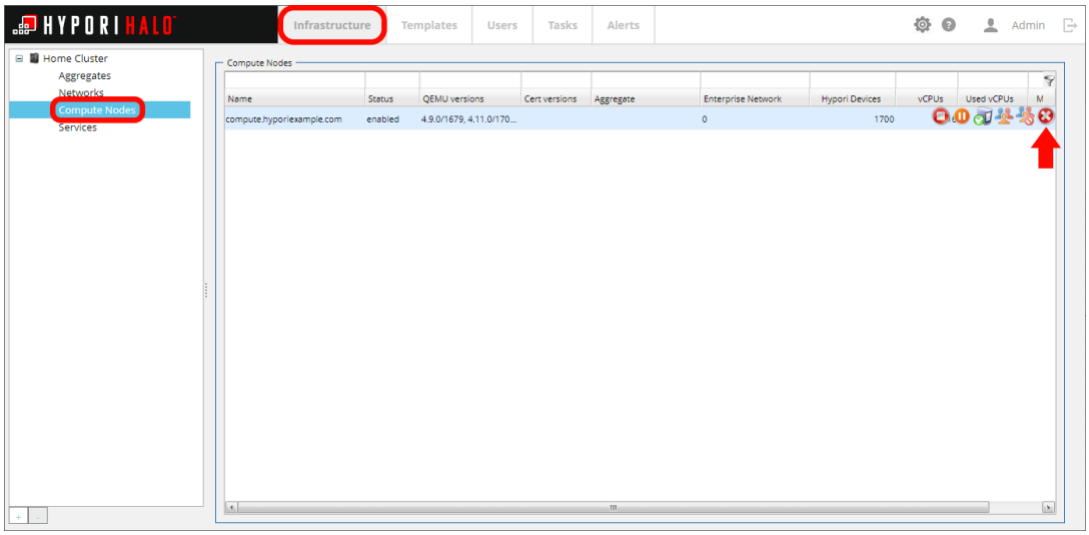
Deleting All Virtual Workspaces on a Compute Node

To delete all virtual workspaces on a compute node:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Infrastructure**.
3. In the navigation pane, expand the server cluster and click **Compute Nodes**.
4. In the table, hover your cursor over the compute node.
5. Click the **Delete Hypori Devices** icon:

6. In the confirmation box, click **Yes**.



Tip:

You can also delete specific virtual workspaces. For more information, see Deleting a Virtual Workspace *(on page 104)*.

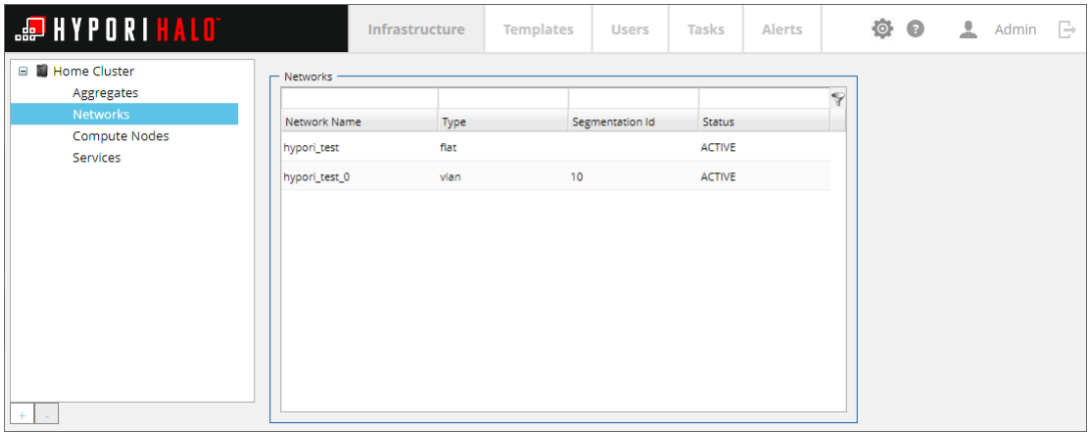
Monitoring Server Clusters

You can monitor and troubleshoot the server cluster using the data in the Hypori Halo Admin Console.

Viewing Networks

To view the information about the enterprise network:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Infrastructure**.
3. In the navigation pane, expand the server cluster and click **Networks**.



The Networks screen shows:

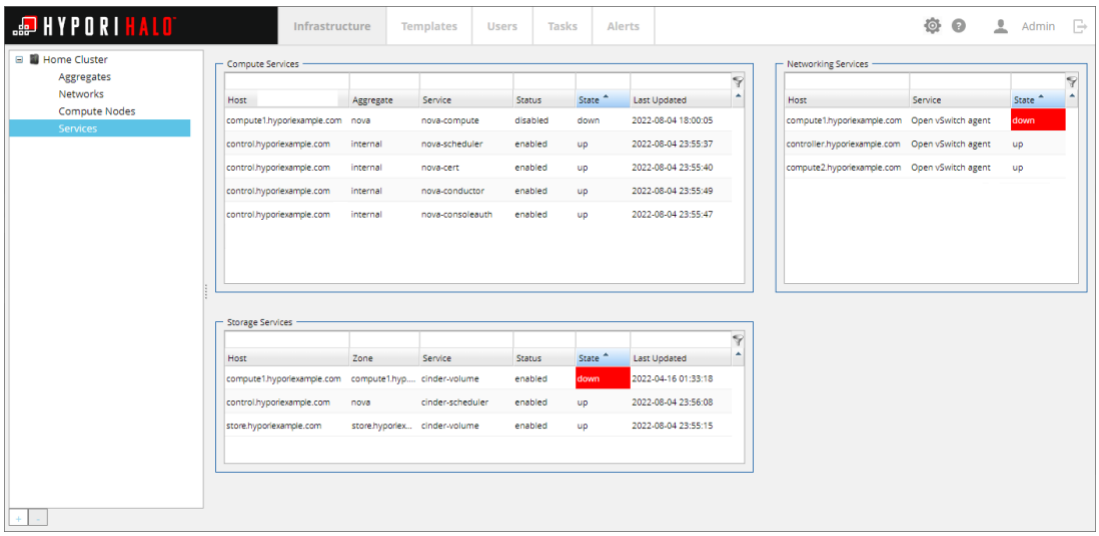
- **Network Name:** The name of the enterprise network, which provides virtual workspaces with access to shared resources in your enterprise.
- **Type:** The type of network design in use for the identified network.
- **Status:** The status of the network.

Viewing Services

To view service information for a server cluster:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Infrastructure**.

3. In the navigation pane, expand the server cluster and click **Services**.



The Services screen shows:

- **Host:** The name of the compute, networking, or storage service host.
- **Aggregate:** The name of the aggregate associated with the service.
- **Zone:** The storage zone associated with the service.
- **Service:** The name of the service.
- **Status:** The status of the service (for compute and storage services only).
- **State:** The current state of the service. Services in the Down state are shown in red.
- **Last Updated:** The date when the service was last updated.

Note:
Not all fields are available for all services.

The following services are available:

Compute Services

Service	Component	Description	Log File
nova-conductor	controller	A module that mediates interactions between nova-compute and the database. Its goal is to eliminate direct accesses to the	`/var/log/nova/conductor.log`

Service	Component	Description	Log File
		cloud database made by nova-compute.	
nova-consoleauth	controller	A daemon that authorizes tokens for users that console proxies provide. This service must be running for console proxies to work.	Unneeded
nova-scheduler	controller	A process that takes a virtual machine instance request from the queue and determines on which compute node it should run.	`/var/log/nova/scheduler.log`
nova-cert	controller	A daemon that manages x509 certificates.	`/var/log/nova/cert.log`
nova-compute	compute	A process that creates and terminates virtual workspace instances through hypervisor APIs.	`/var/log/nova/compute.log`

Storage Services

Service	Component	Description	Log File
cinder-scheduler	controller	A daemon that picks the optimal block storage provider node on which to create the volume.	`/var/log/cinder/scheduler.log`
cinder-volume	compute	A service that responds to requests to	`/var/log/cinder/volume.log`

Service	Component	Description	Log File
		read from and write to the Block Storage database to maintain state.	

Networking Services

Service	Component	Description	Log File
Open vSwitch agent	compute	An agent with vSwitch configurations that consist of bridges and ports. Ports represent connections to other things. Packets from any given port on a bridge are shared with all other ports on that bridge.	`/var/log/neutron/openvswitch-agent.log`
Open vSwitch agent	controller	An agent with vSwitch configurations that consist of bridges and ports. Ports represent connections to other things. Packets from any given port on a bridge are shared with all other ports on that bridge.	`/var/log/neutron/openvswitch-agent.log`

Chapter 4. Templates

Every virtual workspace running on the server has a template that defines its properties. Templates enable multiple virtual workspaces running on the server to use the same set of properties.

Your organization may have templates with different mobile apps, amounts of storage space, and formats. Each user is assigned a template that determines the look and feel and contents of his or her virtual workspace. Users with the same template are given identical virtual workspaces, making them easier to support.

A template must have a published image and a flavor. For more information, see Published Images *(on page 49)* and Flavors *(on page 53)*.

Viewing Template Metrics

To view template usage metrics:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Templates**.
3. In the navigation pane, select the root node.

Tip:

If you want to view information for a specific server cluster, select that server cluster in the navigation pane.

The Templates page shows the following graphs:

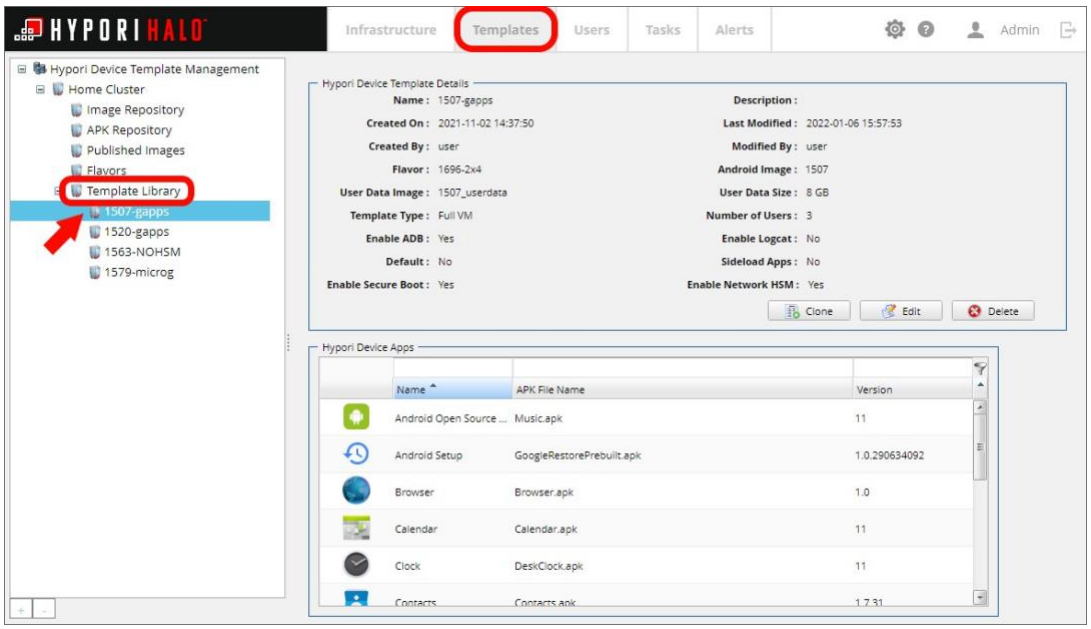
- **Template Usage:** The number of users with each template.
- **Flavor Usage:** The number of users with each flavor.
- **Android Image Usage:** The number of users with each published image.

Viewing Template Details

To view template details:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Templates**.
3. In the navigation pane, select the server cluster and click the **Template Library** node.

4. Select a template sub-node.



The Hypori Device Template Details area shows:

- **Name:** The name of the template.
- **Created On:** The date and time when the template was created.
- **Created By:** The user who created the template.
- **Flavor:** The flavor for the template.
- **User Data Image:** The published image (storage) for the template.
- **Template Type:** Full VM is the only type of template supported.
- **Enable ADB:** Whether the template supports Android Debug Bridge functionality. (This feature enables the administrator to connect to the virtual workspace's ADB port to perform debugging operations.)
- **Default:** Whether the template is the default for new virtual workspaces.
- **Enable Secure Boot:** Whether the template supports Secure Boot functionality.
- **Description:** A description of the template.
- **Last Modified:** The date and time when the template was last modified.
- **Last Modified:** The user who last modified the template.
- **Android Image:** The published image (operating system and apps) for the template.
- **User Data Size (GB):** The amount of data storage available for virtual workspaces that are based on the template, in GB.
- **Number of Users:** The number of users with virtual workspaces based on the template.
- **Enable Logcat:** Whether the template supports logcat functionality.

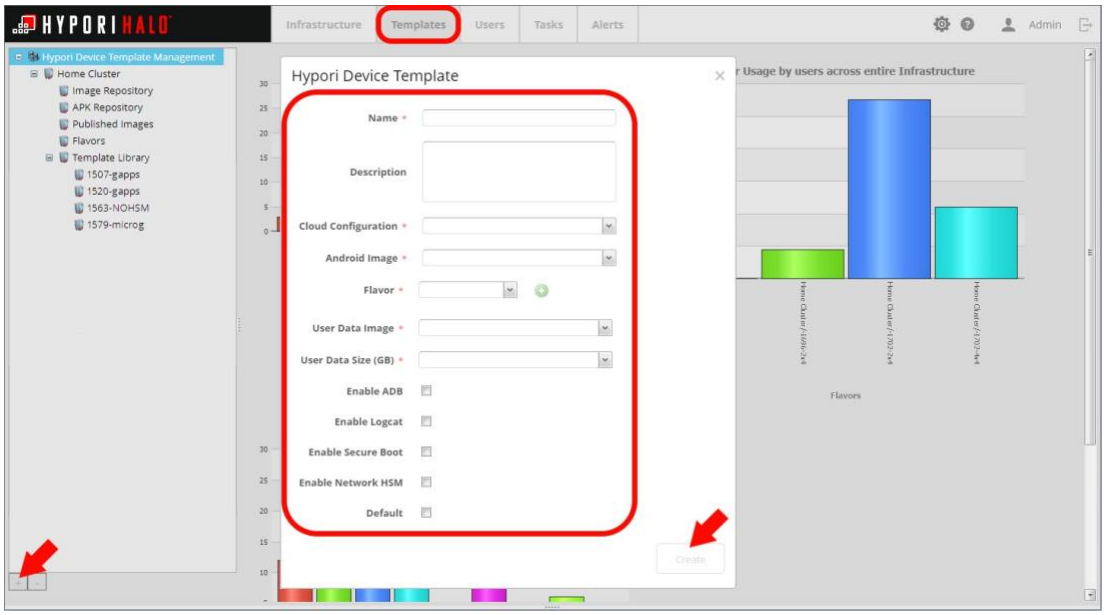
- **Sideload Apps:** Whether users can download and install apps onto their virtual workspace.
- **Enable Network HSM:** Whether the template supports network Hardware Security Module (HSM) functionality.

Adding a New Template

Important:
Before you begin, you must add both a published image and a flavor. See Adding a Published Image *(on page 50)* and Adding a Flavor *(on page 54)* for more information and instructions to add those components.

To add a new template:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Templates**.
3. At the bottom of the navigation pane, click the **add** (**+**) icon.
4. In the Hypori Device Template box, provide the following information:



- **Name:** The name of the template.
- **Description:** A description of the template.
- **Cloud Configuration:** The server cluster associated with the template.
- **Android Image:** The published image (operating system and apps) for the template.
- **Flavor:** The flavor for the template.
- **User Data Image:** The published image (storage) for the template.

- **User Data Size (GB):** The amount of data storage available for virtual workspaces that are based on the template, in GB.
- **Enable ADB:** Whether the template supports Android Debug Bridge functionality. (This feature enables the administrator to connect to the virtual workspace's ADB port to perform debugging operations.)
- **Enable Logcat:** Whether the template supports logcat functionality.
- **Enable Secure Boot:** Whether the template supports Secure Boot functionality.
- **Enable Network HSM:** Whether the template supports network Hardware Security Module (HSM) functionality.
- **Default:** Whether the template is the default for new virtual workspaces.

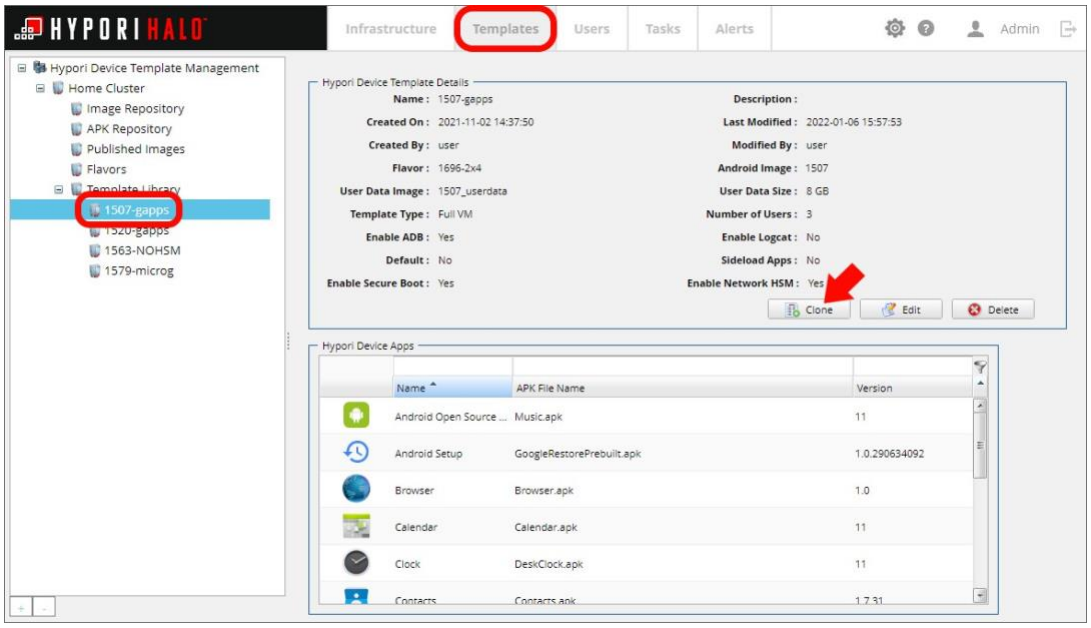
When the required information has been entered, the Create button will no longer be greyed out.

5. Click **Create**.
   The new template is added to the template library and can be applied to any virtual workspace in the server cluster.

Cloning an Existing Template

To clone an existing template:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Templates**.
3. In the navigation pane, select the server cluster and click to expand the **Template Library** node
4. Select the template sub-node you want to clone.
5. In the Hypori Device Template Details area, click **Clone**.



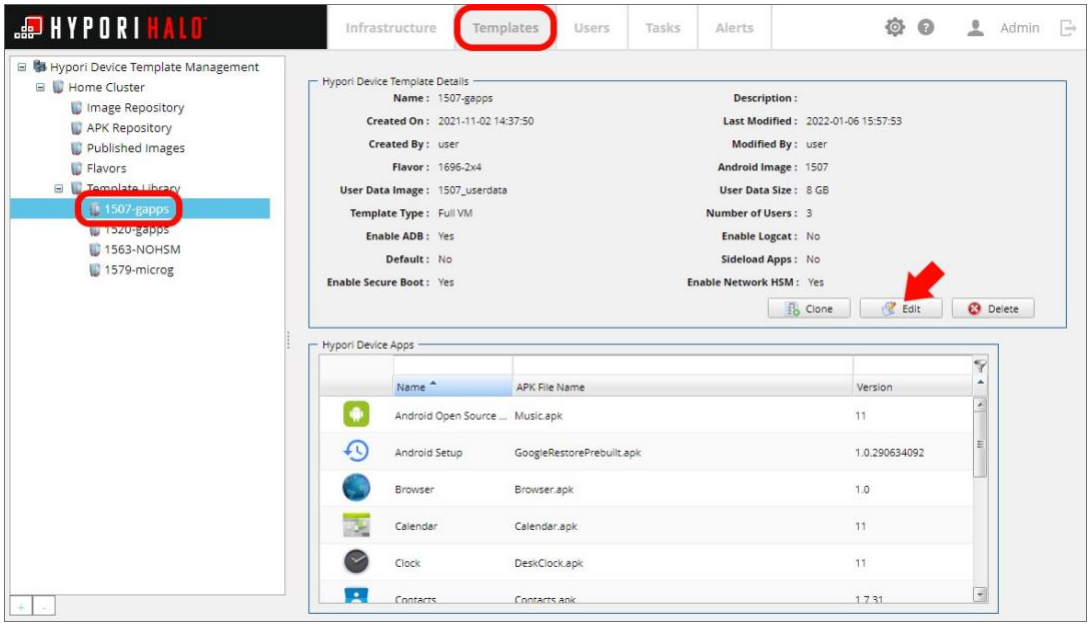
6. In the Hypori Device Template box, modify the following information as needed:
    - **Name:** The name of the template.
    - **Description:** A description of the template.
    - **Template Type:** Full VM is the only type of template supported.
    - **Cloud Configuration:** The server cluster associated with the template.
    - **Android Image:** The published image (operating system and apps) for the template.
    - **Flavor:** The flavor for the template.
    - **User Data Image:** The published image (storage) for the template.
    - **User Data Size (GB):** The amount of data storage available for virtual workspaces that are based on the template, in GB.
    - **Enable ADB:** Whether the template supports Android Debug Bridge functionality. (This feature enables the administrator to connect to the virtual workspace's ADB port to perform debugging operations.)
    - **Enable Logcat:** Whether the template supports logcat functionality.
    - **Default:** Whether the template is the default for new virtual workspaces.
7. Click **Create**.

   The new template is added to the template library.

Editing an Existing Template

To edit an existing template:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Templates**.
3. In the navigation pane, select the server cluster and click to expand the **Template Library** node.
4. Select the template sub-node you want to edit.
5. In the Hypori Device Template Details area, click **Edit**.



6. In the Edit Hypori Device Template box, modify the following information as necessary:
    - **Name:** The name of the template.
    - **Description:** A description of the template.
    - **Template Type:** Full VM is the only type of template supported.
    - **Android Image:** The published image (operating system and apps) for the template.
    - **Flavor:** The flavor for the template.
    - **User Data Image:** The published image (storage) for the template.
    - **User Data Size (GB):** The amount of data storage available for virtual workspaces that are based on the template, in GB.
    - **Enable ADB:** Whether the template supports Android Debug Bridge functionality. (This feature enables the administrator to connect to the virtual workspace's ADB port to perform debugging operations.)
    - **Enable Logcat:** Whether the template supports logcat functionality.
    - **Default:** Whether the template is the default for new virtual workspaces.
7. Click **Apply**.

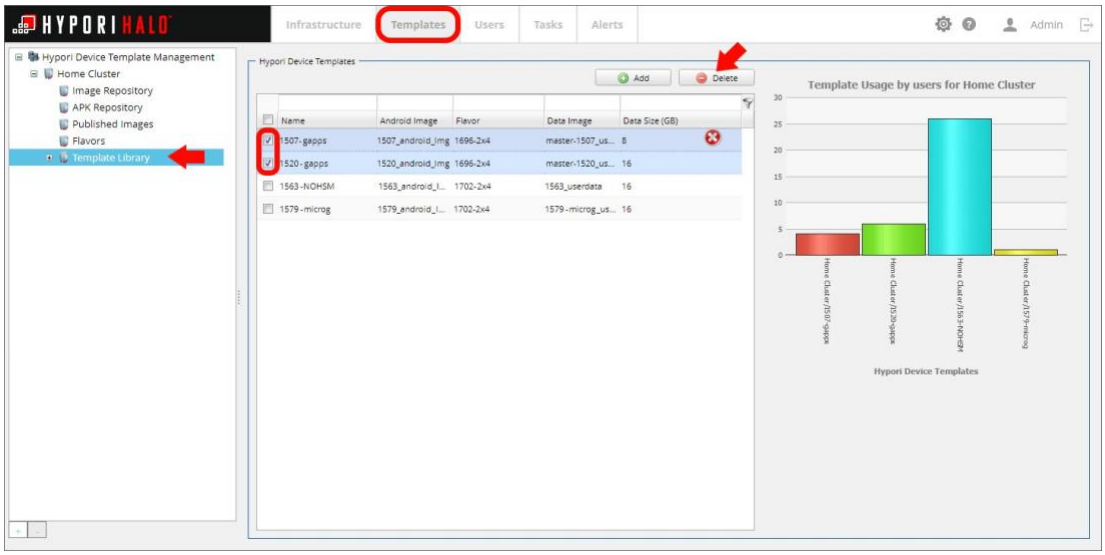
Tip:

You cannot edit a template that is in use.

Deleting a Template

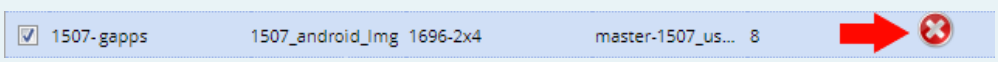
To delete a template:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Templates**.
3. In the navigation pane, select the server cluster and click to highlight the **Template Library** header.
4. In the Hypori Device Templates table, check the box next to the template(s) that you want to delete.
5. In the display area, at the upper right above the Hypori Device Templates table, click **Delete**.



Tip:

You can also delete a template by holding your cursor over the row in the table and clicking the **Delete** icon.



6. In the confirmation box, click **Yes** to remove the template from the server cluster.

Tip:
You cannot delete a template that is in use.

Images

Images are TGZ files that define the Android image for a template. Images are saved in an image repository, and each server cluster has its own image repository.

There must be an image in the image repository, and you must publish it before you can create a template. The Hypori Halo system is shipped with at least one image and additional images can be added. Typically, a new image is only necessary when an updated version of the virtual workspace is shipped from Hypori.

Contact Hypori Halo Support for assistance with creating a new image.

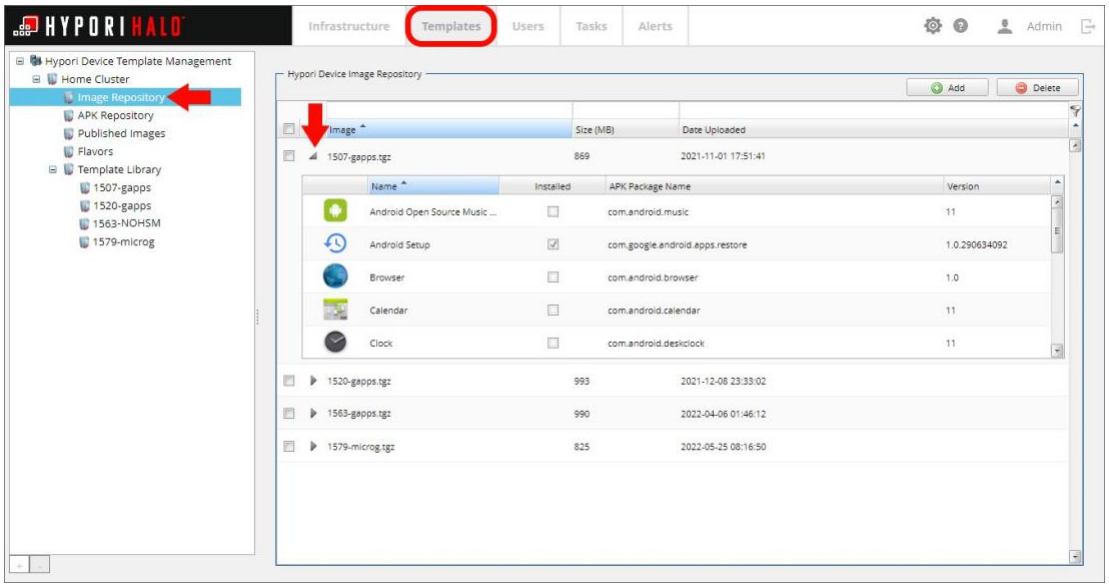
Viewing the Image Repository

The Image Repository contains the images (TGZ files) that define the operating system for a virtual workspace.

To view the list of images in the repository:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Templates**.
3. In the navigation pane, select a server node and click **Image Repository**.
   The list of installed images will be displayed.

4. Click the arrow to the left of the Image column to expand the repository and display the list of apps contained in the image.



For each image, the Hypori Device Image Repository table shows:

- **Image:** The image file name.
- **Size (MB):** The size of the image file, in MB.
- **Date Uploaded:** The date and time that the image file was uploaded to the image repository.

Tip:
To filter the list, select the field above the column heading name, type all or a portion of name or the value, then select the filter icon at the upper right corner of the table.

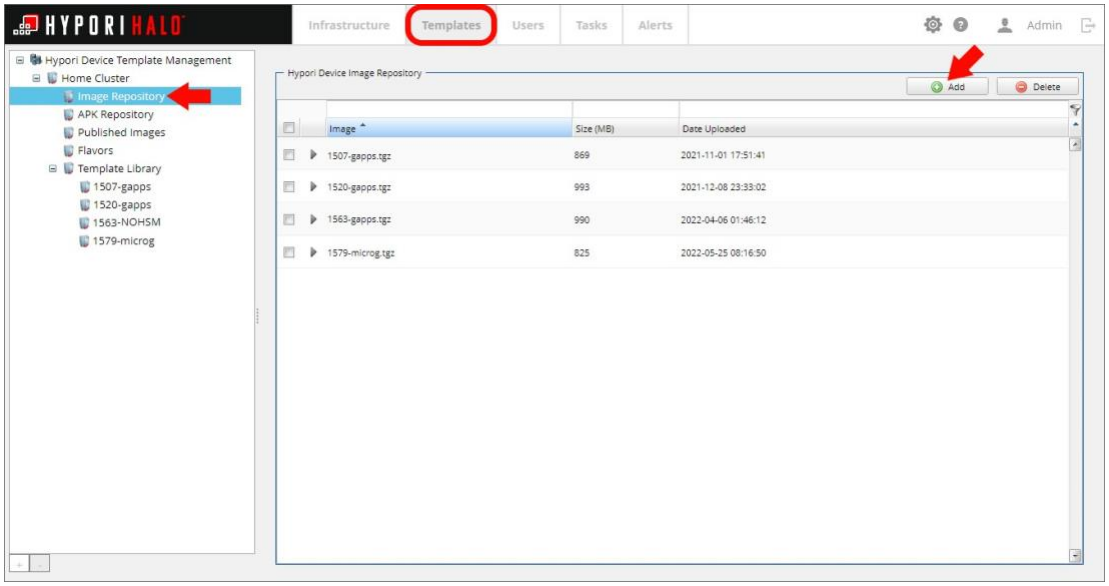
Adding an Image

The Image Repository contains the images (TGZ files) that define the operating system for a virtual workspace. Before you begin, you must have a TGZ file to upload. Contact Product Support *(on page 6)* for more assistance with adding an image.

Note:
After you add an image, you must publish it before you can use it in a template. For more information, see Adding a Published Image *(on page 50)*.

To add an image to the repository:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Templates**.
3. In the navigation pane, select the server cluster where the new image will reside, then click **Image Repository**.
4. Under Hypori Device Image Repository, click **Add**.

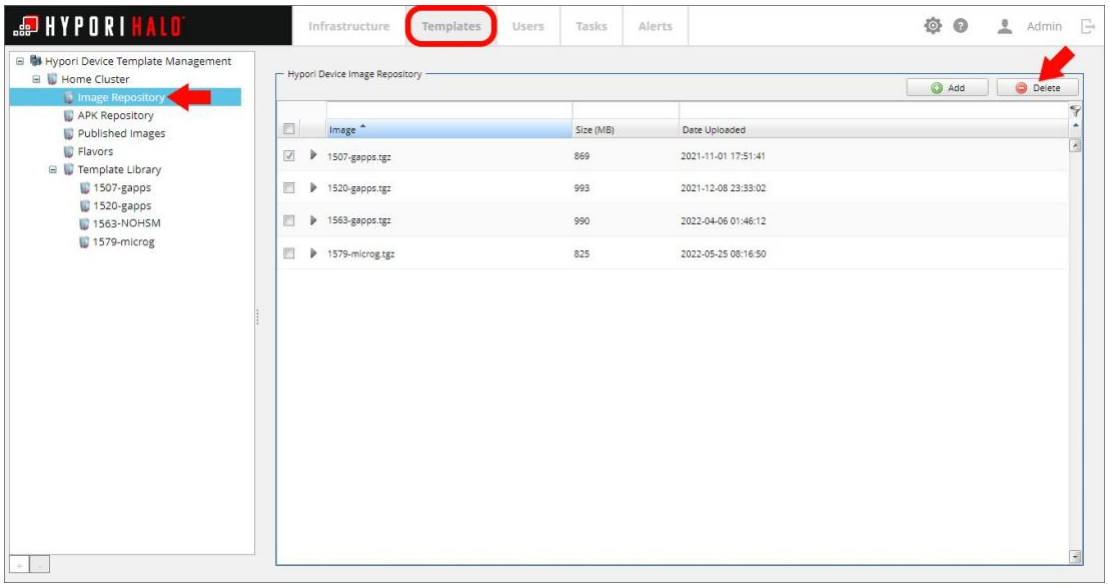


5. Click **Browse**.
6. Select the file you want to upload and click **Upload**.

Deleting an Image

To delete images from the Image Repository:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Templates**.
3. In the navigation pane, select the server cluster containing the image to be deleted, then click **Image Repository**.
4. Under Hypori Device Image Repository, check the box next to the image you are deleting.
5. Click **Delete**.



Tip:

You can also delete an image by holding your cursor over the row in the table and clicking the **Delete** icon:

6. In the confirmation box, click **Yes**.

Tip:

You cannot delete an image that is in use.

APK Files

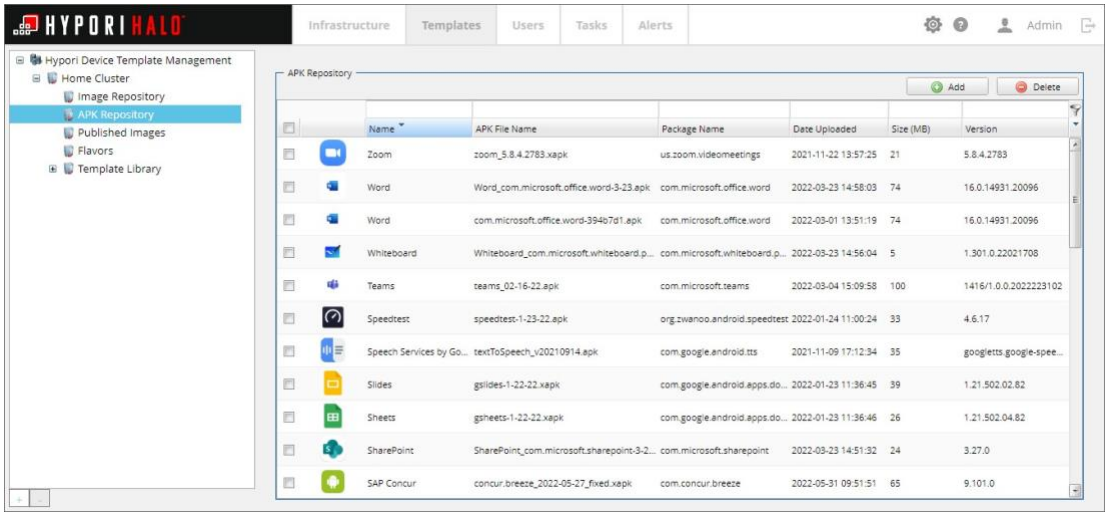
Android application package (APK) files are used to distribute and install mobile apps on devices that run the Android operating system. APK files are saved in the APK repository, and each server cluster has its own APK repository.

For each app that users can access on their virtual workspace, you must have a corresponding APK file in the APK repository and you must include that APK file in a published image that is part of a template.

Viewing the APK Repository

To view the list of available APKs:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Templates**.
3. In the navigation pane, select the server cluster then click **APK Repository**.



For each APK file, the APK Repository table shows:

- **Name:** The app name.
- **APK File Name:** The full name of the APK file.
- **Package Name:** The full name of the app package.
- **Date Uploaded:** The date and time when the APK file was uploaded to the APK Repository.
- **Size (MB):** The size of the APK file, in megabytes.
- **Version:** The app version number.

Tip:
To filter the list, select the field above the column heading name, type all or a portion of the name or the value, then select the filter icon at the upper right corner of the table.

Extracting APK Apps (Single & Split)

1. Login to your Hypori Halo Client using an account that utilizes a GAPPS image.
   For more information about finding your image, see Viewing Published Images *(on page 49)*.
2. Open the Hypori Halo Admin Console.
3. Find the Volume ID.
   a. Click **Users**.
   b. Locate the device you are logged to on the list.
   c. Hover your cursor over the device's entry and select the **Stop Hypori Device** icon.

   d. Click **User Details**.

   e. Record the entries under Hypori Device Compute Node & the Hypori Device Volume ID.
4. SSH into the compute node recorded in the previous step. Run:

```
ssh <account_name>@<compute_node's_IP_address>
```

5. Elevate Privileges. Run:

```
sudo su -
```

6. Create a temporary directory. Run:

```
mkdir /tmp/mnt
```

7. Change to directory where Hypori Device Volumes are stored. Run:

```
cd /var/lib/nova/mnt/<Hypori_Storage_GUID>
```

8. Mount the Hypori Device's Volume ID (from step 3e).

```
mount -o loop volume-<Volume_ID_from_step_3e> /tmp/mnt
```

9. Change to directory to where apps are stored. Run:

```
cd /tmp/mnt/app
```

Note:

Each Android app has its own directory.

```
[root@compute2 app]#  ls
com.adobe.reader-ACVg6oP-(JNFRu9mTRGjlj==    com.google.android.quicksearch-LY_7Fu79eAjvdxw==
com.aefyr.sai-P0lomh09JKr-2klp==             com.google.android.soundpicker-Se4X7YeEQjm-3pp==
com.android.vending-410Lv-Pan8kHo9wjhtg==    com.google.android.tts-0E8yhWDvUTiLAuAbKH0tjg==
com.cisco-im-bDm5mmv84TiONG6h0jg==           com.iraavanan.apkextractor-hJqd5mm84iNGhj5g==
com.dropbox.android-tLmMEEX3pFTgmdlZMG==     com.linkedin.android-PiipmEX3pTgdZGB2deBb59==
com.google.android.gms-2pG6WpkxSCTVloxqX==   com.microsoft.office.excel-fk8rp6pxCVG9CS4C-VQQ==
```

10. Change the directory to the desired destination app directory.
11. Determine if your Android app is a Single APK or a Split (multiple files) APK.
    - **Single APK**

      ```
      [root@compute2 app]# cd com.microsoft.office.excel-fkp6pxCVG9CS4C-VQQ\=\=/
      [root@compute2 com.microsoft.office.excel-fkp6pxCVG9CS4C-VQQ==]# ls
      base.apk  lib  oat
      ```

    - **Split APK**

      ```
      [root@compute2 app]# cd com.cisco-im-bDm5mmv84TiONG6h0jg\=\=/
      [root@compute2 com.cisco-im-bDm5mmv84TiONG6h0jg==]# ls
      base.apk  lib  oat  split_config.armeabi_v7a.apk  split_config.en.apk  split_config.mdpi.apk
      ```

12. Move and rename the APK files.
    - **Single APK**
      a. Copy the file to `/home/hypori` directory, while renaming it to identify the app/version.

      ```
      [root@compute2 com.microsoft.office.excel-fk8rp6pxCVG9CS4C-VQQ==]# cp base.apk /home/hypori/excel_16.0.12827.20140.apk
      [root@compute2
      ```

    - **Split APK**
      a. Zip the `.apk` files identified in the previous step and rename them to identify the app/version using a `.xapk` file extension.

      ```
      [root@compute2 com.cisco.im-bDm5mmv84TiONG6h0jg==]# zip -r jabber_12.8.2.302880.xapk . -i \*.apk
        adding: split_config.armeabi_v7a.apk (deflated 66%)
        adding: base.apk (deflated 21%)
        adding: split_config.mdpi.apk (deflated 13%)
        adding: split_config.en.apk (deflated 90%)
      ```

      ```
      zip -r <file_name (e.g., jabber_12.8.2.302880)>.xapk -i \*.apk
      ```

      b. Move the created `.xapk` file to the `/home/hypori` directory. Run:

      ```
      mv <file_name (e.g., jabber_12.8.2.302880.xapk)> /home/hypori
      ```

13. Change the directory to `/tmp` and unmount the User Device Volume. Run:

    ```
    cd /tmp

    umount /tmp/mnt
    ```

14. Change the directory to `/home/hypori` to prep files for extraction. Run:

    ```
    cd /home/hypori
    ```

15. Check SELinux context on the new `.apk` and `.xapk` files. Run:

    ```
    ls -lZ
    ```

Note:

The 'type' should match 'user_home_t' to allow for file extraction.

```
[root@compute2 hypori]# ls -lZ
-rw-r---r--. root   root   staff_u:object_r:user_home_t:s0 apps.zip
-rw-------. root   root   staff_u:object_r:user_home_t:s0 bugreport-peas-PQ3B.190801.002-2020-05-21-14-15-45.zip
-rw-r---r--. root   root   staff_u:object_r:user_home_t:s0 bug.zip
-rw-r---r--. hypori splunk staff_u:object_r:user_home_t:s0 device_owner_2.xml
-rw-r---r--. root   root   staff_u:object_r:user_home_t:s0 excel_16.0.12827.20140.apk
-rw-------. root   root   staff_u:object_r:user_home_t:s0 instance-0000002c.log
-rw-r---r--. root   root   staff_u:object_r:user_home_t:s0 instance.zip
-rw-r---r--. root   root   staff_u:object_r:user_home_t:s0 jabber_12.8.2.302880.xapk
-rw-r---r--. root   root   staff_u:object_r:user_home_t:s0 jabber.xapj
-rw-r---r--. root   root   staff_u:object_r:user_home_t:s0 pb.p12
```

16. Verify the SELinux content type matches. If the SELinux context type does not match, change the context of the file. Run:

    ```
    chcon staff_u:object_r:user_home_t:s0 <file name (e.g.: jabber_12.8.2.302880.xapk)>
    ```

17. Secure copy the `.apk` and/or `.xapk` files to your admin workstation.
18. Upload the files to the Hypori Halo Admin Console.

Adding APK Files

After you add an APK file, you must include it in a published image before you can use it in a template. For more information, see Adding a Published Image *(on page 50)*.

Important:
Do not add an APK unless you have a license to distribute the app. In addition, you should use APKs with x86 native libraries instead of ARM for maximum compatibility.

To acquire an APK file and add it to the APK repository:

1. On a virtual workspace, install the app and then update it to ensure it is the most recent version.

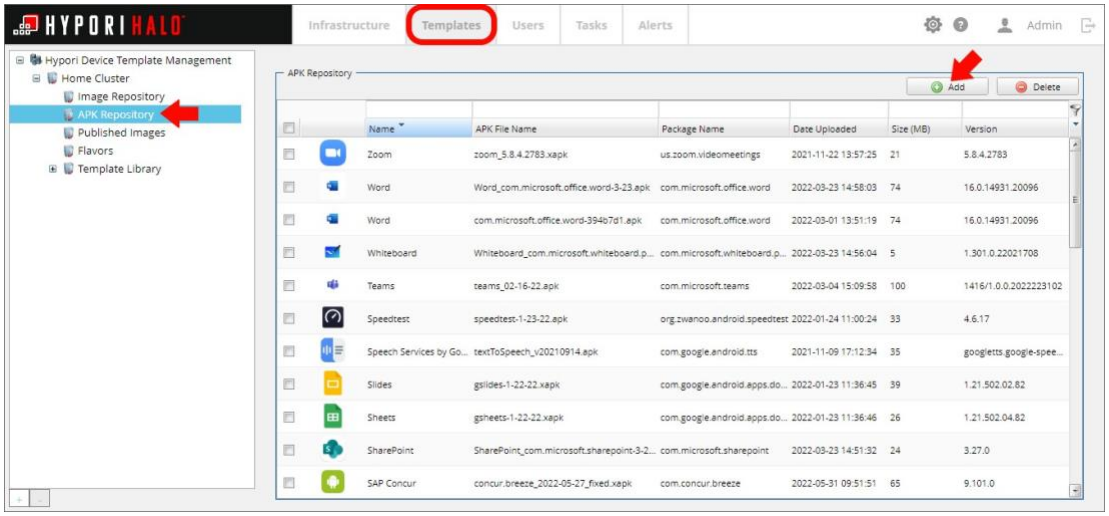
   Note:
   This requires access to a digital distribution platform or mobile device management app.

2. Extract the app from the virtual workspace.

   Note:
   This requires access to an app that enables you to share an APK file.

3. Save the file to your computer.
4. Open the Hypori Halo Admin Console.

5. In the menu, click **Templates**.
6. In the navigation pane, select the server cluster then click **APK Repository**.
7. Click **Add**.

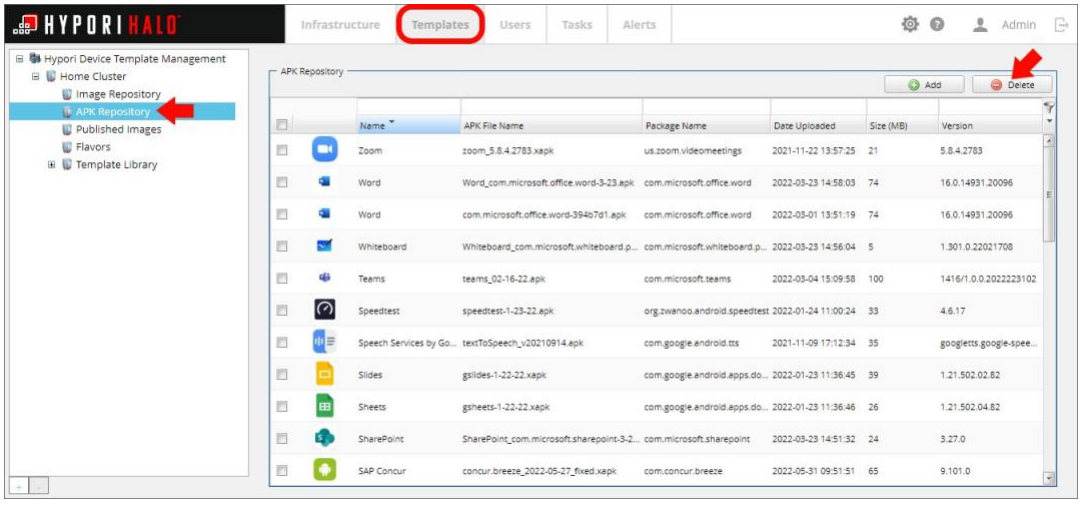


8. Click **Browse**.
9. Select the APK file that you want to upload then click **Upload**.

Deleting APK Files

To delete APK files from the APK repository:

1. In the navigation pane, select the server cluster.
2. In the menu, click **Templates**.
3. In the navigation pane, select the server cluster and click **APK Repository**.
4. Check the box next to one or more APK files that you want to delete.
5. Click **Delete**.



Tip:

You can also delete a single APK file by hovering your cursor over the row in the table then clicking the **Delete** icon:

6. In the confirmation box, click **Yes**.

Tip:

You cannot delete an APK file that is in use.

Published Images

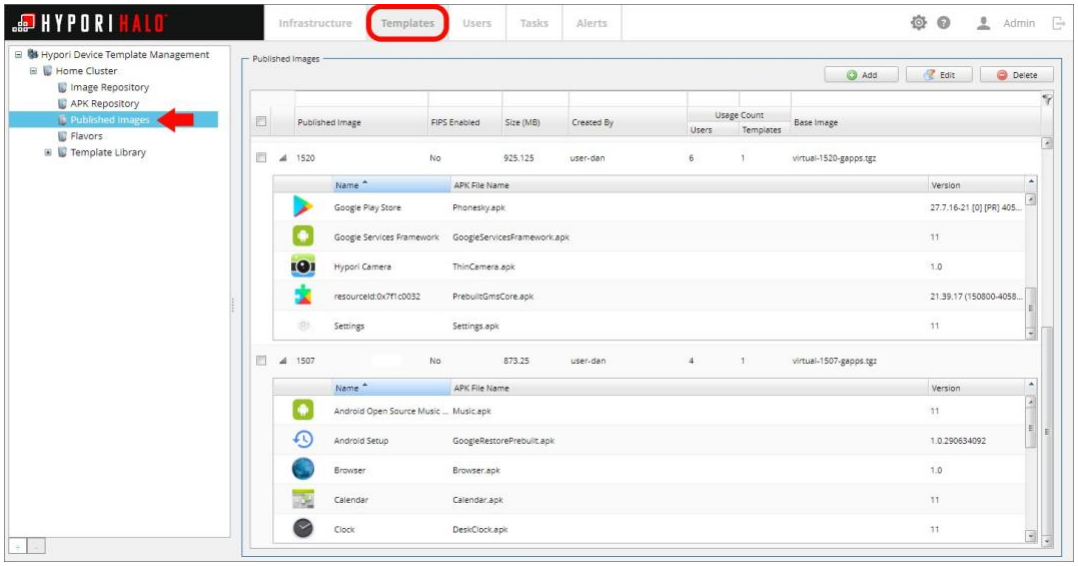
Before you can add an image to a template, you must publish it. A published image contains an image and apps (APK files).

Viewing Published Images

A published image is the combination of an image (the operating system) and one or more apps.

To view the list of published images:

1. In the navigation pane, select the server cluster.
2. In the menu, click **Templates**.
3. In the navigation pane, select the server cluster then click **Published Images**.



For each published image, the Images table shows:

- **Published Name:** The name of the published image.
- **FIPS Enabled:** Whether the published image has been marked as compliant with Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2).
- **Size (MB):** The size of the published image.
- **Created By:** The user who created the published image.
- **Usage Count:** The number of users and templates using this published image.
- **Base Image:** The Android image used for the published image.

Select the arrow to the left of the Published Image column to see the list of apps.

To filter the list:

- Select the field above the column heading name, type all or a portion of name or the value then select the filter icon at the upper right corner of the table.

To see the user count for each published image:

- Hold your cursor over each bar in the Android Image Usage by Users graph.

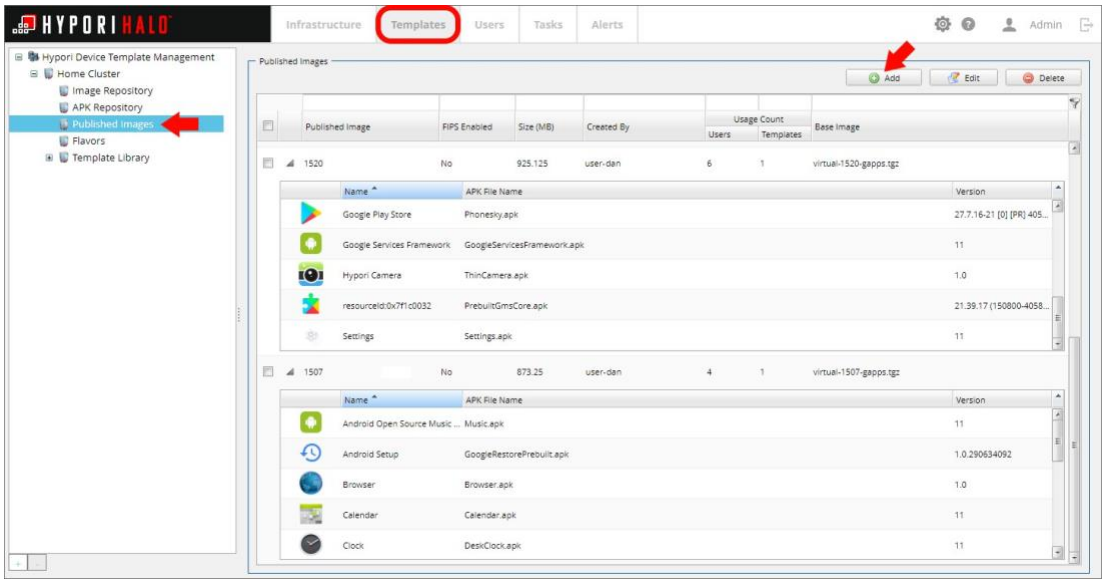
Adding a Published Image

Before you publish an image, you must have at least one image saved in the image repository. For more information, see Adding an Image *(on page 41)*. You should also add any apps (APK files) that you want to include in the published image to the APK repository. For more information, see Adding APK Files *(on page 47)*.

After you publish an image, you can include it in a template. For more information, see Adding a New Template *(on page 35)*.

To create a published image:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Templates**.
3. In the navigation pane, select the server cluster and click **Published Images**.
4. Under Published Images, click **Add**.



5. In the Publish Image box, in the **Name** field, type a descriptive name for the new published image.
6. In the **Select Hypori Image** list, select an image file to associate with this published image.
7. Click **Enable FIPS** if this image must comply with Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2).
8. Under **Select APKs to Include**, check the box next to one or more apps that you want to add to the published image.

> **Tip:**
> It is recommended to include the Downloads app in the published image. Some files may not open correctly if the app is not installed.

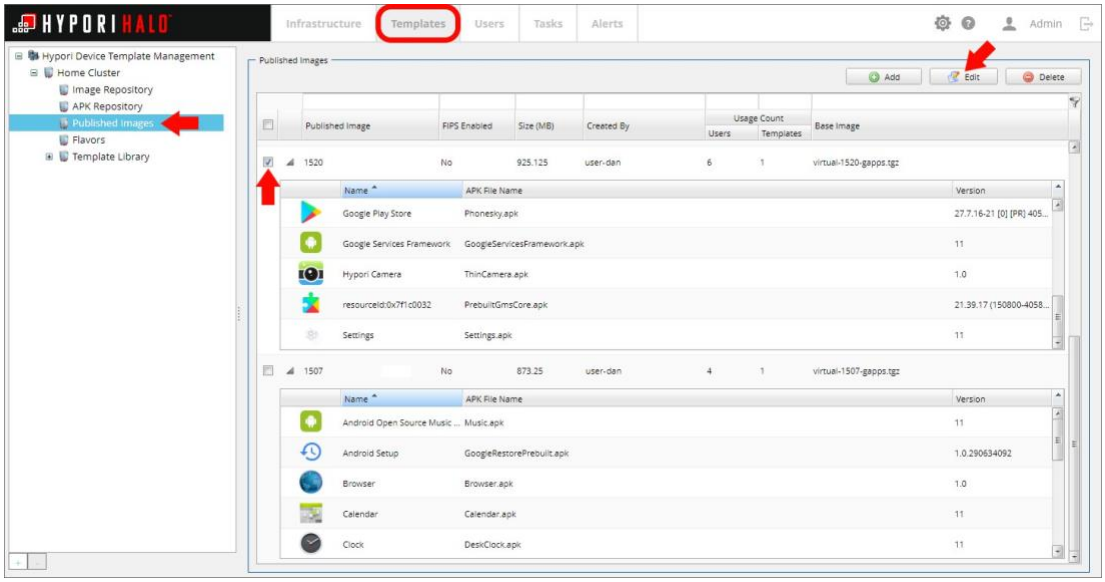
9. Click **Publish**.
10. In the confirmation box, click **Yes**.
11. At the scheduled job confirmation prompt, click **OK**.
    After the scheduled job completes, the new published image is added to the list of published images.

Editing Published Images

To edit a published image:

1. In the menu, click **Templates**.
2. In the navigation pane, select the server cluster and then click **Published Images**.

3. Under Published Images, select the checkbox next to the published image that you want to edit.
4. Click **Edit**.



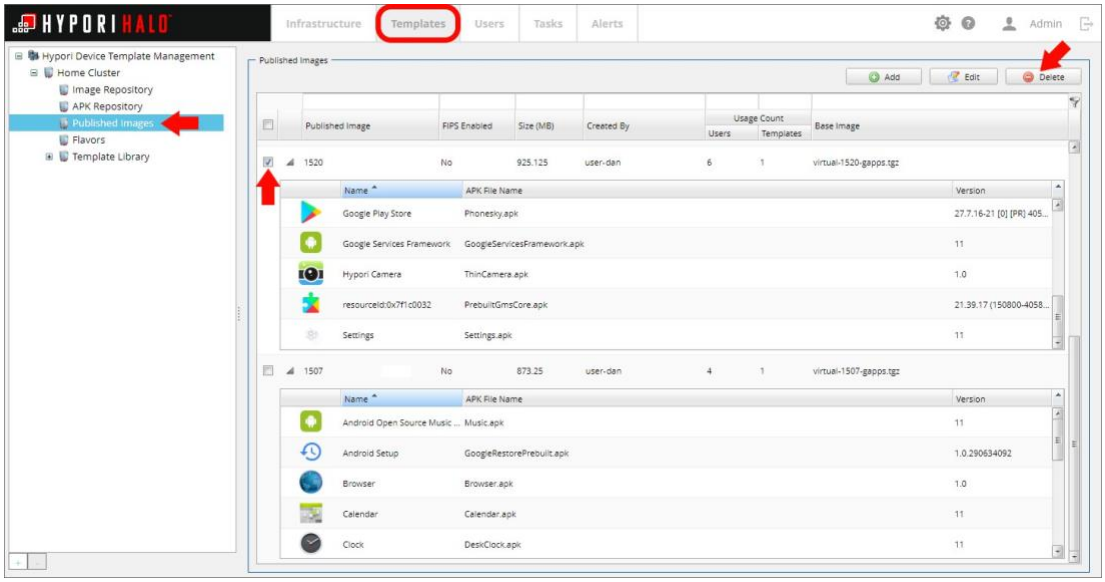
5. In the Publish Image box, in the **Name** field, modify the name for the new published image, as needed.
6. In the **Select Hypori Image** list, select a different image file to associate with this published image, as needed.
7. Click **Enable FIPS** if this image must comply with Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2).
8. Under Select APKs to Include, check the box next to one or more apps that you want to add to the published image. Clear the check from the box next to any apps you do not want to include.
9. Click **Publish**.
10. In the confirmation box, click **OK**.
11. At the scheduled job confirmation prompt, click **OK**.
    After the scheduled job completes, the new published image is added to the list of published images.

Tip:
You cannot delete a published image that is in use.

Deleting Published Images

To delete a published image from the repository:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Templates**.
3. In the navigation pane, select the server cluster containing the image(s) to be deleted, then click **Published Images**.
4. Under Published Images, check the box next to one or more images that you want to delete.
5. Click **Delete**.



6. In the confirmation box, click **Yes** to delete the selected image(s).

Tip:
You cannot delete a published image that is in use.

Flavors

Flavors define the memory, processor, and storage values for templates. You must have a flavor before you can create a template.

Viewing Flavors

To view the flavors associated with the selected server cluster:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Templates**.
3. In the navigation pane, select the server cluster and click **Flavors**.

For each flavor, the Flavors table shows:

- **Name:** The name of the flavor.
- **vCPUs:** The number of virtual CPUs associated with this flavor. (Typically, 2)
- **Memory (MB):** The available memory (shown in MB) for this flavor. Usable values include:
  - 1024 (1024 MB = 1 GB)
  - 2048 (2048 MB = 2 GB)
  - 4096 (4096 MB = 4 GB)
  - 8192 (8192 MB = 8 GB)

  Important:
  There is a bug in the Admin Console when filtering memory values. You must enter the full numerical value (e.g., 1024, 2048, 4096, 8192) for results to be returned. Incomplete numerical values (i.e., 1, 20, 409, 192, etc.) will not return any results.
- **Disk (GB):** The available disk storage for this flavor.
- **QEMU Version:** The QEMU (Hosted virtual machine monitor) version.
- **Cert Version:** The certificate version number.

To see the user count for each flavor, hold your cursor over each bar in the Flavor Usage by User graph.

Adding a Flavor

After you add a flavor, you can include it in a template. For more information, see Adding a New Template *(on page 35)*.

To define a new flavor:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Templates**.
3. In the navigation pane, select the server cluster and click **Flavors**.
4. In the display area, at the upper right above the Flavors table, click **Add**.
5. In the Flavor Configuration box, provide the following information:
   - **Name:** The name of the flavor.
   - **vCPUs:** The number of virtual CPUs associated with this flavor. (Typically, 2)
   - **Memory (MB):** The available memory (shown in MB) for this flavor. Usable values include:

- 1024 (1024 MB = 1 GB)
- 2048 (2048 MB = 2 GB)
- 4096 (4096 MB = 4 GB)
- 8192 (8192 MB = 8 GB)

Important:

There is a bug in the Admin Console when filtering memory values. You must enter the full numerical value (e.g., 1024, 2048, 4096, 8192) for results to be returned. Incomplete numerical values (i.e., 1, 20, 409, 192, etc.) will not return any results.

- **QEMU Version:** The QEMU (Hosted virtual machine monitor) version.
- **Cert Version:** The certificate version number.

6. Click **Create** to save the new flavor definition.

   The new flavor is added to the Flavors table and to the Flavor Usage by Users graph.

Deleting a Flavor

To delete an existing flavor definition:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Templates**.
3. In the navigation pane, select the server cluster containing the flavor being deleted and click **Flavors**.
4. In the Flavors table, check the box next to the flavor that you want to delete.
5. In the display area, at the upper right above the Flavors table, click **Delete**.

Tip:

You can also delete a flavor by holding your cursor over the row in the Flavors table and clicking the **Delete** icon: 

6. In the confirmation box, click **Yes**.

   The flavor is deleted from the server cluster and removed from the Flavors table and the Flavor Usage by Users graph.

Tip:

You cannot delete a flavor that is in use.

Chapter 5. Users and their Virtual Workspaces

Each user must have a user account to access the Hypori Halo environment.

A Hypori Halo user has:

- A user license that enables the user to access the Hypori Halo environment.
- A client certificate that enables the user to access his or her virtual workspace or the Hypori Halo web apps.
- A domain that includes configuration and permission policies.
- A role that defines which parts of the Hypori Halo environment the user can access.
- A virtual workspace that you manage.
- A Hypori Halo client with properties you can configure for all users. (The Hypori Halo client is the app that users install on their mobile devices to access their virtual workspace.)

For information about shared physical devices and the user accounts associated with them, see Managing Shared Devices and Their Users *(on page 117)*.

User Licenses

Every user requires a user account that is associated with a user license. There are two types of user licenses:

- **Named:** Each named license is assigned to a single user and always provides virtual workspace access to that user.
- **Concurrent:** Concurrent license users share a pool of licenses. When all concurrent licenses are in use, the next user is denied access until a concurrent license becomes available. Concurrent users whose virtual workspace are turned off (such as when they are stopped or suspended) will not receive a notification.

Users are assigned a license type when they are added to the Hypori Halo environment. For more information, see Adding Users *(on page 75)*. For information about changing a user's license type, see Changing License Types *(on page 60)*.

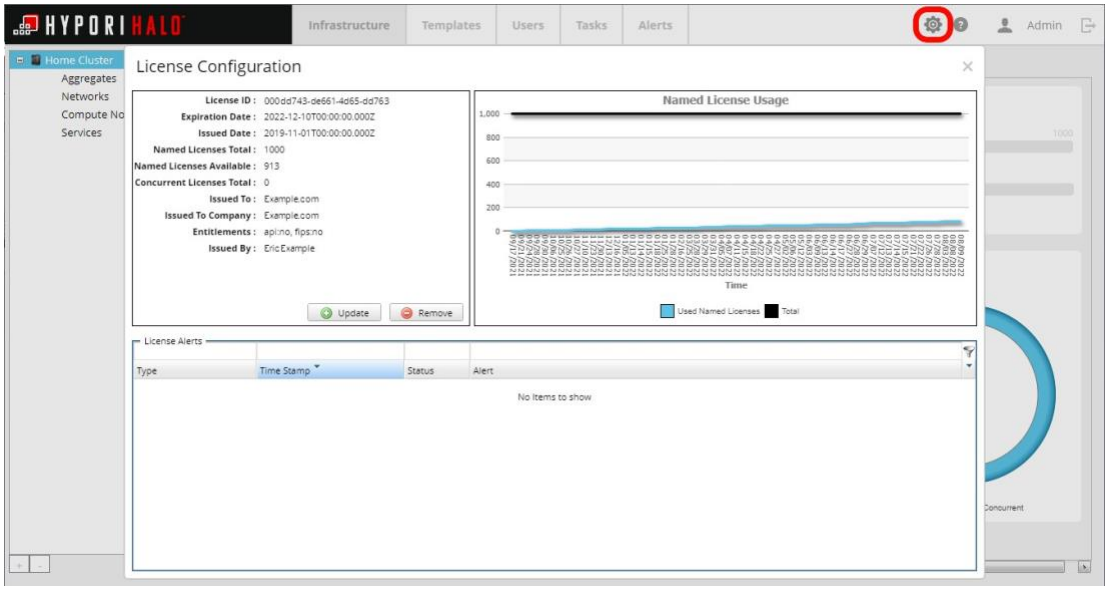
Hypori provides you with a license file that enables access for the named and concurrent licenses you have purchased. For more information, see Updating the License File *(on page 59)*.

Viewing User License Usage

To view the license configuration and see the number of named licenses in use:

1. Open the Hypori Halo Admin Console.
2. In the menu, click the **Settings** icon.

3. Click **Licensing** to open the License Configuration box.



The configuration settings on the left side of the License Configuration box include:

- **License ID:** The unique ID for the user license.
- **Expiration Date:** The expiration date for the license.
- **Issued Date:** The timestamp when the license was issued.
- **Named Licenses Total:** The number of named licenses specified for the license.
- **Named Licenses Available:** The number of available named licenses.
- **Concurrent Licenses Total:** The number of concurrent licenses specified for the license.
- **Issued To:** The name of the person to whom the license file was issued.
- **Issued To Company:** The name of the organization to which the license file was issued.
- **Entitlements:** Whether this license file provides access to additional Hypori products and services.
- **Issued By:** The name of the Hypori Halo administrator who issued the license file.

Tip:

The Named License Usage graph on the right side of the License Configuration box shows the trend in named license usage over time.

Tip:

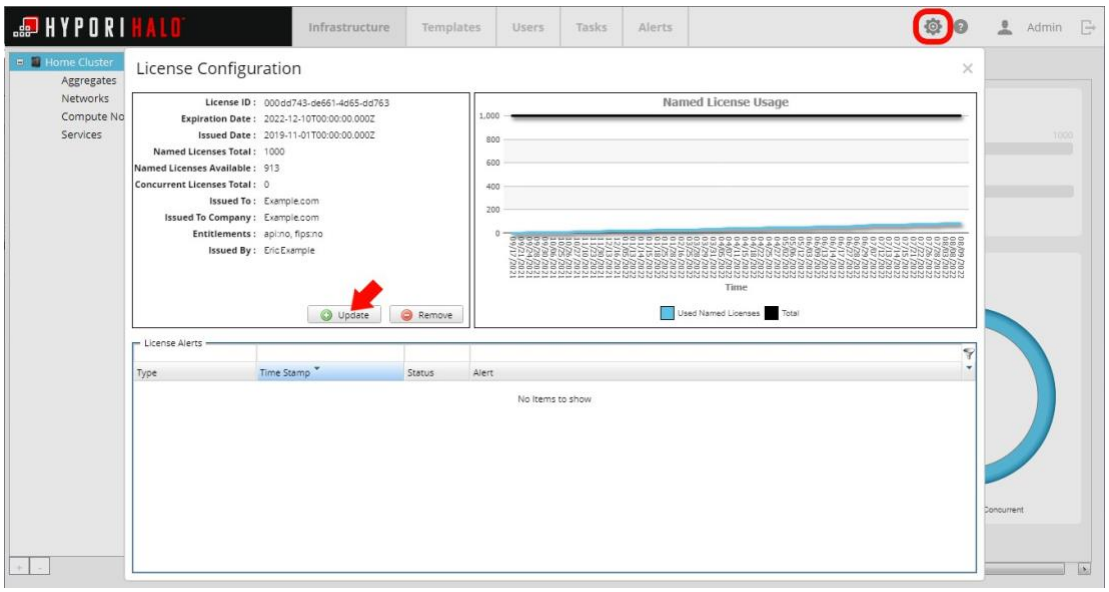
The License Alerts table at the bottom of the License Configuration box shows licensing-related system events.

Updating the License File

To import a new license file:

1. Open the Hypori Halo Admin Console.
2. In the menu, click the **Settings** icon.

3. Click **Licensing** to open the License Configuration box.
4. In the License Configuration box, click **Update**.



5. If you are presented with a EULA file, you must accept it to continue updating the license file.
6. In the Upload License box, click **Browse**.
7. Select the license file sent to you by your Hypori representative.
8. Click **Upload** to install the license file.

Changing License Types

To change the license type assigned to a user:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the user's domain.
4. Click the **Users** tab.
5. In the Users Configuration table, check the box to the left of the username. You can select more than one user.
6. In the Users Configuration area, just above the table, click the **More Actions** icon.

7. In the More Actions menu, click **Change User License Type**.
8. In the Change Users License Type box, click the **License Type** list.
9. Select the license type that you want to assign to the selected user. The current options are:
    - **Named:** An individual license that gives the assigned user constant access to the Hypori Halo environment.
    - **Concurrent:** A shared license from a pool of concurrent licenses. If all concurrent licenses are in use, the next user who tries to access the server with this license type is denied access until a concurrent license becomes available.

> **Tip:**
> The number of available named user licenses is shown next to the Named option in the License Type list.

10. Click **Change User License Type**.
11. In the confirmation box, click **Yes**.
    The specified user is given the selected license type.

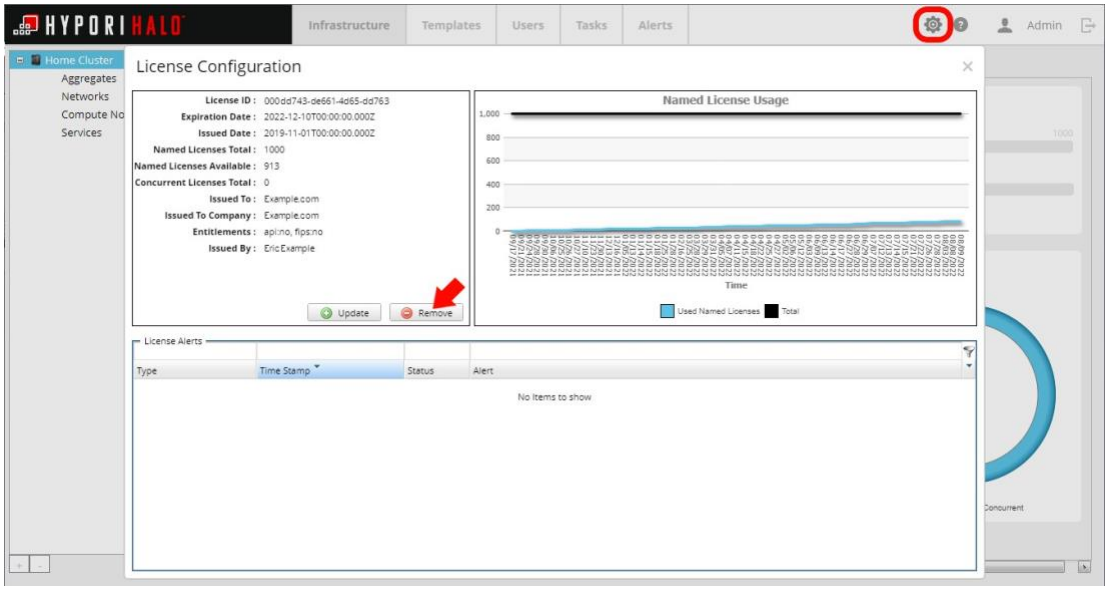
Removing the Current License File

To remove the license file:

1. Open the Hypori Halo Admin Console.
2. In the menu, click the **Settings** icon:

3. Click **Licensing** to open the License Configuration box.

4. Under the License Configuration details, click **Remove**.



5. In the confirmation box, click **Yes**.

User Authentication Configurations

The Hypori Halo system authenticates users with LDAP. Your organization can choose to authenticate your users using the LDAP server shipped with the Hypori Halo system or can choose your own Active Directory server.

By default, the Hypori Halo system authenticates users with an LDAP server running on the management server. There is no need to perform additional configuration.

If your organization chooses to use an OIDC (OpenID Connect) configuration, you must add an OIDC compliant authentication configuration.

If your organization chooses to use Active Directory, you must add an authentication configuration. In addition, any users that you want to add as Hypori Halo users must be in Active Directory.

You can choose to have users enter their Hypori Halo LDAP, OIDC or Active Directory credentials to authenticate with the Hypori Halo environment. This includes users who access the virtual workspace from the Hypori Halo Client and users who access the Hypori Halo Admin Console or Hypori Halo User Management Console (HUMC).

Viewing Authentication Configurations

To view information about an authentication configuration:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the root node.
4. Click the **Configuration** tab.
5. In the Authentication Configuration area, select an authentication configuration.

The Authentication Configuration area shows:

- **Name:** The name of the authentication configuration.
- **Authentication Type:** The type of authentication used.
- **Server:** The name of the authentication server.
- **Search Base:** The distinguished name of the search base object. Input looks like this: dc=domainname,dc=com
- **Query Template:** The distinguished name of the search base object. Input must be in this format: (&(uid={{userPrincipalMap.CN}})(mail={{userPrincipalMap.emailAddress}}))
- **Bind DN:** The common name and domain component IDs associated with the distinguished name parent entity. Input must be in this format: (&(cn={{userPrincipalMap.CN}}) (userPrincipalName={{userPrincipalMap.emailAddress}}))
- **Default:** Whether this is the default authentication configuration for new domains.
- **Secondary Auth:** The protocol used for secondary authentication.
- **Description:** The description of the authentication configuration.
- **Use TLS:** Whether the authentication configuration uses Transport Layer Security (TLS) encryption.
- **Port:** The authentication server's port number.
- **Query Attributes:** The search query attributes that identify users. Input must be in this format: userPrincipalName, cn
- **Use Bind DN:** Whether the Hypori system must use credentials to access the authentication server.
- **Require User Password:** Whether users must enter their LDAP credentials to access the Hypori Halo server from the Hypori Client app and to access the Hypori Halo Admin Console or Hypori Halo User Management Console (HUMC).
- **Login Attribute:** The LDAP attribute that users will enter as their "username".
    - If using Hypori LDAP authentication: `mail`
    - If using Active Directory authentication: `userPrincipalName`
- **Touch ID Auth:** Whether users can authenticate using their fingerprint.

Adding a New Authentication Configuration

To add a new authentication method:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the root node.
4. Click the **Configuration** tab.
5. In the Configuration area, click the **add** (**+**) icon to create a new configuration.

> **Tip:**
> This icon is not available until you select the root node.

6. In the Add New Configuration box, provide the following information:
    - **Name:** The name of the authentication configuration.
    - **Description:** The description of the authentication configuration.
    - **Server:** The name of the authentication server.
    - **Use TLS:** Whether the authentication configuration uses Transport Layer Security (TLS) encryption.
    - **Port:** The authentication server's port number.
    - **Search Base:** The distinguished name of the search base object. Input looks like this: dc=domainname,dc=com
    - **Use Bind DN:** Whether the Hypori system must use credentials to access the authentication server.
    - **Bind DN:** The common name and domain component IDs associated with the distinguished name parent entity. Input must be in this format: (&(cn={{userPrincipalMap.CN}})(userPrincipalName={{userPrincipalMap.emailAddress}}))
    - **Login Attribute:** The LDAP attribute that users will enter as their "username".
        - If using Hypori LDAP authentication: `mail`
        - If using Active Directory authentication: `userPrincipalName`
    - **Password:** The password for the authentication server.
    - **Query Template:** The distinguished name of the search base object. Input must be in this format: (&(uid={{userPrincipalMap.CN}})(mail={{userPrincipalMap.emailAddress}}))
    - **Query Attributes:** The search query attributes that identify users. Input must be in this format: userPrincipalName, cn
    - **Require User Password:** Whether users must enter their LDAP credentials to access the Hypori Halo server from the Hypori Client app and to access the Hypori Halo Admin Console or Hypori Halo User Management Console (HUMC).

- **Allow TouchId Authentication:** Whether users can authenticate using their fingerprint.
- **Default:** Whether this is the default authentication configuration for new domains.

7. Click **Create**.

Editing Authentication Configurations

To edit an authentication method:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the root node.
4. Click the **Configuration** tab.
5. In the Configuration area, select an authentication configuration and click **Edit**.
6. In the Update Configuration box, provide the following information:
    - **Name:** The name of the authentication configuration.
    - **Description:** The description of the authentication configuration.
    - **Server:** The name of the authentication server.
    - **Use TLS:** Whether the authentication configuration uses Transport Layer Security (TLS) encryption.
    - **Port:** The authentication server's port number.
    - **Search Base:** The distinguished name of the search base object. Input looks like this: dc=domainname,dc=com
    - **Use Bind DN:** Whether the Hypori system must use credentials to access the authentication server.
    - **Bind DN:** The common name and domain component IDs associated with the distinguished name parent entity. Input must be in this format: (&(cn={{userPrincipalMap.CN}})(userPrincipalName={{userPrincipalMap.emailAddress}}))
    - **Login Attribute:** The LDAP attribute that users will enter as their "username".
        - If using Hypori LDAP authentication: `mail`
        - If using Active Directory authentication: `userPrincipalName`
    - **Password:** The password for the authentication server.
    - **Query Template:** The distinguished name of the search base object. Input must be in this format: (&(uid={{userPrincipalMap.CN}})(mail={{userPrincipalMap.emailAddress}}))
    - **Query Attributes:** The search query attributes that identify users. Input must be in this format: userPrincipalName, cn
    - **Require User Password:** Whether users must enter their LDAP credentials to access the Hypori Halo server from the Hypori Client app and to access the Hypori Halo Admin Console or Hypori Halo User Management Console (HUMC).

- **Allow TouchId Authentication:** Whether users can authenticate using their fingerprint.
- **Default:** Whether this is the default authentication configuration for new domains.

7. Click **Apply**.

Testing Authentication Configuration Connections

To test the authentication configuration server connection:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the root node.
4. Click the **Configuration** tab.
5. In the Authentication Configuration area, select an authentication configuration.
6. Click **Test Connection**.
7. In the Test Connection box, click **Start Test**.
   The connection test executes and generates a confirmation message, if successful.
   When the testing is complete, you can click **Re-run Test** to repeat the test procedure.
8. Click the ✕ to close the Test Connection box when you have completed the testing.

Managing Secondary Authentication

Your authentication configuration can use a secondary authentication protocol.

To add or modify secondary authentication information:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the root node.
4. Click the **Configuration** tab.
5. In the Authentication Configuration area, select an authentication configuration and click **Manage Secondary Auth**.
6. In the Configure Secondary Auth box, provide the following information:
   - **Type:** The protocol used for secondary authentication. Hypori Halo supports TOTP.
   - **Authenticator Name:** The name of the authenticator used for your secondary authentication.
   - **Duration:** The amount of time a user has available to enter their authenticator code before their connection is reset.
   - **Algorithm:** The list of available algorithms to use for your secondary authentication.

- **Secret Key Size:** Designates the number of characters required for the secret key.
- **TOTP Size:** Designates the number of characters required for the TOTP.

7. Click **Save**.

Configuring Location-Based Authentication

Enabling Location-Based Authentication will require manually editing server config files, outside of the UI, and is not recommended. Please contact Product Support *(on page 6)* for more information.

Deleting an Authentication Configuration

To delete an existing authentication method for the selected domain:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the root node.
4. Click the **Configuration** tab.
5. In the Authentication Configuration area, select an authentication configuration and click the **minus** (-) icon.
6. In the confirmation box, click **Yes**.

Managing Client Certificates

Users must have a certificate to access the Hypori Halo server from their Hypori Halo Client and to access the Hypori Halo Admin Console or Hypori Halo User Management Console. (HUMC)

Providing certificates from an email

You can send a user a system email that contains a QR code and a temporary password. The user scans the QR code to obtain a certificate. If the user cannot scan the QR code, he or she can enter the one-time password (OTP), which is valid for seven days.

If you choose this option:

- You must configure SMTP settings. See Configuring SMTP Settings *(on page 67)*.
- You can send the email when adding the user or afterward. See Adding Users Authenticated with Active Directory *(on page 76)*, Adding Users Authenticated with Hypori Halo LDAP *(on page 78)*, or Sending a One-Time Password in Email *(on page 67)*.
- You can configure the email content. See the *Hypori Halo Server Installation Guide*.

Configuring SMTP Settings

To configure settings for your SMTP server:

1. Log into the Hypori Halo Admin Console.
2. In the upper right corner of the screen, click the **Settings** icon.

3. Click **SMTP Settings** to open the SMTP Configuration box.
4. Click **Update**.
5. In the **SMTP Server** field, type the fully qualified name of your SMTP server.
6. In the **Port** field, type the port number used to access the SMTP server. This value is 587 by default.
7. In the **From (Name)** field, type your name.
8. In the **From (Email)** field, type your email address.
9. If you want to use Transport Layer Security (TLS) to ensure privacy when communicating with the SMTP server, click **Use TLS**.
10. If you want to use credentials to access the SMTP Server, click **Use Authentication** and then type the proper credentials in the **User Name** and **Password** fields.
11. Click **Apply**.

To test your connection by sending an email:

1. Click **Test**.
2. In the Test SMTP Configuration box, type your email address in the **To (Email) field**.
3. In the **Email Subject** field, type a subject for the test email.
4. In the **Email Text** field, type content for the test email.
5. Click **Send Test Email**.

Sending a One-Time Password in Email

You can send a user an email with a One-Time Password (OTP) and a QR code that enables the user to download a client certificate.

To send a user an email with an OTP and QR code:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. Click the **Users** tab.

4. In the navigation pane, select the user's domain.
5. In the Users Configuration table for the domain, hold your cursor over the user to whom you want to send the email.
6. Click the **Email One-Time Password** icon:

7. In the confirmation box, click **Yes**.

Viewing Client Certificates

Note:
As an administrator, you can view the client certificates for each shared device you have provisioned.

To view the certificates associated with a user:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. Click the **Users** tab.
4. In the navigation pane, select a user's domain.
5. In the Users Configuration table for this domain, hold your cursor over the user.
6. Click the **View Credentials** icon:

The Certificates tab on the User Credentials box shows:

- **Distinguished Name:** The distinguished name used for the user's certificate.
- **Email:** The email address for the user.

For each certificate, the table shows:

- **Issuer:** Information about the entity that generated the certificate.
- **Last Used:** The date and time when the certificate was used last.
- **Status:** The present state of the certificate.
- **Issued On:** The date and time when the certificate was issued.
- **Expires On:** The date and time when the certificate expires.
- **Serial No:** The serial number of the certificate.

- **Shared:** Whether this certificate is for a shared device. (Users with the administrator role who have added a shared device have the shared device certificates listed with their user certificates.)
- **Device Info:** The unique identifier for the shared device.

Click the arrow to the left of the Issuer column to see the following information about when the certificate was used:

- **Time:** The date and time that the certificate was used.
- **Activity:** The activity that occurred.
- **Details:** Additional information about the activity.

Blocking Client Certificates

To block a user's client certificate:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. Click the **Users** tab.
4. In the navigation pane, select the user's domain.
5. In the Users Configuration table for this domain, hold your cursor over the user.
6. Click the **View Credentials** icon:

7. In the Certificates table, hold your cursor over the certificate you want to block.
8. Click the **Block Certificate** icon:

9. In the confirmation box, click **Yes**.

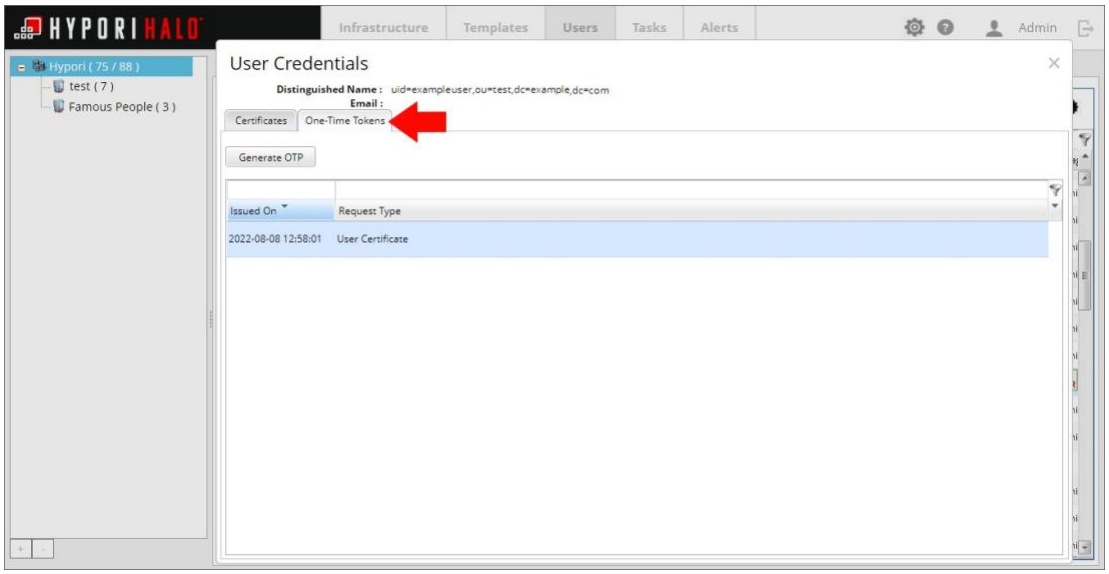
Viewing One-Time Tokens

Tip:
As an administrator, you can view the one-time tokens available for a user.

To view the one-time tokens associated with a user:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. Click the **Users** tab.
4. In the navigation pane, select the user's domain.
5. In the Users Configuration table for this domain, hold your cursor over the user.
6. Click the **View Credentials** icon:

7. Click the **One-Time Tokens** tab.



The One-Time Tokens tab on the User Credentials box shows:

- **Distinguished Name:** The distinguished name used for the user's certificate.
- **Email:** The email address for the user.

For each certificate, the table shows:

- **Issued On:** The date and time when the token was issued.
- **Request Type:** The type of token requested.

Revoking a One-Time Token

To revoke a one-time token:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.

3. Click the **Users** tab.
4. In the navigation pane, select the user's domain.
5. In the Users Configuration table for this domain, hold your cursor over the user whose one-time tokens you want to revoke.
6. Click the **View Credentials** icon:

7. Click the **One-Time Tokens** tab.
8. In the One-Time Tokens table, hold your cursor over the token you want to revoke.
9. Click the **Revoke Token** icon:

10. In the confirmation box, click **Yes**.

Managing Domains

A domain is a means of grouping together similar users. A domain has a collection of server clusters, authentication configurations, templates, roles, and policies that are assigned to its users. Each user is assigned to a domain to simplify user management.

Viewing Domains

To view information about a domain:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. Click the **Configuration** tab.
4. In the navigation pane, select the domain you want to view.

The Configuration tab shows:

- **General Configuration**
  - **Name:** The name of the domain.
  - **User Limit:** The maximum number of users in this domain.
  - **Description:** A brief description of the domain.
- **Home Cluster**
  - **Name:** The name of the server cluster.
  - **Authentication URL:** The URL for the controller node.

- **Default Aggregate:** The name of the aggregate to which new virtual workspaces are added by default.
- **UserName:** The username for the controller node.
- **Description:** A brief description of the server cluster.
- **Tenant:** The tenant resource container within the compute node.
- **VM Network:** The name of the enterprise network, which provides virtual workspaces with access to shared resources in your enterprise.
- **Default:** Whether this is the server cluster to which new virtual workspaces are added by default.

- **Authentication Configuration (for each configuration)**
  - **Name:** The name of the authentication configuration.
  - **Authentication Type:** The type of authentication used.
  - **Server:** The name of the authentication server.
  - **Search Base:** The distinguished name of the search base object. Input looks like this: dc=domainname,dc=com
  - **Query Template:** The distinguished name of the search base object. Input must be in this format: (&(uid={{userPrincipalMap.CN}})(mail={{userPrincipalMap.emailAddress}}))
  - **Bind DN:** The common name and domain component IDs associated with the distinguished name parent entity. Input must be in this format: (&(cn={{userPrincipalMap.CN}})(userPrincipalName={{userPrincipalMap.emailAddress}}))
  - **Default:** Whether this is the default authentication configuration for new domains.
  - **Secondary Auth:** The protocol used for secondary authentication.
  - **Description:** The description of the authentication configuration.
  - **Use TLS:** Whether the authentication configuration uses Transport Layer Security (TLS) encryption.
  - **Port:** The authentication server's port number.
  - **Query Attributes:** The search query attributes that identify users. Input must be in this format: userPrincipalName, cn
  - **Use Bind DN:** Whether the Hypori system must use credentials to access the authentication server.
  - **Require User Password:** Whether users must enter their LDAP credentials to access the Hypori Halo server from the Hypori Client app and to access the Hypori Halo Admin Console or Hypori Halo User Management Console (HUMC).
  - **Login Attribute:** The LDAP attribute that users will enter as their "username".
    - If using Hypori LDAP authentication: `mail`
    - If using Active Directory authentication: `userPrincipalName`
  - **Touch ID Auth:** Whether users can authenticate using their fingerprint.

- **Hypori Device Policies**
  - **Name:** The name of the Hypori Device Policy.
  - **Default:** Whether the selected policy is the default policy.
  - **Description:** Admin defined description of the selected policy.
  - **Hypori Device Policy:** A listing of the contents of the policy document, in XML format.
- **Client Device Policies**
  - **Name:** The name of the client device policy.
  - **Default:** Whether the selected policy is the default policy.
  - **Description:** Admin defined description of the selected policy.
  - **Client Device Policy:** A listing of the contents of the policy document, in JSON format.
- **Hypori Device Templates (for each template)**
  - **Name:** The name of the template.
  - **Flavor:** The flavor for the template.
  - **User Data Image:** The published image (storage) for the template.
  - **Description:** A description of the template.
  - **Android Image:** The published image (operating system and apps) for the template.
  - **User Data Size (GB):** The amount of data storage available for virtual workspaces that are based on the template, in GB.

Adding Domains

Before you begin, ensure that the server cluster, authentication configuration, templates, roles, and policies that you want to include in the domain are available in the Hypori Halo environment.

By default, a new domain inherits the characteristics of its parent domain.

To add a new domain:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the server cluster that will be the parent of the new domain.
4. At the bottom of the navigation pane, click the **add** (**+**) icon.
5. In the General Configuration box, provide the following information:
   - **Name:** The name of the domain.
   - **User Limit:** The maximum number of users in this domain.
   - **Description:** A brief description of the domain.
   - **Server Clusters:** If this domain has access to a separate set of server clusters, click to clear the **Inherit Home Clusters from Parent** check box. In the **Include in Domain**

column, select the check boxes for the server clusters you want to include. Click the **Set as Default** check box to designate the default server cluster.

- **Hypori Device Policies:** If this domain has access to different policies than its parent, click to clear the **Inherit Hypori Device Policies from parent** check box. In the **Include in Domain** column, select the check boxes for the templates you want to include. Click the **Set as Default** check box to designate the default template.
- **Hypori Device Templates:** If this domain has access to different templates than its parent, click to clear the **Inherit Hypori Device Templates from parent** check box. In the **Include in Domain** column, select the check boxes for the templates you want to include. Click the **Set as Default** check box to designate the default template.
- **Authentication Configuration:** If this domain uses a different authentication configuration than its parent, click to clear the **Inherit Authentication Configuration from parent** check box. In the **Include in Domain** column, select the check boxes for the configurations you want to include. Click the **Set as Default** check box to designate the default authentication configuration.
- **Aggregates:** If this domain supports different aggregates than its parent, click to clear the **Inherit Aggregates from parent** check box. In the **Include in Domain** column, select the check boxes for the configurations you want to include. Click the **Set as Default** check box to designate the default role.
- **Client Device Policies:** If this domain has access to different policies than its parent, click to clear the **Inherit Client Device Policies from parent** check box. In the **Include in Domain** column, select the check boxes for the templates you want to include. Click the **Set as Default** check box to designate the default template.

6. Click **Create Domain**.

The new domain configuration is added to the list of available domains and can be applied to any user in the server cluster. See Adding Users *(on page 75)* and Changing Domains *(on page 84)*.

Editing Domains

To edit domain settings:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. Click the **Configuration** tab.
4. In the navigation pane, select the domain to be edited.
5. Under General Configuration, click **Edit**.
6. Modify the following properties as necessary:

- **Name:** The name of the domain.
- **User Limit:** The maximum number of users in this domain.
- **Description:** A brief description of the domain.

7. Click **Apply**.

In addition, you can make changes to the user authentication settings. See User Authentication Configurations *(on page 61)*.

Deleting Domains

> **Note:**
> You cannot delete a domain that has users assigned to it. Any users in a domain that is to be deleted must be moved to a new domain before the current domain may be deleted.

To delete a domain:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. Click the **Users** tab.
4. In the navigation pane, verify the domain you want to delete has no users associated with it.
5. Select the name of the domain being deleted.
6. At the bottom of the navigation pane, click the **minus** (**-**) icon to delete the selected domain.
7. In the confirmation box, click **Yes**.

Managing Users

Users have access to the Hypori Halo environments based on the information in their user accounts. You can manage user accounts from the Hypori Halo Admin Console.

Adding Users

When you add a user to the Hypori Halo environment, you must ensure that the user can authenticate and access his or her virtual workspace. Here is the process:

- Ensure that the user is in your designated OIDC environment (if OIDC is being used) or add the user to the Hypori Halo LDAP server.
- Add the user to the Hypori Halo environment and send the user an email with instructions for connecting to the environment from the Hypori Halo Client.

- The user installs the Hypori Halo Client on his or her mobile device.
- The user scans the QR code or goes to the website in your email to request a certificate.
- The user logs on to the Hypori Halo server using the instructions in your email and his or her OIDC or LDAP credentials, if required.

Note:
For information about shared physical devices and the user accounts associated with them, see Managing Shared Devices and Their Users *(on page 117)*.

Adding Users Authenticated with Active Directory

Before you begin, ensure that the user you want to add to the Hypori system is available in Active Directory. Not every organization will utilize Active Directory (AD). If your organization is not using AD, skip this section.

To add a user:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the domain for the new user.
4. Click the **Users** tab.
5. Under Users Configuration, click **Add** to open the Add Users box.
6. In the **Authentication Configuration** list, select the configuration that will be used to authenticate the new user.
7. In the **LDAP Search Scope** list, select the LDAP organization for the user.
8. In the **LDAP Filter** list, select the LDAP query that will be run to find the user.
9. In the **User License Type** list, select the license type that you want to associate with the new user.
    - **Named:** An individual license that gives the assigned user constant access to the Hypori Halo environment.
    - **Concurrent:** A shared license from a pool of concurrent licenses. If all concurrent licenses are in use, the next user who tries to access the server with this license type is denied access until a concurrent license becomes available.
10. In the **Allocate Hypori Device** box, select if you want to make this user's virtual workspace available automatically after adding the user. If you do not allocate the virtual workspace at this point, you must do so manually before the user can access his or her virtual workspace.

11. In the **Email OTP** box , select whether you want to send this user an email that contains information about accessing a certificate to authenticate with the Hypori Halo environment from the Hypori Halo Client.
12. In the **Home Cluster** list, select the server cluster for the new user.
13. In the **Aggregate** list, select the aggregate that you want to run the user's virtual workspace.
14. In the **Hypori Device Template** list, select the template that will define the look and feel of the user's virtual workspace.
15. In the **User Role** list, check the box next to one or more user roles for the new user. Roles are cumulative.

    Options include:

    - **End User:** The End User role allows the user to connect to their designated virtual workspace using the Hypori Halo Client.

      Important:
      Hypori recommends only using the End User role to connect to virtual workspaces. Other roles (e.g., administrators, template managers, or domain managers) that require access to a virtual workspace should use a second account, with an End User role, to access their virtual workspace.

    - **Domain Manager:** The Domain Manager role allows connections to the Hypori Halo User Management Console (HUMC) to support user account creation and deletion. Domain Managers are only able to create or remove users in the domain in which the Domain Manager resides. Users with only the Domain Manager role are unable to access the Hypori Halo Admin Console and cannot connect to a virtual workspace from the Hypori Halo Client, however this role can be paired with the End User role to allow connections to a virtual workspace.
    - **Read Only:** The Read Only role allows connections to the Hypori Halo Admin Console, but in view-only mode. Users with this role cannot modify any Hypori Halo Admin Console settings or connect to a virtual workspace using the Hypori Halo Client.
    - **Auditor:** The Auditor role allows the user to view virtual workspace statistics and snapshots of the virtual workspace screens for any user within the Auditor's designated domain. This role must be paired with either the Administrator or Read Only role.
    - **Template Manager:** The Template Manager role allows connections to the Hypori Halo Admin Console and supports both create and update privileges for their designated user's virtual workspaces. Template Managers can upload Android images and APK files using them to publish images. Users with only the Template Manager role cannot connect to a virtual workspace using the Hypori Halo Client, however the Template

Manager role can be paired with the End User role to allow connections to a virtual workspace.

- **Administrator:** The Administrator role includes all read and update privileges in the Hypori Halo Admin Console. Administrators can also connect to virtual workspaces using the Hypori Halo Client.

16. Click **Fetch Users from LDAP** to populate the users list. If the user is not in the list, you may need to add the user in Active Directory.
17. In the users list table, check the box next to the name of the users that you want to add.

> **Note:**
> You cannot add users that are already in the Hypori Halo user database.

18. Click **Add Users**.

Adding Users Authenticated with Hypori Halo LDAP

This process adds the user to the Hypori Halo LDAP server, adds the user to the Hypori Halo environment, and optionally allocates the virtual workspace.

> **Note:**
> Each user must have a unique first and last name combination.

To add a user:

1. In the menu, click **Users**.
2. In the navigation pane, select the domain for the new user.
3. Click the **Configuration** tab.
4. Under Authentication Configuration, select the configuration to which the user will be added and then click **Manage LDAP Users**.
5. Click **Add User to LDAP** to open the Add New User box.
6. In the **Parent DN** field, type the organizational unit (OU) and domain component (DC) where the user will be stored in LDAP. It must be in the format: `ou=MyDepartment,dc=ExampleCompany,dc=com`, where *MyDepartment* is the name of the organization and *ExampleCompany.com* is the domain.
7. In the **First Name** field, type the first name of the user.
8. In the **Last Name** field, type the last name of the user.
9. In the **Email** field, type the email address of the user.
10. In the **Password** field, type password the user will use to authenticate.

11. In the **Confirm Password** field, type the password again.
12. In the **Allocate Hypori Device** box, select if you want to make this user's virtual workspace available automatically after adding the user. If you do not allocate the virtual workspace at this point, you must do so manually before the user can access his or her virtual workspace.
13. Click **Add User to LDAP**.
14. In the **User License Type** list, select the license type that you want to associate with the new user.
    - **Named:** An individual license that gives the assigned user constant access to the Hypori Halo environment.
    - **Concurrent:** A shared license from a pool of concurrent licenses. If all concurrent licenses are in use, the next user who tries to access the server with this license type is denied access until a concurrent license becomes available.
15. In the **Home Cluster** list, select the server cluster for the new user.
16. In the **Aggregate** list, select the aggregate that you want to run the user's virtual workspace.
17. In the **Hypori Device Template** list, select the template that will define the look and feel of the user's virtual workspace.
18. In the **User Role** list, check the box next to one or more user roles for the new user. Roles are cumulative.

    Options include:
    - **End User:** The End User role allows the user to connect to their designated virtual workspace using the Hypori Halo Client.

      Important:
      Hypori recommends only using the End User role to connect to virtual workspaces. Other roles (e.g., administrators, template managers, or domain managers) that require access to a virtual workspace should use a second account, with an End User role, to access their virtual workspace.
    - **Domain Manager:** The Domain Manager role allows connections to the Hypori Halo User Management Console (HUMC) to support user account creation and deletion. Domain Managers are only able to create or remove users in the domain in which the Domain Manager resides. Users with only the Domain Manager role are unable to access the Hypori Halo Admin Console and cannot connect to a virtual workspace from the Hypori Halo Client, however this role can be paired with the End User role to allow connections to a virtual workspace.
    - **Read Only:** The Read Only role allows connections to the Hypori Halo Admin Console, but in view-only mode. Users with this role cannot modify any Hypori Halo Admin Console settings or connect to a virtual workspace using the Hypori Halo Client.

- **Auditor:** The Auditor role allows the user to view virtual workspace statistics and snapshots of the virtual workspace screens for any user within the Auditor's designated domain. This role must be paired with either the Administrator or Read Only role.
- **Template Manager:** The Template Manager role allows connections to the Hypori Halo Admin Console and supports both create and update privileges for their designated user's virtual workspaces. Template Managers can upload Android images and APK files using them to publish images. Users with only the Template Manager role cannot connect to a virtual workspace using the Hypori Halo Client, however the Template Manager role can be paired with the End User role to allow connections to a virtual workspace.
- **Administrator:** The Administrator role includes all read and update privileges in the Hypori Halo Admin Console. Administrators can also connect to virtual workspaces using the Hypori Halo Client.

19. In the **Email OTP** box , select whether you want to send this user an email that contains information about accessing a certificate to authenticate with the Hypori Halo environment from the Hypori Halo Client.
20. Click **Allocate Hypori Device**.

Viewing Users

To view the list of users:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the root node to open it.

> **Tip:**
> To refresh the list of users, click the **Refresh** icon.

The navigation pane shows sub-nodes for each domain, identifying the number of users that are assigned to the domain. The root node user count identifies the number of administrator-level user accounts associated with the server cluster and the total number of users in the domain.

For each user, the Users Configuration table shows:

- **Status:** Whether the user has an active connection (green) to their virtual workspace through the Hypori Halo Client.
- **User Name:** The user's name.

- **User Role:** The user's role.
  - **Administrator:** The Administrator role includes all read and update privileges in the Hypori Halo Admin Console. Administrators can also connect to virtual workspaces using the Hypori Halo Client.
  - **Read Only:** The Read Only role allows connections to the Hypori Halo Admin Console, but in view-only mode. Users with this role cannot modify any Hypori Halo Admin Console settings or connect to a virtual workspace using the Hypori Halo Client.
  - **Auditor:** The Auditor role allows the user to view virtual workspace statistics and snapshots of the virtual workspace screens for any user within the Auditor's designated domain. This role must be paired with either the Administrator or Read Only role.
  - **End User:** The End User role allows the user to connect to their designated virtual workspace using the Hypori Halo Client.

    Important:
    Hypori recommends only using the End User role to connect to virtual workspaces. Other roles (e.g., administrators, template managers, or domain managers) that require access to a virtual workspace should use a second account, with an End User role, to access their virtual workspace.

  - **Template Manager:** The Template Manager role allows connections to the Hypori Halo Admin Console and supports both create and update privileges for their designated user's virtual workspaces. Template Managers can upload Android images and APK files using them to publish images. Users with only the Template Manager role cannot connect to a virtual workspace using the Hypori Halo Client, however the Template Manager role can be paired with the End User role to allow connections to a virtual workspace.
  - **Domain Manager:** The Domain Manager role allows connections to the Hypori Halo User Management Console (HUMC) to support user account creation and deletion. Domain Managers are only able to create or remove users in the domain in which the Domain Manager resides. Users with only the Domain Manager role are unable to access the Hypori Halo Admin Console and cannot connect to a virtual workspace from the Hypori Halo Client, however this role can be paired with the End User role to allow connections to a virtual workspace.
- **Enabled:** Whether the user's account is enabled.
- **Hypori Device State:** The state of the user's virtual workspace, such as whether it is unallocated or active.
- **Hypori Device Template:** The template that defines the look and feel of the user's virtual workspace.

- **Aggregate:** The aggregate that contains the compute node that runs the user's virtual workspace.
- **Storage Zone:** The storage zone that stores the user's virtual workspace data.
- **Compute Node:** The compute node that runs the user's virtual workspace.

Tip:

The table displays an alert icon  next to users whose virtual workspace has not been allocated.

Viewing User Account Details

To view the user detail information:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the user's domain.
4. Click the **Users** tab.
5. In the Users Configuration table, check the box to the left of the username.
6. In the Users Configuration area, just above the table, click the **More Actions** icon.

   
7. From the More Actions menu, click **View Details**.

Tip:

You can also view user account details by holding your cursor over the row in the table and clicking the **View Details** icon:

The User Details box displays the following information about the selected user account:

- **ID:** The Hypori Halo system identifier for the user.
- **LDAP/AD GUID:** The LDAP identifier for the user.
- **Distinguished Name:** The distinguished name used for the user's certificate.
- **Login ID:** The login name of the user.
- **User Name:** The first and last name of the user.

- **Email:** The email address of the user.
- **Account Type:** The type of account associated with this user.
- **User License Type:** The type of license assigned to the user.
- **Session Status:** The status of the current (or last) session.
- **Session Status Time Stamp:** The date and time when the current session started (for active sessions) or the last session ended (for inactive sessions).
- **Infrastructure:** The name of the server cluster that hosts the user's virtual workspace.
- **System Client Policy:** A rule that directs the client to behave in specific ways that cannot be further modified by the end user.
- **Target Aggregate:** The aggregate to which the user has been most recently assigned.
- **Authentication Configuration:** The configuration used to authenticate the user.
- **Hypori Device Template:** The template assigned to the user's virtual workspace.
- **Hypori Device IP Address:** The IP address of the user's virtual workspace on the compute node.
- **Hypori Device MAC Address:** The MAC address of the user's virtual workspace.
- **Hypori Device Port:** The port number on which the user's Hypori Halo client connects to the user's virtual workspace.
- **Hypori Device State:** Whether the user's virtual workspace is active.
- **Hypori Device State Details:** Additional information about the state of the user's virtual workspace.
- **Hypori Device ID:** The system identifier for the user's virtual workspace.
- **Hypori Device Name:** The name of the user's virtual workspace in the Hypori Halo environment.
- **Current Aggregate:** The aggregate that contains the compute node that runs the user's virtual workspace.
- **Hypori Device Volume ID:** The system identifier for the user's data on the virtual workspace.
- **Hypori Storage Zone:** The storage zone that stores data for the user's virtual workspace.

Searching for Users

To search for users:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. Click the **Users** tab.
4. Under Users Configuration, click **Search** to open the Search for Users Across All Domains box.
5. In the **Search By** list, click a category to focus the search.
6. In the **Operator** list, click an operator for the search expression.
7. In the **Value** field, type or select the text that you want to use for the search.

For each matched user, the results table shows:

- **Name:** The user's name.
- **Email:** The user's email address.
- **Domain:** The user's domain.
- **Host:** The compute node that runs the user's virtual workspace.
- **Hypori Device Status:** The state of the user's virtual workspace, such as whether it is unallocated or active.

Changing User Passwords

Note:
This procedure can only change the password for a user who is authenticated with Hypori LDAP. Changing the user passwords in the Active Directory (AD) will also result in the changes filtering down to the Hypori LDAP, but altering the AD is not supported.

To change a user's password:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the user's domain.
4. Click the **Configuration** tab.
5. Under Authentication Configuration, click **Manage LDAP Users** to open the Manage Users box.
6. In the **LDAP Search Scope** list, select the LDAP organization for the user.
7. In the **LDAP Filter** list, select the LDAP query that will be run to find the user.
8. Click **Fetch Users from LDAP**.
9. In the list of users, hold your cursor over the user whose password you want to change.
10. Click the **Reset User Password** icon:

11. In the Reset Password box, type the new password in the **Password** and **Confirm Password** fields and click **Reset Password**.

Changing Domains

To change the domain to which a user is assigned:

1. In the menu, click **Users**.
2. In the navigation pane, select the user's domain.
3. Click the **Users** tab.
4. In the Users Configuration table, check the box to the left of the username. You can select more than one user.
5. In the Users Configuration area, just above the table, click the **More Actions** icon.

6. From the More Actions menu, click **Change Domain**.
7. In the Change Users Domain box, click the **Target Domain** list.
8. Select the name of the new domain that you want to assign to the user.
9. Click **Change Domain**.
10. In the confirmation box, click **Yes**.

    The specified user is assigned to the selected domain.

Changing Roles

To change a selected user's role:

1. In the menu, click **Users**.
2. In the navigation pane, select the user's domain.
3. Click the **Users** tab.
4. In the Users Configuration table, check the box to the left of the username. You can select more than one user.
5. In the Users Configuration area, just above the table, click the **More Actions** icon.

6. From the More Actions menu, click **Change Role**.
7. In the Change Users Role box, click the **New User Role** list.
8. Select one or more user roles that you want to assign to the user. Options include:
    - **Administrator:** The Administrator role includes all read and update privileges in the Hypori Halo Admin Console. Administrators can also connect to virtual workspaces using the Hypori Halo Client.
    - **Read Only:** The Read Only role allows connections to the Hypori Halo Admin Console, but in view-only mode. Users with this role cannot modify any Hypori Halo Admin Console settings or connect to a virtual workspace using the Hypori Halo Client.

- **Auditor:** The Auditor role allows the user to view virtual workspace statistics and snapshots of the virtual workspace screens for any user within the Auditor's designated domain. This role must be paired with either the Administrator or Read Only role.
- **End User:** The End User role allows the user to connect to their designated virtual workspace using the Hypori Halo Client.

  Important:
  Hypori recommends only using the End User role to connect to virtual workspaces. Other roles (e.g., administrators, template managers, or domain managers) that require access to a virtual workspace should use a second account, with an End User role, to access their virtual workspace.

- **Template Manager:** The Template Manager role allows connections to the Hypori Halo Admin Console and supports both create and update privileges for their designated user's virtual workspaces. Template Managers can upload Android images and APK files using them to publish images. Users with only the Template Manager role cannot connect to a virtual workspace using the Hypori Halo Client, however the Template Manager role can be paired with the End User role to allow connections to a virtual workspace.
- **Domain Manager:** The Domain Manager role allows connections to the Hypori Halo User Management Console (HUMC) to support user account creation and deletion. Domain Managers are only able to create or remove users in the domain in which the Domain Manager resides. Users with only the Domain Manager role are unable to access the Hypori Halo Admin Console and cannot connect to a virtual workspace from the Hypori Halo Client, however this role can be paired with the End User role to allow connections to a virtual workspace.

9. Click **Change Role**.
10. In the confirmation box, click **Yes**.
    The specified user is given the selected roles.

Cancelling Scheduled User Jobs

You can cancel jobs that are scheduled for a user, such as allocating, starting, or suspending their virtual workspace. You cannot cancel a job that is in progress.

To cancel a job that has been scheduled:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.

3. In the navigation pane, select the user's domain.
4. Click the **Users** tab.
5. In the Users Configuration table, select the checkbox to the left of the username. You can select more than one user.
6. In the Users Configuration area, just above the table, click the **More Actions** icon.

7. From the More Actions menu, click **Cancel Running Jobs**.
8. In the confirmation box, click **Yes**.

Disabling Users

To disable selected user accounts:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the user's domain.
4. Click the **Users** tab.
5. In the Users Configuration table, check the box to the left of the username. You can select more than one user.
6. In the Users Configuration area, just above the table, click the **More Actions** icon.

7. From the More Actions menu, click **Disable Users**.
8. In the confirmation box, click **Yes**.
9. At the Disable Users prompt, you can enter a message to appear if someone tries to log into the account. Enter a message, if needed, then click **Apply**.

The user account is disabled for the selected user.

A disabled user:

- Cannot access the Hypori Halo Admin Console or Hypori Halo User Management Console (HUMC).
- Cannot request a new authentication token from the Hypori Halo environment through the Hypori Halo Client. As a result, after the current token expires, the user will not be able to access their virtual workspace.
  To ensure that a user cannot connect, even with a cached authentication token, stop the user's virtual workspace after disabling the user's account. For more information, see Stopping and Starting a Virtual Workspace *(on page 100)*.

You can also disable all users on a compute node. For more information, see Disabling All User Accounts on a Compute Node *(on page 25)*.

Enabling Users

To enable selected user accounts:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the user's domain.
4. Click the **Users** tab.
5. In the Users Configuration table, check the box to the left of the username. You can select more than one user.
6. In the Users Configuration area, just above the table, click the **More Actions** icon.
   
7. From the More Actions menu, click **Enable Users**.
8. In the confirmation box, click **Yes**.

The user accounts are enabled for the selected users.

Tip:
You can also enable all users on a compute node. For more information, see Enabling All User Accounts on a Compute Node *(on page 26)*.

Deleting Users

Deleting a user deletes the user's virtual workspace but does not delete the user's data. If you add this user again and have not deleted the data, the user can use the same user data volume. To delete users altogether, you must also remove their user data. See Deleting User Data *(on page 105)*.

To delete a user:

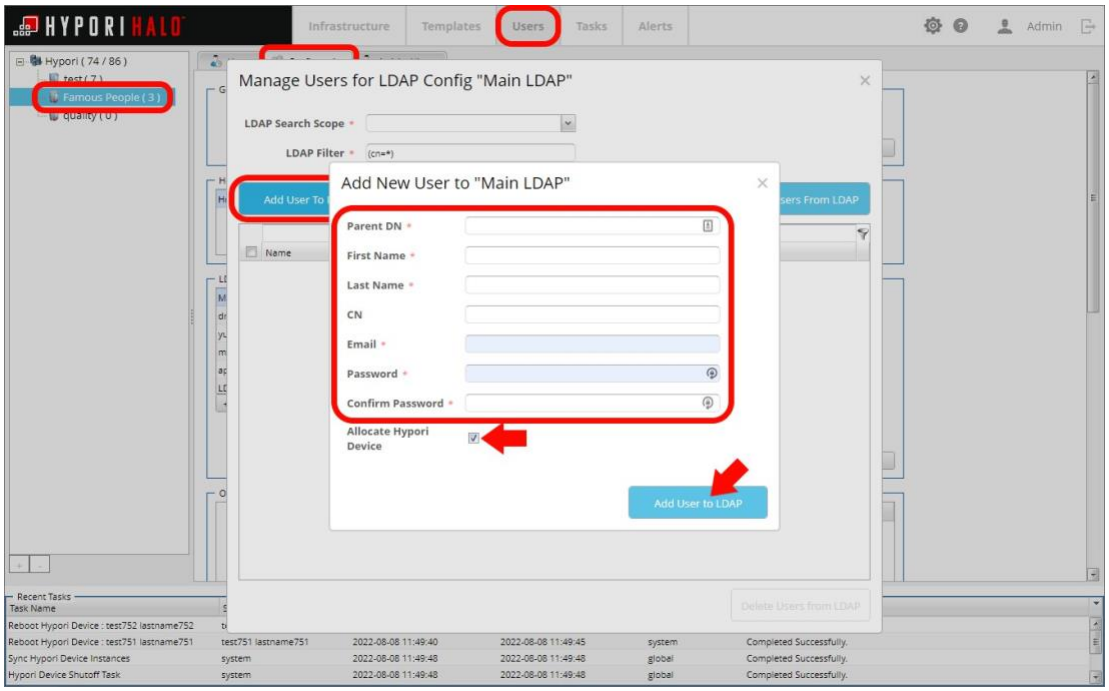
1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select a domain.
4. Click the **Users** tab.
5. In the Users Configuration table, check the box to the left of the username. You can select more than one user.
6. In the Users Configuration area, just above the table, click the **More Actions** icon.

   
7. From the More Actions menu, click **Delete Users**.
   You can also delete a user by holding your cursor over the row in the table and clicking the **Delete** icon.
8. In the confirmation box, click **Yes**.
   The selected user account is deleted.

Creating a New Admin Account

It is a best practice to disable the default Admin account used to setup Hypori Halo since it has a known username and password. Before doing so, a new Administrator account must be created.

1. Log into the Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the default domain.
4. Click the **Configuration** tab.
5. Click **Manage LDAP Users**.
6. Set the LDAP Search Scope to `"ou=Admins,dc=example,dc=com"`.
7. Select **Add User to LDAP**.
8. Fill in the required fields but do **not** select Allocate Hypori Device.
9. Click **Add User to LDAP**.



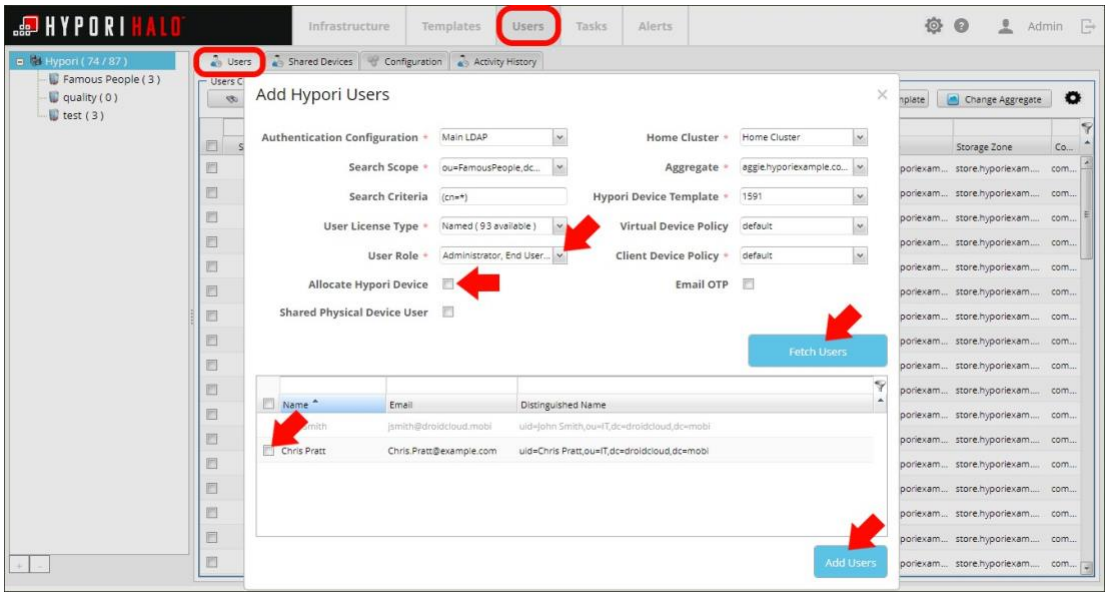
10. Close the list of users.
11. In the menu, click **Users**, then click the **Users** tab.
12. Click the **Add** (**+**) button.
13. Set the LDAP Search Scope to the appropriate settings, which should be formatted similarly to the following example:

```
ou=FamousPeople,dc=example,dc=com
```

14. Select **User Role** and check the box next to Admin.

> **Note:**
> This will enable all other user types listed.

15. Deselect the box next to Allocate Hypori Device.
16. Leave all other settings at defaults.
17. Click **Fetch Users**.
18. Check the box next to the new Admin account and click **Add Users**.



19. Select **Yes** when prompted to confirm you want to add the new Admin account.

> **Important:**
> It is recommended you complete the steps listed in the Import the Client Certificate *(on page 2)* section and the Logging on to the Hypori Halo Admin Console *(on page 4)* portions of this guide using the credentials of the newly created Admin account to verify it is functioning properly before continuing.

Disabling the Default Admin Account

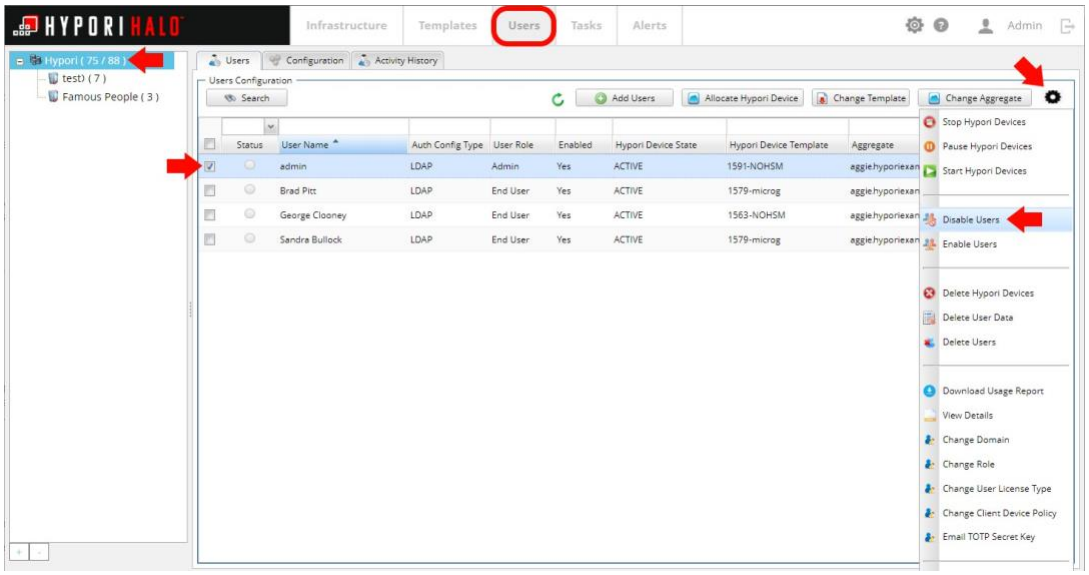
> **Important:**
> Verify you have completed the Creating a New Admin Account *(on page 89)* section of this guide and that account is functioning before disabling the default Admin account.

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the default domain.
4. Click the **Users** tab.
5. Locate and check the box next to the default Admin account.
6. In the Users Configuration area, just above the table, click the **More Actions** icon.

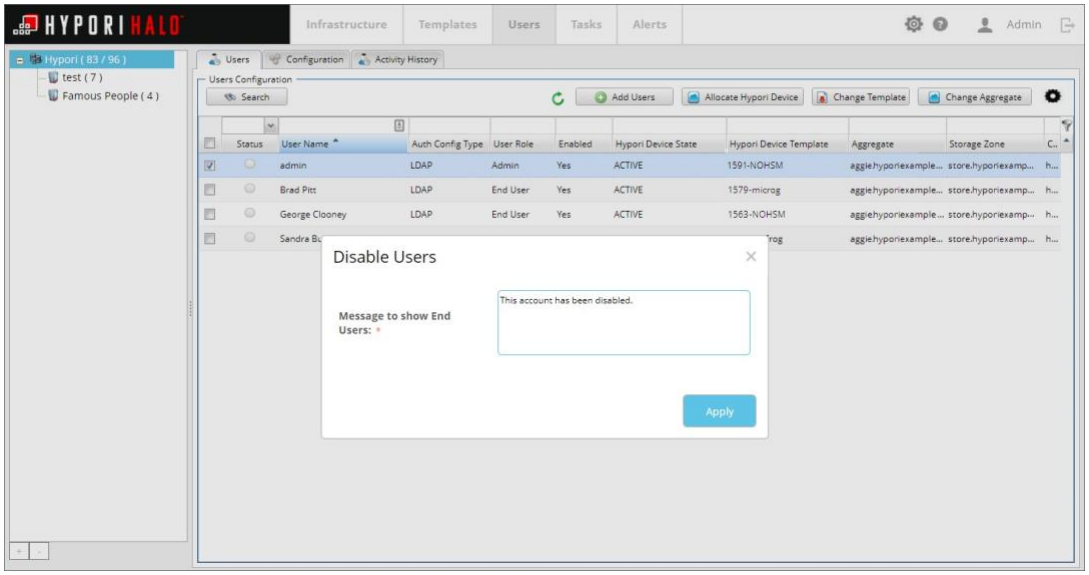
7. Click the **Disable Users** icon.

Warning:

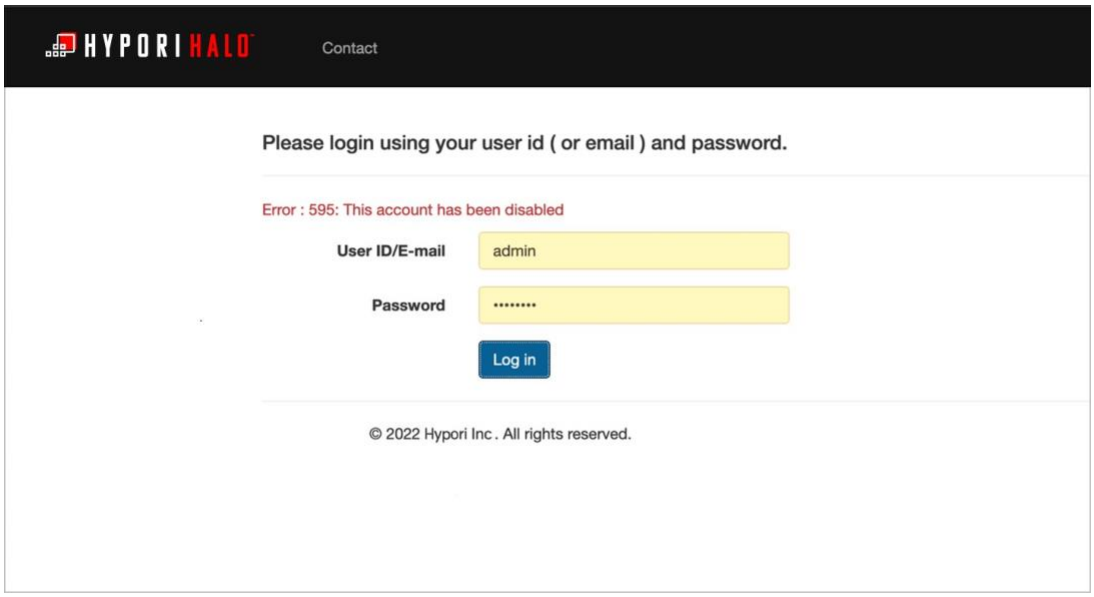
Do not choose the Delete Users option as this would result in basic functionality issues.



8. You will be asked to confirm if you are sure you want to disable the account, click **Yes**.
9. At the Disable Users prompt, you can enter a message to appear if someone tries to log into the account. Enter a message, if needed, then click **Apply**.



Should the Admin Account attempt to authenticate on the User Setup site, they will see the following:



Important:
You will no longer be able to log in as the default Admin account and will need to log using the alternate admin account created in the previous section. Access to the Hypori Halo Admin Console will still be granted from any workstation that has the default Admin account's certificate. It is recommended to delete this certificate from the workstation(s) to prevent accessing the Admin Console using the default Admin account.

Viewing the User Activity History

The Activity History page shows server events generated by users, which is stored as the Users Activity Log.

To view the Users Activity Log:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select either the root node or a domain.
4. Click the **Activity History** tab.
5. Under Users Activity Log, scroll through the list of activities. By default, the table is filtered to show the last 50 activities that occurred since yesterday.

6. To filter the list, select one of the following options in the **Fetch History since** list:
    - **Yesterday:** Shows alerts that occurred with a timestamp one day before the current date.
    - **Last Week:** Shows alerts that occurred over the seven-day period from the previous week.
    - **Last Month:** Shows alerts that occurred in the previous calendar month.
    - **Last Year:** Shows alerts that occurred in the previous calendar year.
    - **All:** Shows all logged alerts.
7. To limit the number of records retrieved, select an option from the Max Records to Fetch list.

For each task, the User Activity Log table shows:

- **User Name:** The name of the user who initiated the activity.
- **Time:** The date and time that the task was initiated.
- **Activity:** The type of user activity.
- **Details:** Additional information about the user activity.

Using the ADB User Data Push

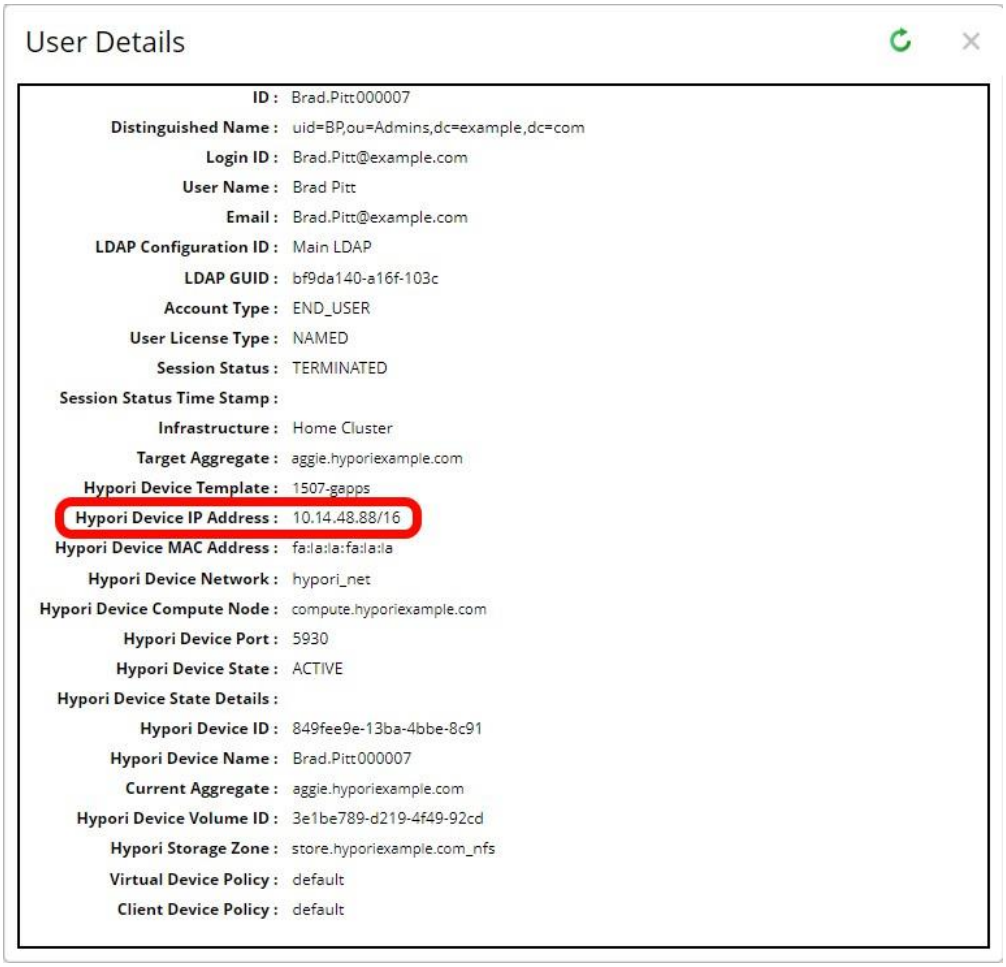
You can use the ADB User Data Push process to push files to virtual workspaces.

Note:
An example of this process being used is to move files from an old virtual workspace to a newer virtual workspace.

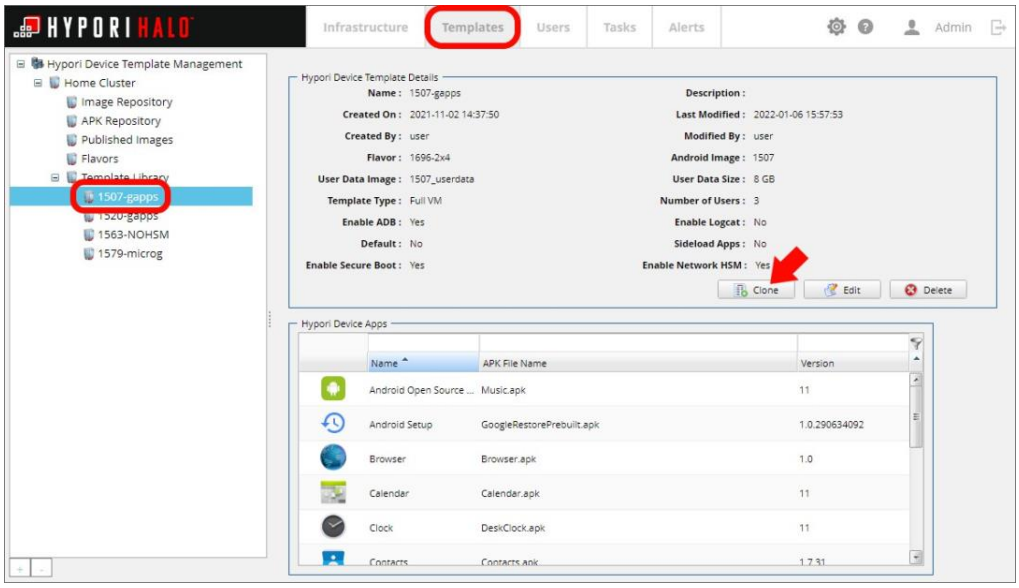
To use the ADB User Data Push:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the user's domain.
4. Click the **Users** tab.
5. In the Users Configuration table for this domain, hover your cursor over the user who needs to receive the data push.
6. Click the **User Details** icon:

7. Locate the Hypori Device IP Address for the user



8. Verify ADB is enabled in the user's template.
    a. Click **Templates**.
    b. In the navigation pane, under the Template Library, select on the template that is currently deployed on the user's virtual workspace.
    c. Click **Clone**.

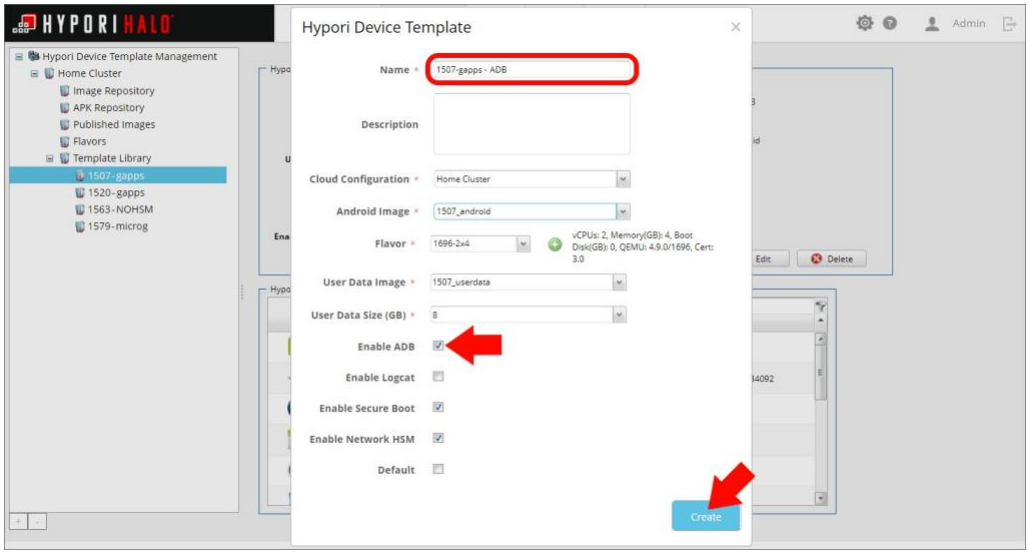


d. Change the name to follow your naming convention.

e. Check the box next to **Enable ADB**.

> **Note:**
>
> ADB must be enabled for the file transfer to work.

f. Click **Create**.

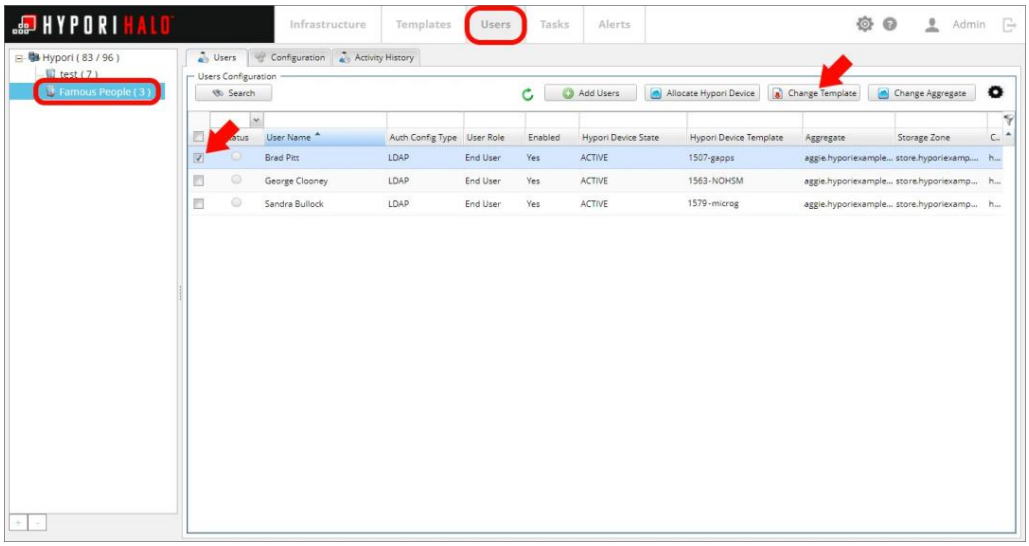


g. In the menu, click **Users**.

h. In the navigation pane, select the domain to which the user belongs.

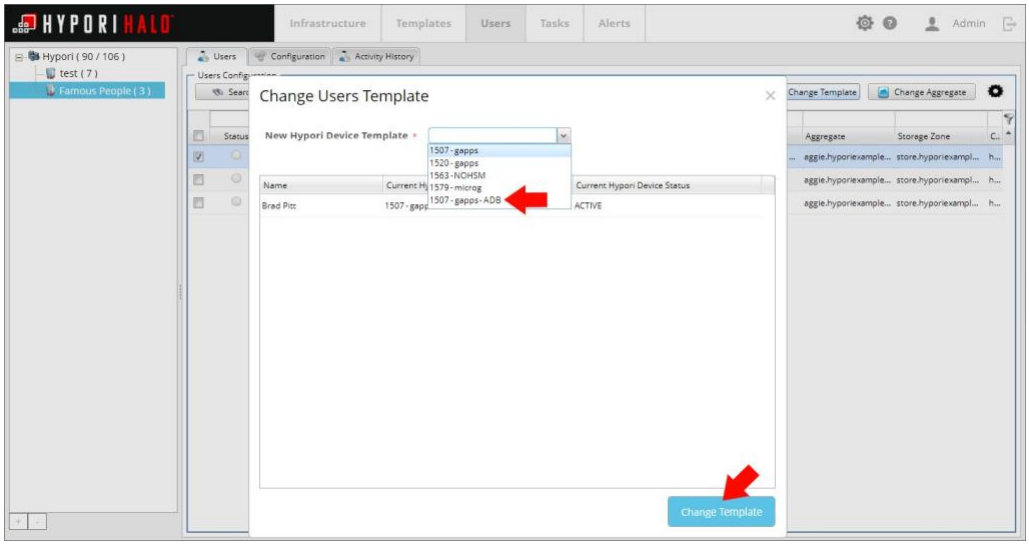
i. Find the user and check the box next to their name.

j. Click **Change Template**.



k. Select the newly cloned template in the drop-down list.

l. Click **Change Template**.



9. Hover your cursor over the virtual workspace's entry and select the **Stop Hypori Device** icon.
10. SSH into the provisioning server. Run:

```
ssh <account_name>@<provisioning_server's_IP_address>
```

11. Elevate privileges. Run:

```
sudo su
```

12. Create an android-tools repository. Run:

```
createrepo /opt/hypori/repos/Hypori/com/hypori/android-tools/
```

13. SSH into the compute node. Run:

```
ssh <account_name>@<compute_node's_IP_address>
```

14. Elevate privileges. Run:

```
sudo su
```

15. Clear any cached yum packages and install android-tools. Run:

```
yum clean all

yum install android-tools
```

16. Transfer the files being moved to the `/tmp` directory on the management server.
17. SSH into the management server.

```
ssh <account_name>@<management_server's_IP_address>
```

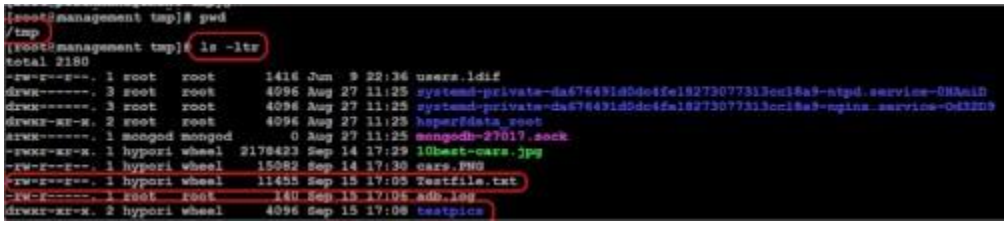
18. Elevate privileges. Run:

```
sudo su
```

19. Install ADB. Run:

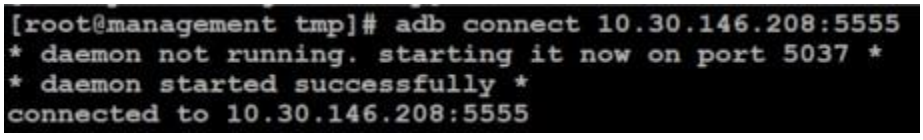
```
yum install adb
```

20. Locate the files in the `/tmp` directory that were imported in step 8.



21. Connect to the user's virtual workspace. Run:

```
adb connect <ip_address_of_virtual_workspace>:5555
```



22. Select the directory containing the files and copy the files to the user's virtual workspace. Run:

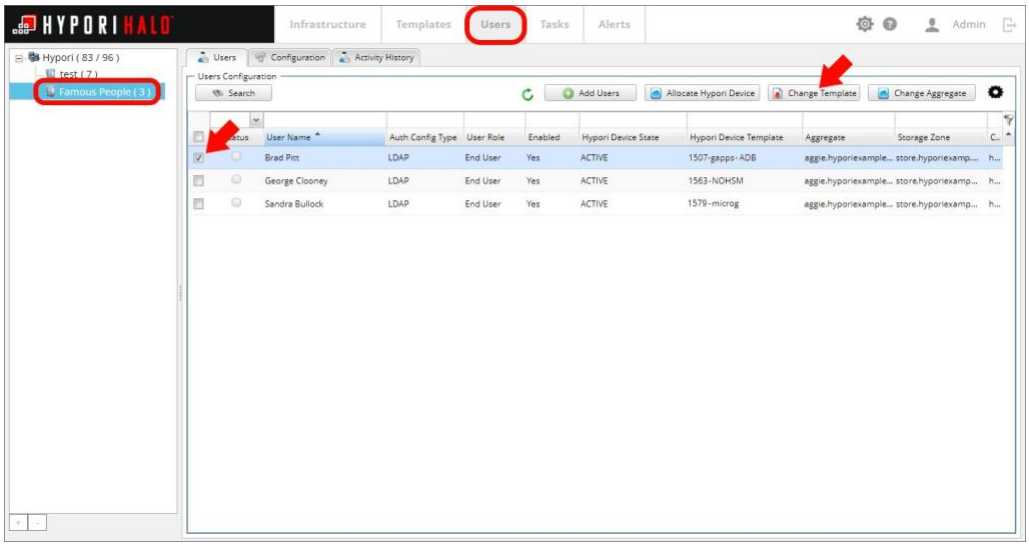
```
adb -s <ip_address_of_virtual_workspace>:5555 push /tmp/<file_name>
```

23. Once the files are transferred, disconnect the shell window. Run:

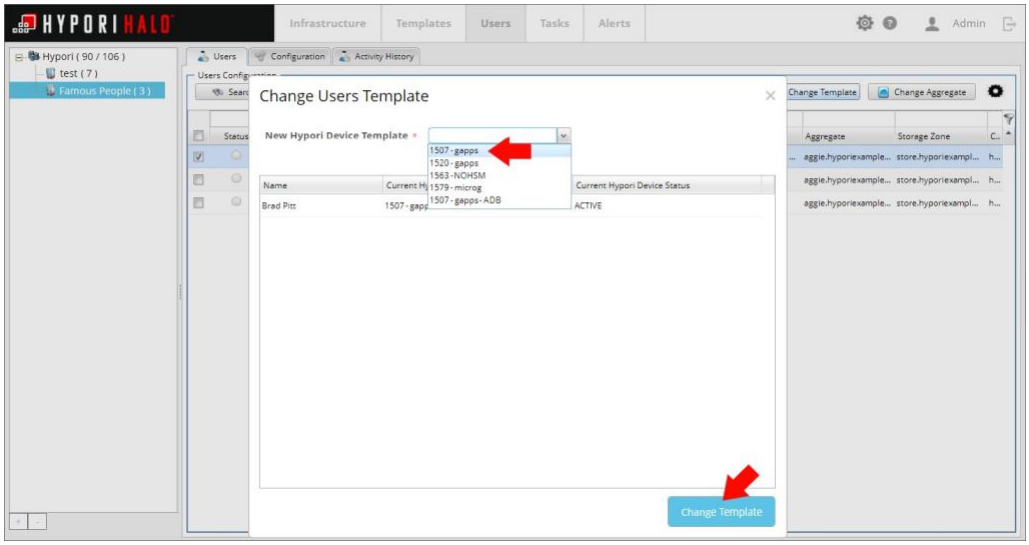
```
adb kill-server
```

```
[root@management tmp]# adb kill-server
[root@management tmp]#
```

24. Switch the user back to their original template.
    a. In the menu, click **Users**.
    b. In the navigation pane, select the domain to which the user belongs.
    c. Find the user and check the box next to their name.
    d. Click **Change Template**.



    e. Select the original template in the drop-down list.
    f. Click **Change Template**.



25. Delete the cloned template that has ADB enabled.

a. Click the **Template** tab.
b. Under the Template Library, select the cloned template that has ADB enabled.
c. Click **Delete**.

Managing Hypori Halo Virtual Workspaces

You can manage users' virtual workspaces from the Hypori Halo Admin Console.

Allocating a Virtual Workspace

You must allocate a virtual workspace before the corresponding user can access it. Until you allocate them a virtual workspace, the Hypori Halo Admin Console flags the user in the User Configuration table with an exclamation point and shows a Status value of UNALLOCATED.

To allocate a virtual workspace to a user:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the user's domain.
4. Click the **Users** tab.
5. In the Users Configuration table, check the box to the left of the user's name. You can select more than one user.
6. Click **Allocate Hypori Device**.
7. In the confirmation box, click **Yes**.
   A virtual workspace will be allocated to the user based on the template associated with the user's account.

Stopping and Starting a Virtual Workspace

When you stop a virtual workspace, you are effectively powering it off.

Tip:
When the virtual workspace (also referred to as a Hypori Device in the Admin Console's User Interface) is in the stopped state, users cannot access the virtual workspace and notifications are not available.

Stopping and then starting a virtual workspace effectively reboots it. All apps that were running when it was stopped must be restarted when the virtual workspace is restarted.

You can stop virtual workspaces for individual users, select users within a domain, or all users on a compute node.

To stop or start a user's virtual workspace:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the user's domain.
4. Click the **Users** tab.
5. In the Users Configuration table, check the box to the left of the user's name. You can select more than one user.
6. In the Users Configuration area, just above the table, click the **More Actions** icon.

7. From the More Actions menu, click **Stop Hypori Devices** or **Start Hypori Devices**.
8. In the confirmation box, click **Yes**.

You can also stop all virtual workspaces on a compute node. For more information, see Stopping All Virtual Workspaces on a Compute Node *(on page 21)*.

Pausing a Virtual Workspace

When you pause a virtual workspace, you are effectively putting it to sleep. It can be activated quickly because it does not have to load or boot. Pausing a virtual workspace requires memory and swap space.

Note: When the virtual workspace is in the paused state, notifications are not available to the end user.

To pause a user's virtual workspace:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the user's domain.
4. Click the **Users** tab.
5. In the Users Configuration table, check the box to the left of the user's name.

> **Tip:**
> You can select more than one user,

6. In the Users Configuration area, just above the table, click the **More Actions** icon..

7. From the More Actions menu, click **Pause Hypori Devices**.
8. In the confirmation box, click **Yes**.

Rebooting a Virtual Workspace

To reboot a user's virtual workspace:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the user's domain.
4. Click the **Users** tab.
5. In the Users Configuration table, hover your cursor over the row associated with the user.
6. Click the **Reboot Hypori Device** icon.

7. In the confirmation box, click **Yes**.

The status indicator in the Users Configuration table may remain green through the reboot.

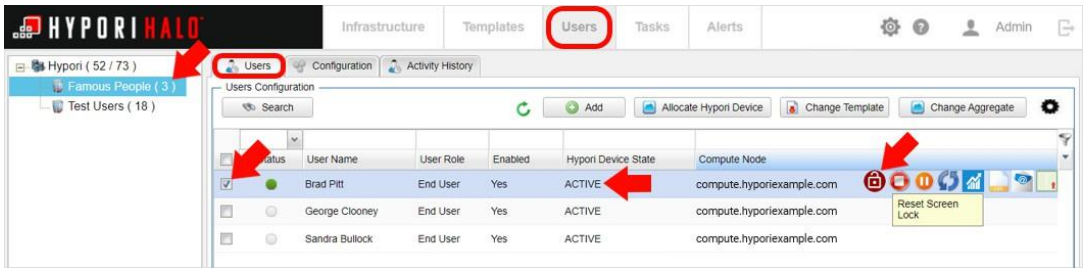
Resetting the Screen Lock in a Virtual Workspace

Hypori Halo Administrators can unlock an end user's virtual workspace if the device gets locked due to an incorrect PIN being entered too many times.

Tip:
The number of maximum failed login attempts is defined in the virtual workspace policy.

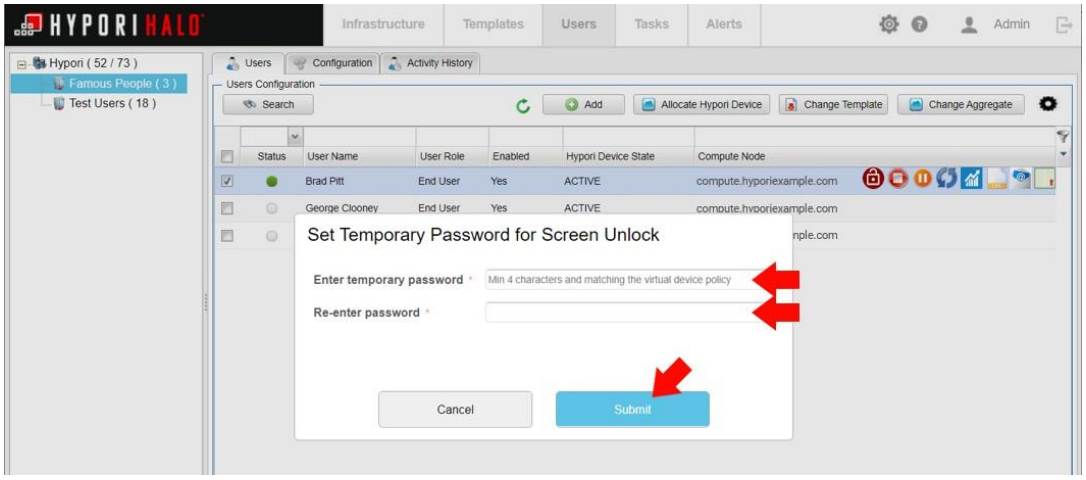
To reset the screen lock on a user's virtual workspace, perform these steps:

1. Open the Hypori Halo Admin Console.
2. In the menu , click **Users**.
3. In the navigation pane, select the user's domain.
4. Click the **Users** tab.
5. Search for the user needing to be reset from the user list.
6. Select the user from the list, **after verifying the Hypori Device State is listed as being in an ACTIVE state**.

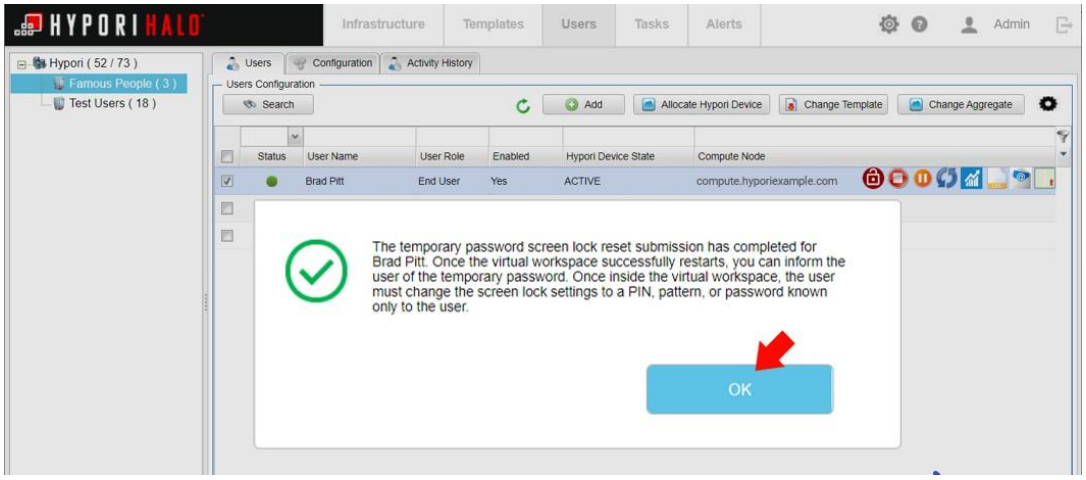


7. Click the **Reset Screen Lock** icon (the red unlock icon).

8. Enter a temporary password for the account and click **Submit**. The user's virtual workspace will be rebooted as part of the screen lock reset process.



9. Check the dialog box to confirm the password was successfully reset, then click **OK**.



10. The administrator should share the temporary password with the user. Once the user logs on, they will be prompted to enter the temporary password.

Important:

Once inside the virtual workspace, the user is responsible to change the screen lock settings to a PIN, pattern, or password only known to the user. The user will be prompted to enter the temporary password again when setting up new screen lock credentials.

Deleting a Virtual Workspace

To delete the virtual workspace for a specific user:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the user's domain.
4. Click the **Users** tab.
5. In the Users Configuration table, check the box to the left of the user's name.

   Tip:

   You can select more than one user.
6. In the Users Configuration area, just above the table, click the **More Actions** icon.

   
7. From the More Actions menu, click **Delete Hypori Devices**.

   You can also delete a virtual workspace by holding your cursor over the row in the table and clicking the **Delete** icon.
8. In the confirmation box, click **Yes**.

   The virtual workspace for the selected user is deleted.

You can also delete all virtual workspaces on a compute node. For more information, see Deleting All Virtual Workspaces on a Compute Node *(on page 27)*.

Creating User Volumes

To create a user volume:

1. In the menu, click **Users**.
2. In the navigation pane, select the user's domain.

3. Click the **Users** tab.
4. In the Users Configuration table, check the box to the left of the user's name. You can select more than one user.
5. In the Users Configuration area, just above the table, click the **More Actions** icon.

6. From the More Actions menu, click **Create User Volume**.
7. In the confirmation box, click **Yes**.

Deleting User Data

Before you begin, you must Delete (un-allocate) the user's virtual workspace. *(on page 104)*.

To delete user data for specific users:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the user's domain.
4. Click the **Users** tab.
5. In the Users Configuration table, check the box to the left of the username. You can select more than one user.
6. In the Users Configuration area, just above the table, click the **More Actions** icon.

7. From the More Actions menu, click **Delete User Data**.
   You can also delete user data by holding your cursor over the row in the table and clicking the **Delete User Data** icon.
8. In the confirmation box, click **Yes**.
   The user volume for the selected user is deleted.

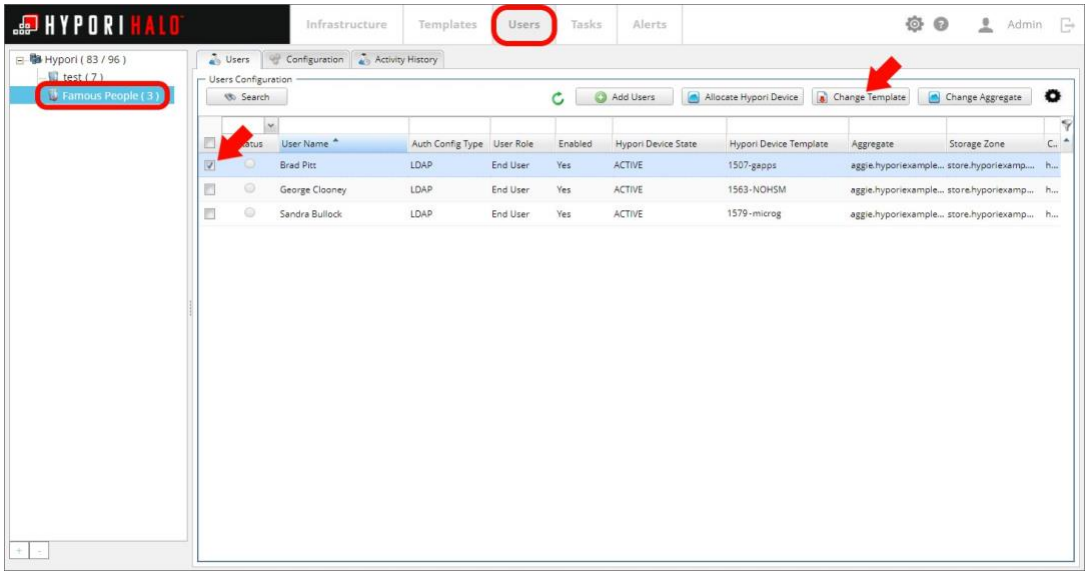
Changing Templates

To change the template associated with a user account:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the user's domain.
4. Click the **Users** tab.
5. In the Users Configuration table, check the box to the left of the user's name.

> **Note:**
> You can select more than one user.

6. Click **Change Template**.



7. In the Change Template box, select a template from the **New Hypori Device Template** list.
8. Click **Change Template**.

The selected user accounts are assigned the new template. During this process, the virtual workspace is shut down and the user is logged out.

Changing Aggregates

You can move a virtual workspace from one aggregate to a different aggregate if the new aggregate shares the same storage zone.

To change the aggregate for a user:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the user's domain.
4. Click the **Users** tab.
5. In the Users Configuration table, check the box to the left of the user's name.

> **Tip:**
> You can select more than one user.

6. Click **Change Aggregate**.
7. In the Change Aggregate box, select a server from the **Target Aggregate** list.
8. Click **Change Aggregate**.

The selected user accounts are assigned the new aggregate, and the user's virtual workspace is migrated to the new aggregate at the next login from the Hypori Halo Client.

Changing the Default Authentication Time

In some situations, it may become necessary to increase or decrease the authentication token time on the Hypori Halo virtual workspace.

> **Note:**
> This task is performed outside of the Hypori Halo Admin Console.

To change the Authentication Time parameters:

1. SSH to the provisioning server. Run:

```
ssh <account_name>@<provisioning_server's_IP_address>
```

2. Elevate privileges. Run:

```
sudo su -
```

3. Edit the `hostinfo.yaml` file. Run:

```
vi /root/hypori/hostinfo.yaml
```

4. Add the following values to the management server section:

```
profile::mgmt::auth_token_ttls:
  VM: 3600
  Notification: 604800
  WEBAPP: 600
  WEBAPP2: 600
  ADMIN_PORTAL: 600
  SHARED_CLIENT_DEVICE: 60
```

Note:

The values are specified in seconds.

- 60 = 1 minute
- 600 = 10 minutes
- 3600 = 1 hour
- 604800 = 1 week

5. Change the values as required.

   The Token Types and their default settings are:

Token Type	Token Description	Default Setting
VM	Token for the Clients to connect to their virtual workspace	3600
Notification	Token for the Clients to get notifications	604800
WEBAPP	Token for webapp without secondary auth	600
WEBAPP2	Token for webapp with secondary auth	600
ADMIN_PORTAL	Token for the admin console	3600
SHARED_CLIENT_DE-VICE	Token for shared device clients	60
VIRTUALDEVICE	Token for virtual workspaces	3600

6. Save and close the file.
7. Run the `step2` script to re-provision the servers. Run:

```
/root/hypori/step2-autoProvision.sh <foreman_admin_password> <root_password_new_hosts>
 [bootloader_password_new_hosts]
```

   where:

   - *foreman_admin_password* is the password you set when you installed the provisioning server.
   - *root_password_new_hosts* is the password that will be used for the `root` user on all newly provisioned hosts.

Viewing Virtual Workspace App Usage

The App Usage tab shows information about apps the user has accessed on the virtual workspace from the time the user was created.

To view app usage details:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the user's domain.
4. Click the **Users** tab.
5. In the Users Configuration table, hover your cursor over the user whose information you want to view.
6. Click the **Hypori Device Details** icon:

7. In the Hypori Device Details box, click the **App Usage** tab.
8. Click the **Refresh** button to refresh the data on the tab.

The App Usage tab shows:

- **ID:** The Hypori Halo system identifier for the user.
- **User Name:** The first and last name of the user.
- **Last Connected:** The date and time when the user's last virtual workspace session ended.
- **Total table:** Information about app usage from the time the user was created.
- **Dated tables:** Information about app usage for the day specified.
- Each table shows the following information, which is gathered when the user disconnects from the virtual workspace:
    - **App icon:** The icon associated with the app. A placeholder icon is shown for apps that are not in the APK repository.
    - **App Name:** The name of the app.
    - **Count:** The number of times the app has been accessed.
    - **Time:** The total amount of time the app has been in focus while the user was connected to the virtual workspace.

Viewing Virtual Workspace Session Statistics

To view virtual workspace session statistics:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the user's domain.
4. Click the **Users** tab.
5. In the Users Configuration table, hold your cursor over the user whose information you want to view.
6. Click the **Hypori Device Details** icon:

7. In the Hypori Device Details box, click the **Sessions** tab.
8. Click the **Refresh** button to refresh the data on this tab.

The Sessions tab shows:

- **ID:** The Hypori Halo system identifier for the user.
- **User Name:** The first and last name of the user.
- **Last Connected:** The date and time when the user's last virtual workspace session ended.
- **Sessions:** The number of times the user connected to the virtual workspace in the last 30 days.
- **Time Spent on Hypori Device:** The amount of time the user has spent connected to the virtual workspace in the last 30 days.
- The chart shows the number of sessions and time spent on the virtual workspace, by date.

Viewing Virtual Workspace Data Usage

To view virtual workspace data usage statistics:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the user's domain.
4. Click the **Users** tab.
5. In the Users Configuration table, hold your cursor over the user whose information you want to view.
6. Click the **Hypori Device Details** icon:

7. In the Hypori Device Details box, click the **Data Usage** tab.
8. Click the **Refresh** button to refresh the data on this tab.

The Data Usage tab shows:

- **ID:** The Hypori Halo system identifier for the user.
- **User Name:** The first and last name of the user.
- **Last Connected:** The date and time when the user's last virtual workspace session ended.
- **Data Sent/Received from Client:** The amount of data sent to and received from the Hypori Halo Client in the last 30 days.
- The chart shows the data sent and received using Wi-Fi versus cellular.

Data Usage and the Virtual Workspace Launcher

In the event a user is experiencing excessive data usage, verify they are using the Hypori Halo Client Launcher and not the Virtual Workspace Launcher. The Client Launcher is set as the default. Using the Virtual Workspace Launcher will consume excessive amounts of data and will be less responsive than using the Client Launcher.

Note:
There is a toggle to specify whether the **All User Settings** option is visible or not. This information is provided in JSON data. If the option is set to not visible, users are unable to select the Virtual Workspace Launcher.

Viewing Virtual Workspace Usage Locations

To view the locations on a map where a virtual workspace has been recently accessed:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the user's domain.
4. Click the **Users** tab.
5. In the Users Configuration table, hold your cursor over the user whose information you want to view.
6. Click the **Hypori Device Details** icon:

   
7. In the Hypori Device Details box, click the **Locations** tab.
8. Click the **Refresh** button to refresh the data on this tab.

The Locations tab shows:

- **ID:** The Hypori Halo system identifier for the user.
- **User Name:** The first and last name of the user.
- **Last Connected:** The date and time when the user's last virtual workspace session ended.
- The map shows the locations from which the user has accessed their virtual workspace in the last 30 days.

Viewing Screenshots of a Virtual Workspace

To view a screenshot of the user's virtual workspace:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the user's domain.
4. Click the **Users** tab.
5. In the Users Configuration table, hold your cursor over the user whose screen you want to view.
6. Click the **Hypori Device Details** icon:

7. In the Hypori Device Details box, click the **Screenshot** tab.
8. Click the **Refresh** button to refresh the data on this tab.

The Screenshot tab shows:

- **ID:** The Hypori Halo system identifier for the user.
- **User Name:** The first and last name of the user.
- **Last Connected:** The date and time when the user's last virtual workspace session ended.
- A snapshot of the user's virtual workspace screen.

Disabling the View Screenshot Feature

By default, users with the administrator or auditor role can view virtual workspace usage statistics and the virtual workspace screen of any user. This feature can be disabled globally, but this task is performed outside of the Hypori Halo Admin Console.

To disable the view screenshot feature:

1. SSH to the provisioning server. Run:

```
ssh <account_name>@<provisioning_server's_IP_address>
```

2. Elevate privileges. Run:

```
sudo su -
```

3. Edit the `/usr/share/openstack-puppet/modules/profile/templates/mgmt/services.yml.erb` file. Run:

```
vi /usr/share/openstack-puppet/modules/profile/templates/mgmt/services.yml.erb
```

4. Locate the `miscConfig` section and change the value of the `enableVirtualDeviceScreenshots` property to `false`.
5. Save and close the file.
6. Perform a manual Puppet update on the management server.

    a. SSH to the management server. Run:

    ```
    ssh <account_name>@<targeted_node's_IP_address>
    ```

    b. Elevate privileges. Run:

    ```
    sudo su -
    ```

    c. Instruct the server to conduct a manual Puppet update. Run:

    ```
    puppet agent -tv
    ```

Managing Hypori Halo Network Settings

Configuring SMTP Settings

To configure settings for your SMTP server:

1. Log into the Hypori Halo Admin Console.
2. In the upper right corner of the screen, click the **Settings** icon.

3. Click **SMTP Settings** to open the SMTP Configuration box.
4. Click **Update**.
5. In the **SMTP Server** field, type the fully qualified name of your SMTP server.
6. In the **Port** field, type the port number used to access the SMTP server. This value is 587 by default.
7. In the **From (Name)** field, type your name.
8. In the **From (Email)** field, type your email address.

9. If you want to use Transport Layer Security (TLS) to ensure privacy when communicating with the SMTP server, click **Use TLS**.
10. If you want to use credentials to access the SMTP Server, click **Use Authentication** and then type the proper credentials in the **User Name** and **Password** fields.
11. Click **Apply**.

To test your connection by sending an email:

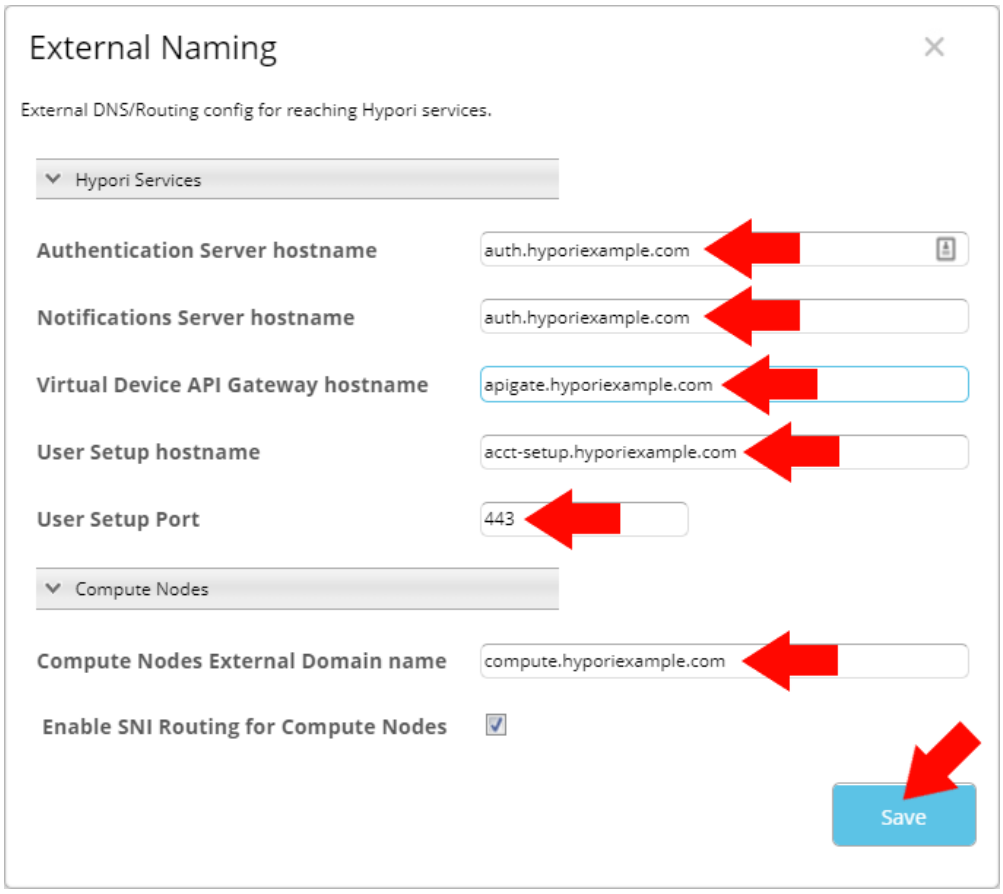
1. Click **Test**.
2. In the Test SMTP Configuration box, type your email address in the **To (Email) field**.
3. In the **Email Subject** field, type a subject for the test email.
4. In the **Email Text** field, type content for the test email.
5. Click **Send Test Email**.

Configuring External DNS Naming

External naming allows the administrator to select the domain name used to access the Hypori Halo services.

Note:
If users are provisioned and the hostname information is altered, any previously provisioned users will be unable to connect.

1. Log into the Hypori Halo Admin Console.
2. Click the **Settings** icon in the upper right corner of the screen.
3. Select **External Naming** from the menu.
4. Enter the desired external DNS name or port information into the following fields:
    - Authentication server hostname
    - Notification server hostname
    - Virtual Device API Gateway hostname
    - User Setup hostname
    - User Setup port (this should be 443 by default)
    - Compute node(s) external domain name(s)



5. Click **Save**, then click the ✕ in the upper right corner to exit this screen.

Configuring Single Port Access

Single Port Access is an optional feature of the Hypori Halo environment. It allows the public network to utilize a single port instead of requiring a range of ports.

Configuration:

1. The TLS (Transport Layer Security) Proxy must be properly configured:
   - Compute nodes will require certificates which contain a wildcard for every host. (e.g.: *.compute1.hyporiexample.com)

> **Note:**
> This is especially needed for customers who wish to deploy their own custom server certificates, rather than depending on Hypori's tool generated internal server certificates.

2. The SNI (Server Name Indicator) routing flag within the Hypori Halo Admin Console must be enabled:

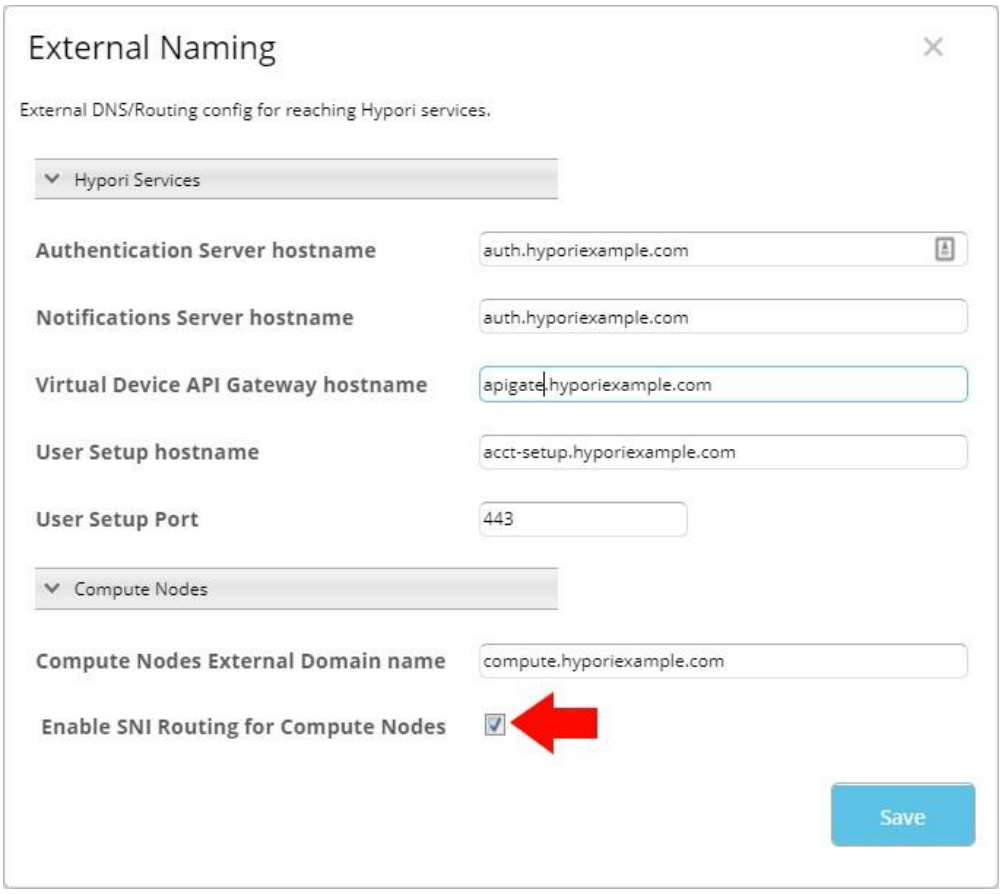
    a. Log into the Hypori Halo Admin Console

    b. In the upper right corner of the screen, click the **Settings** icon.

    c. Select **External Naming** from the menu.

    d. Check the box next to **Enable SNI Routing for Compute Nodes**.

    e. Click **Save**.

Managing Shared Devices and Their Users

The Hypori Halo environment supports shared devices, which are physical devices that are provisioned by the administrator and can be used by users with a shared device account to access their virtual workspaces.

Note:
A shared device must have a camera, due to the requirement to provision the device using a QR code.

Users with shared device accounts are different from other Hypori Halo users.

Users with shared device accounts:

- Do not install or configure anything on the physical shared device used to access the virtual workspace.
- Do not have a client certificate. Instead, the client certificate on the physical device is associated with the shared device itself.
- Shared device users must authenticate with the virtual workspace using their Active Directory or LDAP credentials.
- Can only have the end-user role.

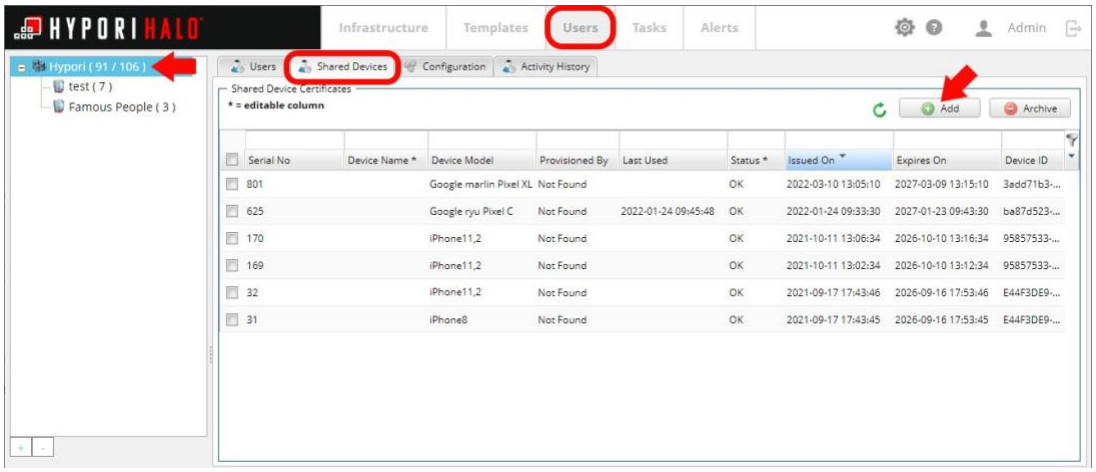
Adding Shared Devices

You must have the administrator role to add a shared device. When you scan a QR code to add a new shared device, a unique certificate is installed on the device to identify it to the Hypori Halo environment.

Before you begin, install the Hypori Halo Client on the shared device.

To add a shared device:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. Click the top-level domain if it is not already selected.
4. Click the **Shared Devices** tab.
5. Click **Add**.

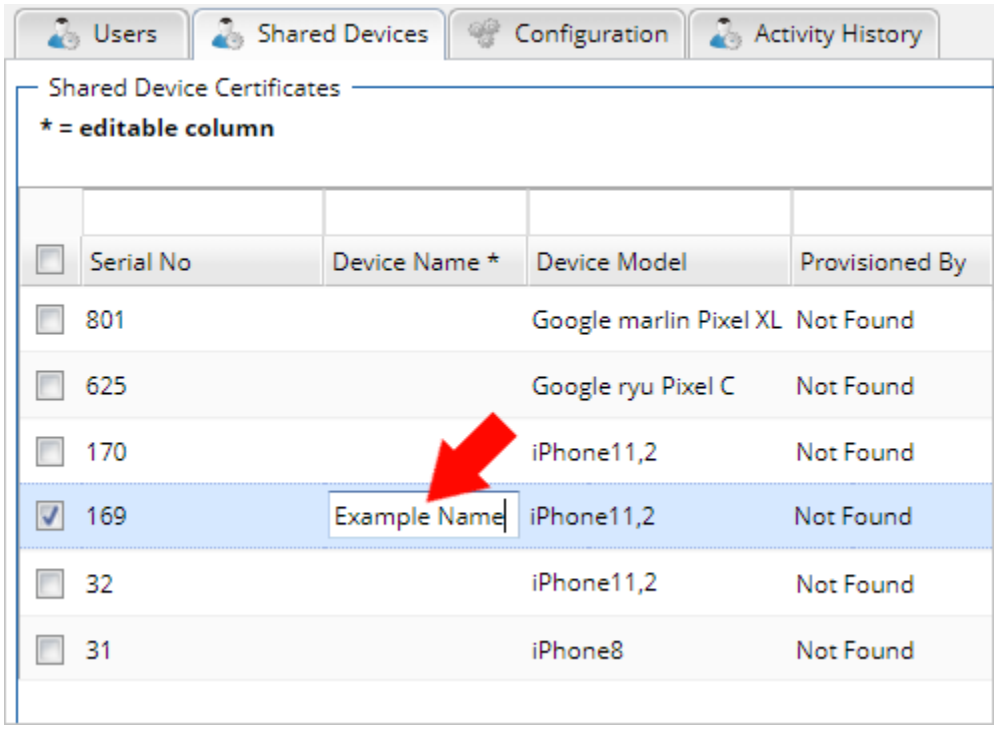


The Provision Shared Device box shows a QR code for the shared device.

6. On the shared device, open the Hypori Halo Client and scan the QR code.

> **Tip:**
> To provision another device, click the **Refresh** icon, generate a new QR code, and scan it with the new shared device.

7. Return to the Hypori Halo Admin Console, where you will see the table shows the shared device.
8. If you want to add a name that identifies the device, select the Device Name cell for the shared device and type a descriptive name.



Adding Users with Shared Device Accounts

Before you begin, ensure that the user you want to add to the Hypori Halo environment is available on the Hypori LDAP server or your Active Directory server.

> **Tip:**
> To make it easier to manage users with shared device accounts, it is highly recommended that you include these users in a separate domain.

To add a user:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the domain for the new user.
4. Click the **Users** tab.
5. Under Users Configuration, click **Add** to open the Add Users box.
6. Click **Shared Physical Device User**.
7. In the **Authentication Configuration** list, select the configuration that will be used to authenticate the new user.
8. In the **LDAP Search Scope** list, select the LDAP organization for the user.
9. In the **LDAP Filter** list, select the LDAP query that will be run to find the user.
10. In the **User License Type** list, select the license type that you want to associate with the new user.
    - **Named:** An individual license that gives the assigned user constant access to the Hypori Halo environment.
    - **Concurrent:** A shared license from a pool of concurrent licenses. If all concurrent licenses are in use, the next user who tries to access the server with this license type is denied access until a concurrent license becomes available.
11. In the **Allocate Hypori Device** box, select if you want to make this user's virtual workspace available automatically after adding the user. If you do not allocate the virtual workspace at this point, you must do so manually before the user can access his or her virtual workspace.
12. In the **Home Cluster** list, select the server cluster for the new user.
13. In the **Aggregate** list, select the aggregate that you want to run the user's virtual workspace.
14. In the **Hypori Device Template** list, select the template that will define the look and feel of the user's virtual workspace.
15. Click **Fetch Users from LDAP** to populate the users list. If the user is not in the list, you may need to add the user in Active Directory.

16. In the users list table, check the box next to the name of the users that you want to add. You cannot add users that are already in the Hypori Halo user database.
17. Click **Add Users**.

Users with a shared device account can access their virtual workspace from any shared device, using their LDAP or Active Directory credentials.

Revoking Client Certificates for Shared Devices

To revoke a certificate for a shared device:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. Select the top-level domain if it is not already selected.
4. Click the **Shared Devices** tab.
5. Select the Status cell for the device.
6. Click **REVOKED**.
7. In the confirmation box, click **Yes**.

Archiving Certificates for Shared Devices

Before you begin, you must revoke the certificate you want to archive. For more information, see Revoking Client Certificates for Shared Devices *(on page 120)*.

To archive a certificate for a shared device:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. Select the top-level domain if it is not already selected.
4. Click the **Shared Devices** tab.
5. In the table, check the box for the row associated with the shared device.

> **Tip:**
> You can select more than one.

6. Click **Archive**.
7. In the confirmation box, click **Yes**.

Chapter 6. Hypori Halo Client

The Hypori Halo Client is the app on the user's mobile device that uses secure encrypted protocols to communicate with their virtual workspace located in the secure Hypori Halo environment.

Operating System Requirements

The Hypori Halo Client is designed to run on Apple, Android, and Windows devices using the following Operating Systems:

Android OS

- Android 8.1 [Oreo (Go edition)] or later

Apple OS

- iOS 14.8 or later

Windows OS

- Windows 10 (64 bit)
    - minimum version 21H1 or later

Configuring Client Device Policies

You can define and manage policies for the Hypori Halo Client with the Client Device Policies in the Hypori Halo Admin Console.

To configure the Client Device Policies:

1. Open the Hypori Halo Admin Console.
2. Click **Users**.
3. In the navigation pane, select the domain you want to view.
4. Click the **Configuration** tab.
5. Scroll down to the Client Device policies box.
    - Click **Clone** to create a copy of the selected policy.
    - Click **View Policy** to review the selected policy.
6. If there is more than one policy listed, select the version to be modified and click **Edit**.

7. Locate the setting(s) you want to update.
8. Change the setting under Value to the desired entry.

> **Note:**
> Valid entries are listed under Type.

9. When the desired settings are updated, click **Apply**.
10. Click the ✕ in the upper right corner to close the window.
    - The policy change will take affect only when the user must authenticate.
    - How often the user authenticates is controlled by the configuration setting.
    - To force an immediate re-authentication, the virtual workspace must be stopped. For more information, see Stopping and Starting a Virtual Workspace *(on page 100)*.

Downloading Client Device Policies

You can download a copy of the policies for the Hypori Halo Client in the Hypori Halo Admin Console. This can be used by an administrator who prefers using a specific JSON editor.

To download the Client Device Policies:

1. Open the Hypori Halo Admin Console.
2. Click **Users**.
3. Click the **Configuration** tab.
4. Scroll down to the Client Device Policies box.
5. If there is more than one policy listed, select the version to be downloaded and click **Edit**.
6. Click the **Download Policy** icon.

7. If you have a popup blocker, you will have to click **Allow Once**.
8. Click **Save** to download the file to the Windows Downloads folder.

Uploading Client Device Policies

You can upload a copy of the policies for the Hypori Halo Client in the Hypori Halo Admin Console. This can be used by an administrator who prefers using a specific JSON editor or who has a pre-made policy document they wish to implement.

To upload Client Device Policies:

1. Open the Hypori Halo Admin Console.
2. Click **Users**.
3. Click the **Configuration** tab.
4. Scroll down to the Client Device Policies box and click **Edit**.
5. Click the **Upload Policy** icon.

6. If you have a popup blocker, you will have to click **Allow Once**.
7. Click **Browse**.
8. Navigate to the file you wish to upload and click **Open**.
9. Click **Upload**. When the file has completed uploading, close the window.
10. Click **Apply**.

System Configuration Policies

These settings define and enforce specific system policies that are configured by the management server administrator. An end user cannot modify system policy.

Important:
Any enabled System Configuration Policies must be in the 'system' section of the Client Device Policy.

Client Launcher Border Color

This setting (`client-launcher-border-color`) specifies the color of the border surrounding the client launcher. If no value is specified, then no border will be drawn.

Valid values include: `blue`, `green`, `orange`, `red`, `yellow` or no value specified.

Default: no value specified

Platforms: Android, iOS

Require Device Administrator

This setting (`require-device-admin`) specifies whether the device must be configured with the device manager or other security features enabled (i.e., a complex password must be used instead of a PIN), before the user may connect to the virtual workspace.

Valid values include: `true` and `false`

Default: `false`

Platforms: Android

Expire Password Time Period

This setting (`password-age-days`) specifies the timeframe for the account password before it expires and must be changed. If a timeframe is not designated, then the password will not expire.

Valid values include: `any number` and `no value specified`

Default: `no value specified`

Platforms: Android

Note:
This policy only applies if the *Require Device Administrator* policy is set to true.

Password Complexity

This setting (`password-quality`) specifies the password/PIN complexity required for connecting to the virtual workspace on Android Operating Systems. If the policy is set to unspecified in the system policies, then there are no requirements imposed on users to have complex passwords.

Valid values include: `complex`, `unspecified`, `numeric`, `alphabetic`, and `alphanumeric`.

Default: `unspecified`.

Platforms: Android

Note:
This policy only applies if the *Require Device Administrator* policy is set to true.

Disable Camera/Enable Camera

This setting (`camera-enable`) specifies whether the camera is enabled for use by the Hypori Halo Client. By default, allowing the use of the camera in the client app is recommended.

Valid values include: `true` and `false`

Default: `true` (if the policy is not specified in the system settings)

Platforms: Android (only if the *Require Device Administrator* policy is set to true), iOS

Enable Screenshots

This setting (`screenshots-enable`) specifies whether screenshots are enabled for accounts using an Android device.

Valid values include: `true` and `false`

Default: `false` (if the policy is not specified in the system settings)

Note:
Having this policy set to false provides the most security when connected to the virtual workspace, as users are not allowed to take screenshots of the devices display.

Platforms: Android

Enable Restart on Next Connect

This setting (`connect-restart-enable`) specifies whether the *Enable Restart on Next Connect* option is available to the user on the Account Settings page.

Valid values include: `true` and `false`

Default: `true` (if the policy is not specified in the system settings)

Platforms: Android, iOS

Enable Push Notifications

This setting (`push-notifications-enable`) specifies whether handling of push notifications is handled in the client app.

Valid values include: `true` and `false`

Default: `false` (if the policy is not specified in the system settings)

Note:
By default, the management server is not configured to use push notifications.

Platforms: Android, iOS

Notification Interval

This setting (`notification-interval`) specifies the frequency for polling for notifications in seconds. A value of 0 or less means no polling will occur.

Valid values include: `any number`

Platforms: Android, iOS

Account (User Accessible) Policies

These settings define and enforce specific account level policies that can be configured by the management server administrator. The policies defined here are accessible by the end user unless they have been disabled on the management server.

> **Note:**
> Any enabled Account Policies must be in the 'settings' section of the Client Device Policy.

Allow Phone Dialer Bypass

This setting (`allow-phone-dialer-bypass`) specifies whether to allow the user to tap a phone number link in the virtual workspace and connect to the phone number using the physical phone's dialing capabilities.

Default: `true`.

Platform: Android, iOS

> **Note:**
> Users running Hypori Halo Client version 1.5 or earlier will continue to use the (`allow_phone_dialer_bypass`) setting which has a default value of `false`.

Use Local Keyboard

This setting (`use-local-soft-keyboard`) specifies whether the user to uses the phone's soft keyboard instead of the virtual workspace's soft keyboard.

Default: `true`.

Platform: Android, iOS

Enable Bluetooth

This setting (`bluetooth-enable`) specifies whether to allow the use of Bluetooth on the virtual workspace.

Default: `false`.

Platform: Android, iOS

Remember Password

This setting (`remember-password`) specifies whether the connection password to the Hypori Halo environment is cached so that it does not need to be entered every time a user connects to the virtual workspace. A value of `true` caches the connection password and hides this setting from the user. A value of `false` requires users to enter a password every time a connection is attempted and hides this setting from the user. When the administrator does not set a value, users can view and edit the setting.

Default: `false`.

Platform: Android, iOS

Enable Notifications

This setting (`notification-enable`) specifies whether the user can enable or disable notifications from the virtual workspace. If the setting is visible, modifiable and either the `notification-interval` is > 0 or `push-notifications-enable` is `true`, then the user can select the value, otherwise the 'Enable Notifications' setting will be hidden.

Default: `true`.

Platform: Android, iOS

Disconnect Policy

This setting (`disconnect-policy`) defines the amount of time to wait before terminating the Hypori Halo Client connection to the virtual workspace after a user leaves the client. A value of `delayed1` terminates the client connection to the virtual workspace after one minute. A value of `immediately` terminates the connection as soon as the client is closed. A value of `keepopen` maintains the client connection to the virtual workspace indefinitely.

Default: `delayed1`.

Platform: Android, iOS

Allow Compromised Devices

This setting (`allow-unsavory-devices`) specifies whether to allow a connection to a compromised or rooted mobile device. When the value is set to `false`, a connection to a compromised mobile device is not allowed.

Default: `false`.

> **Note:**
> Hypori Halo checks devices for common rooting, cloaking, or other dangerous packages. On Android devices, Hypori Halo also checks for suspicious processes, verifies the correct signing keys are in use, and ensures that important directories are not writable.

Platform: Android, iOS

Log Level

This setting (`logging-level`) specifies the logging level for the Hypori Halo Client. This setting only applies to Android devices. When the value is set to `none`, no logging occurs. A value of `error` results in only fatal errors or errors that impact the system functionality being logged. A value of `warning` results in non-fatal issues, worth noting, being logged. The `info` value is rarely used. The `debug` value is used to log any information relevant to a programmer being logged. A value of `verbose` results in everything being logged.

Default: `debug`.

Platform: Android

Sample Client Device Policy

When viewed, the Client Device Policy resembles the sample documentation below:

```
{
  "settings": {
    "allow-phone-dialer-bypass": {
      "description": "Indicates whether the phone dialer bypass is enabled in the Hypori client app. true if
 the bypass is enabled; false if not.",
      "modifiable": true,
      "platforms": [
```

```
        "Android",
        "iOS"
      ],
      "title": "Enable Client Phone Dialer",
      "type": "boolean",
      "value": true,
      "visible": true
    },
    "allow-unsavory-devices": {
      "description": "The user may connect to the virtual device if their physical device is compromised. The
default value is false, but the user can override it in the account settings.",
      "modifiable": true,
      "platforms": [
        "Android",
        "iOS"
      ],
      "title": "Allow Compromised Devices",
      "type": "boolean",
      "value": false,
      "visible": true
    },
    "bluetooth-enable": {
      "description": "the bluetooth capabilities of the Hypori client are disabled and can not be enabled by
the user.",
      "modifiable": false,
      "platforms": [
        "Android",
        "iOS"
      ],
      "title": "Enable Bluetooth",
      "type": "boolean",
      "value": false,
      "visible": false
    },
    "client-launcher-enable": {
      "description": "The Hypori client app should use the client-side launcher. The default value is true",
      "modifiable": true,
```

```
      "platforms": [
        "Android",
        "iOS"
      ],
      "title": "Use Client Launcher",
      "type": "boolean",
      "value": true,
      "visible": true
    },
    "disconnect-policy": {
      "description": "When the client should disconnect after the application is moved to the background.
The valid values are 'immediately' (disconnect immediately), 'delayed1' (disconnect after 1 minute),
'keepopen' (keep the connection open as long as possible)",
      "modifiable": true,
      "platforms": [
        "Android",
        "iOS"
      ],
      "title": "Disconnect Policy",
      "type": [
        "immediately",
        "delayed1",
        "keepopen"
      ],
      "value": "delayed1",
      "visible": true
    },
    "logging-level": {
      "description": "Enables debug logging level for the client when the app is connected to the account.",
      "modifiable": false,
      "platforms": ["Android"],
      "title": "Log Level",
      "type": [
        "none",
        "error",
        "warning",
        "info",
```

```
        "debug",
        "verbose"
      ],
      "value": "debug",
      "visible": false
    },
    "notification-enable": {
      "description": "If this setting is visible and modifiable and notification-interval is > 0 or
push-notifications-enable is true, the user can disable or enable notifications.",
      "modifiable": true,
      "platforms": [
        "Android",
        "iOS"
      ],
      "title": "Enable Notifications",
      "type": "boolean",
      "value": true,
      "visible": true
    },
    "remember-password": {
      "description": "the last password entered by the end user when authenticating should be remembered.
true if the password should be remembered, false if not. The default value is false. This is the most secure
setting for this policy.",
      "modifiable": false,
      "platforms": [
        "Android",
        "iOS"
      ],
      "title": "Remember Password",
      "type": "boolean",
      "value": false,
      "visible": false
    },
    "use-local-soft-keyboard": {
      "description": "Choose the device's soft keyboard instead of the soft keyboard in the virtual device. The
default value is true.",
      "modifiable": true,
```

```
      "platforms": [
        "Android",
        "iOS"
      ],
      "title": "Use Local Keyboard",
      "type": "boolean",
      "value": true,
      "visible": true
    }
  },
  "system": {
    "camera-enable": {
      "description": "The camera use by the Hypori client should be enabled. The default is true if the policy is not specified in the system settings.",
      "platforms": [
        "Android",
        "iOS"
      ],
      "title": "Enable Camera",
      "type": "boolean",
      "value": true
    },
    "client-launcher-border-color": {
      "description": "The color of the border to place around the client launcher. If no value is specified, no border will be drawn. Display the default launcher background pattern. The default is for no value to be specified in the system policies.",
      "platforms": [
        "Android",
        "iOS"
      ],
      "title": "Client Launcher Border Color",
      "type": "string",
      "value": "none"
    },
    "connect-restart-enable": {
```

```
     "description": "The Connect on Next Restart setting should be made available to the end user in the
account's Account Settings page. The default value is true if the policy is not specified in the system
settings.",
     "platforms": [
       "Android",
       "iOS"
     ],
     "title": "Enable Restart on Next Connect",
     "type": "boolean",
     "value": true
   },
   "notification-interval": {
     "description": "The frequency for polling for notifications in seconds. A value of 0 or less means no
polling.",
     "platforms": [
       "Android",
       "iOS"
     ],
     "title": "Notification Interval",
     "type": "number",
     "value": 120
   },
   "push-notifications-enable": {
     "description": "Handling of push notifications should be enabled in the client app. The default value
is false if the policy is not specified in the system settings. By default, the management server is not
configured to use push notifications.",
     "platforms": [
       "Android",
       "iOS"
     ],
     "title": "Enable Push Notifications",
     "type": "boolean",
     "value": true
   },
   "screenshots-enable": {
```

```
      "description": "Screen shots are enabled for the screens displayed for this account. The default is false
 if the policy is not specified in the system settings. This setting provides the most security when connected
 to the virtual device as it does not allow screen shots of those connected screens.",
      "platforms": ["Android"],
      "title": "Enable Screenshots",
      "type": "boolean",
      "value": false
    }
  },
  "version": {
    "major": 2,
    "minor": 0
  }
}
```


Configuring Virtual Workspace Policy

You can define and manage policies for the Hypori Halo virtual workspace with the Hypori Device Policies in the Hypori Halo Admin Console.

To configure the Virtual Workspace Policies:

1. Open the Hypori Halo Admin Console.
2. Click **Users**.
3. In the navigation pane, select the domain you want to view.
4. Click **Configuration**.
5. Scroll down to the Hypori Device Policies box.
    - Click **Download Schema** if you wish to use a schema editor.
    - Click **Clone** to create a copy of the selected policy.
    - Click **View Policy** to review the selected policy.
6. If there is more than one policy listed, select the version to be modified and click **Edit**.
7. Locate the setting(s) you want to update.
   If you are using variables in your virtual workspace policies, refer to:
8. Change the setting to the desired entry. Common settings for Android API level 23 are listed in the table below.
9. When the settings are updated, click **Apply**.
10. Click the ✕ in the upper right corner to close the window.

Setting Type	External Link (internet access required)
Global Settings	https://developer.android.com/reference/android/app/admin/DevicePolicyManager#setGlobalSetting
Secure Settings	https://developer.android.com/reference/android/app/admin/DevicePolicyManager#setSecureSetting
Manifest Permission	https://developer.android.com/reference/android/Manifest.permission

Downloading Virtual Workspace Policy

You can download a copy of the policies for the Hypori Halo virtual workspace in the Hypori Halo Admin Console. This can be used by an administrator who prefers using a specific XML editor.

To download the virtual workspace policies:

1. Open the Hypori Halo Admin Console.
2. Click **Users**.
3. Click the **Configuration** tab.
4. Scroll down to the Hypori Device Policies box.
5. If there is more than one policy listed, select the version to be downloaded and click **Edit**.
6. Click the **Download Policy** icon.

7. If you have a popup blocker, you will have to click **Allow Once**.
8. Click **Save** to download the file to the Windows Downloads folder.

Uploading Virtual Workspace Policy

You can upload a copy of the policies for the Hypori Halo virtual workspace in the Hypori Halo Admin Console. This can be used by an administrator who prefers using a specific XML editor or who has a pre-made policy document they wish to implement.

To upload virtual workspace policies:

1. Open the Hypori Halo Admin Console.
2. Click **Users**.
3. Click the **Configuration** tab.
4. Scroll down to the Hypori Device Policies box and click **Edit**.

5. Click the **Upload Policy** icon.

6. If you have a popup blocker, you will have to click **Allow Once**.
7. Click **Browse**.
8. Navigate to the file you wish to upload and click **Open**.
9. Click **Upload**. When the file has completed uploading, close the window.
10. Click **Apply**.

Virtual Workspace Policy Settings

These settings configure and enforce specific virtual workspace policies that are administered via the Hypori Halo Admin Console. These policies are only applied when the virtual workspace boots up. End users cannot modify virtual workspace policies.

Environment

The environment section is filled in by the server

> **Note:**
> This section should not be manually edited.

Applications

The applications section will allow you to manage, configure and control applications. There are further descriptions contained in each sub-section listed below

Application-Restrictions-Set

This section enables an admin to configure properties or settings within a given set of applications.

> **Note:**
> The actual settings are determined by the application.

Disabled-Apps

This section allows the administrator to disable one or more apps that are on the image, without showing the user that the app(s) is(are) disabled

Kiosk

This section enables Kiosk Mode, which is a way to run only a small collection of related applications in the virtual workspace using a single application as the "home" or start app/component. Kiosk mode only allows the packages contained in the list of packages in the kiosk. Android calls these 'LockTaskPackages'. The home-component is the activity of one of the app packages that should be launched when the virtual workspace starts - it is the 'home'.

Note:
Kiosk Mode is not commonly used as it specifically configures the device such that a single application is started and only a limited set of packages can be used.

The home-component must call 'Android.startLockTask()' to start the kiosk.

Settings

The settings section will allow you to manage, configure and control various settings in the virtual workspace.

Commonly Used Policy Entry under Settings: PIN/Password Requirements

A commonly used option that resides under Settings is the ability for the Administrator to enforce certain PIN/Password requirements.

Note:
All the attributes below are optional.

Example: `<password-requirements quality="something" min-length="7" max-failed-attempts="5" min-uppercase="1" min-lowercase="2" min-letters="3" min-numbers="4" min-symbols="5" min-non-letters="6" />`

Note:
"Quality" can utilize following values:

- unspecified
- something
- numeric
- numeric_complex

- alphabetic
- alphanumeric

Admin-Delegates

This section allows applications the explicit permission to implement various administrative functions using the setDelegatedScopes() API. These functions would otherwise be unable to be performed. For example, one can delegate credential/ certificate management to an application package that can manage the keychain. How these apps/packages are configured is dependent upon each individually. However, using application_restrictions as described above would be an excellent way to do it if you wanted to control it all from within this policy file.

Note:
See https://developer.android.com/reference/android/app/admin/DevicePolicyManager for details on the various scopes of administrative rights that can be delegated.

Disable-Camera

This setting allows an admin to disable access to the camera for applications within the virtual workspace (this setting does not impact the client).

Valid selections include: `true` and `false`

Default: `false` (if the policy is not specified in the system settings)

Disable-Keyguard

This setting disables the keyguard - only applies if a PIN/pattern/password has NOT been set.

Valid selections include: `true` and `false`

Default: `false` (if the policy is not specified in the system settings)

Disable-Screenshot

This setting disables/enables screen capture/recording inside the virtual workspace.

Valid selections include: `true` and `false`

Default: `false` (if the policy is not specified in the system settings)

Disable-Status-Bar

This setting will disable/enable the status bar from showing.

> **Note:**
> Disabling the status bar will block notifications and quick settings.

Valid selections include: `true` and `false`

Default: `false` (if the policy is not specified in the system settings)

Lockscreen-Warning

This setting enables the admin to set both a title and a message on the lock screen (PIN, Pattern, password screen)

This setting has two sub-sections:

- lockscreen-warning-title
- lockscreen-warning-message

Permission-Settings Default-Policy

These settings allow the admin to set permission policies for individual packages. If no default permission policy is set, then android default ("prompt") will be used except for those that are explicitly specified. Permission fields can be a constant as defined in Manfiest.permission or can be a string value.

Valid states include: `grant`, `prompt` and `deny`.

Pinned-Location

This setting allows the admin to fix the GPS location to the specified longitude and latitude.

Global-Settings

This section has been mostly deprecated, but you still can set the ADB_ENABLED, USB_MASS_STORAGE_ENABLED, STAY_ON_WHILE_PLUGED_IN and WIFI_DEVICE_OWNER_CONFIGS_LOCKDOWN

Commonly Used Policy Entry under Global Settings: Set NTP Server for Virtual Workspace

If a virtual workspace exists in a locked down environment, it is unable to retrieve time from the default time.android.com. An administrator can designate an internal NTP server for the virtual workspace by setting `<global name="ntp_server" value="time.android.com"/>` within the `<global-settings>` section of the virtual workspace policy.

Note:
The server must be accessible from the virtual workspace networking.

To confirm that setting was applied, ADB to the virtual workspace and run:

```
logcat -b events | grep -i ntp
```

This should show the server used for NTP by the virtual workspace and whether it was successful or not.

Note:
See https://developer.android.com/reference/android/provider/Settings.Global for details on the values that are still available and can be set.

Secure Settings

This section has been mostly deprecated, but you still can set the `default_input_method` (name of input the method) and `skip_first_use_hits` setting values.

Valid selections include: `0` (to show hints) and `1` (to disable hints)

Trust-Duration

This setting controls when the PIN screen is shown to the user. If the value-in-seconds is set to 0, then you will be required to enter your PIN every time you connect. If it is set to -1, you will never have to enter the PIN after the first time after a reboot. If it is set to a number > 0, Android will ask for a PIN no less than every "value-in-seconds" after the last time. As an example, if value-in-seconds is 600, and you disconnect 2 minutes after you enter your pin, then connect back within 8 minutes, you will not have to enter your PIN. If you connect back after 8:01, you will need to re-enter your pin.

User-Restriction-Settings

This section enables an admin to restrict the user from performing designated activities. Examples of this include (but are not limited to): Preventing users from installing apps or installing them from unknown sources, disabling autofill and disabling content capture. Both Android and Hypori define the names used here. You can also use the

name as defined in the Android JavaDoc within UserManager or you can put the actual text value in the name attribute.

Examples:

- DISALLOW_CONFIG_VPN can be utilized to prevent users from creating a VPN within the virtual workspace.
- DISALLOW_MOUNT_PHYSICAL_MEDIA can also be specified as "no_mount_physical_media"
- DISALLOW_PRINTING can also be specified as "no_printing"
- DISALLOW_SET_WALLPAPER can also be specified as "no_set_wallpaper"

For a full list of the available options that can be enabled, see the UserManager page at https://developer.android.com/reference/android/os/UserManager.html and look under Constants header. The valid options will be the strings that begin with DISALLOW_*.

Wallpaper

This setting defines the background that is displayed on your virtual workspace. There are 3 options when specifying your wallpaper selection:

1. Attach the coding of a PNG file
2. Set the resource as a named color:
   Valid selections include: `red`, `blue`, `green`, `black`, `white`, `cyan`, `yellow`, and `magenta`
3. Set the value to be a 6-digit RGB hex value
   Example: `<color value="#dddddd">`

Truststore

This section allows the administrator to add and store CA certificates from trusted sources, which Hypori uses for establishing trust between different servers within an enterprise or intranet.

Using Variables within Virtual Workspace Policies

The Hypori Halo environment has support for using variables within the virtual workspace policies. This feature allows the policies to become a template and therefore be used for multiple users.

There are two sets of variables that can be used when creating virtual workspace policy:

Variables that start with hypori.sys

These variables are pre-defined.

These variables are reserved for Hypori.

(e.g., `hypori.sys.deviceowner`)

Variables that start with hypori.user

These variables are exposed by the LDAP/AD directory.

These variables are strictly controlled by the Authentication Configuration.

These variables need to be a subset of the variables in the QueryAttributes, which are configured by the Administrator.

(e.g., `hypori.user.mail`, `hypori.user.guid`)

Example:

```
        <application-restrictions package="com.android.mail">
               <string key="customerLicense" value="23AF15B8"/>
               <string key="server" value="exchange-01.sample.com"/>
               <integer key="port" value="443"/>
               <boolean key="useSSL" value="true"/>
               <string key="username" value="{{{hypori.user.cn}}}"/>
               <string key="email" value="{{{hypori.user.mail}}}"/>
           </application-restrictions>
```

The example above lists a `hypori.user` variable in both the 6th and 7th lines.

Sample Virtual Workspace Policy

When assembled and viewed, the virtual workspace policy resembles the sample version below:

```
<hypori-configuration>
<hypori-device-policy>


    <environment>
        <device-owner component="hypori"/>
        <guid>b624714a-33f6-103a-99d4-77bd267186ca</guid>
        <subject>Bogus Name</subject>
        <subject-alt-name uid="BName" name="subject@alt.name"/>
    </environment>


    <applications>
```

```
<application-restrictions-set>
    <application-restrictions package="com.android.mail">
        <string key="customerLicense" value="23AF15B8"/>
        <string key="server" value="exchange-01.sample.com"/>
        <integer key="port" value="443"/>
        <boolean key="useSSL" value="true"/>
        <string key="username" value="{{{hypori.user.cn}}}"/>
        <string key="email" value="{{{hypori.user.mail}}}"/>
    </application-restrictions>

    <application-restrictions package="com.hypori.sample">
        <boolean key="a boolean" value="true"/>
        <bundle key="bundle-o-values">
            <boolean key="embedded-bundle-bool" value="false"/>
            <string key="key-in-embedded-bundle" value="key here"/>
        </bundle>
        <bundle-array key="list-o-bundles">
            <value>
                <boolean key="in an array" value="true"/>
                <integer key="how-many" value="2"/>
            </value>
            <value>
                <boolean key="bundle-typing" value="false"/>
                <string key="values" value="can be anything"/>
            </value>
        </bundle-array>
        <integer key="intkey" value="12345"/>
            <string key="string" value="a string"/>
            <string-array key="coins">
                <value>Penny</value>
                <value>Nickel</value>
                <value>Dime</value>
                <value>Quarter</value>
            </string-array>
      </application-restrictions>
  </application-restrictions-set>
```

```
        <disabled-apps>
            <app package="com.android.dialer"/>
         </disabled-apps>

         <kiosk home-component="com.android.contacts/.activities.PeopleActivity">
             <app package="com.android.contacts/.activities.PeopleActivity"/>
         </kiosk>
</applications>

<settings>
    <admin-delegates>
        <delegate-package package="com.acme.sample">
            <scope>DELEGATION_CERT_INSTALL</scope>
            <scope>DELEGATION_ENABLE_SYSTEM_APP</scope>
        </delegate-package>
    </admin-delegates>

    <disable-camera value="false"/>
    <disable-keyguard value="false"/>
    <disable-screen-shot value="false"/>
    <disable-status-bar value="false"/>

    <lockscreen-warning-title message="Restricted System"/>
    <lockscreen-warning-message message="You are connecting to a restricted system ..... "/>

    <permission-settings default-policy="deny">
        <permission-state
            package="com.isec7.android.med"
            permission="android.permission.READ_EXTERNAL_STORAGE"
            state="grant"
            user-controllable="false"
        />
    </permission-settings>

    <pinned-location longitude="19.3910036" latitude="-99.2840409"/>

    <global-settings>
```

```
        <global name="adb_enabled" value="0"/>
    </global-settings>

    <secure-settings>
        <secure name="skip_first_use_hits" value="1"/>
    </secure-settings>

    <trust-duration value-in-seconds="600"/>

    <user-restriction-settings>
        <user-restriction name="DISALLOW_INSTALL_APPS"/>\
        <user-restriction name="DISALLOW_INSTALL_UNKNOWN_SOURCES"/>
    </user-restriction-settings>

    <wallpaper>
         <color value="#dddddd">
    </wallpaper>
</settings>

<truststore>
    <ca>
-----BEGIN CERTIFICATE-----
MIICJDCCAaqgAwIBAgIBDzAKBggqhkjOPQQDAzBbMQswCQYDVQQGEwJVUzEYMBYG
A1UEChMPVS5TLiBHb3Zlcm5tZW50MQwwCgYDVQQLEwNEb0QxDDAKBgNVBAsTA1BL
STEWMBQGA1UEAxMNRG9EIFJvb3QgQ0EgNTAeFw0xNjA2MTQxNzE3MjdaFw00MTA2
MTQxNzE3MjdaMFsxCzAJBgNVBAYTAlVTMRgwFgYDVQQKEw9VLlMuIEdvdmVybml1
bnQxDDAKBgNVBAsTA0RvRDEMMAoGA1UECxMDUEtJMRYwFAYDVQQDEw1Eb0QgUm9v
dCBDQSA1MHYwEAYHKoZIzj0CAQYFK4EEACIDYgAENmLeC07Ax9cpRTp/HJnmKiF2
sQDdjEf/wLG0+s46TlL7p+02LRweHJCNl6orpuLTc3N8XBzQZ/QKKdOQhOtR5fFe
HMDShoTFbdEkSQ7sF4nkaMjeGlwaBtA4GTMpARqBo0IwQDAdBgNVHQ4EFgQUhsAV
Qvtxdtw+LRFbIRBENcrB3BQwDgYDVR0PAQH/BAQDAgEGMA8GA1UdEwEB/wQFMAMB
Af8wCgYIKoZIzj0EAwMDaAAwZQIwQQbk3t5iNJ3fuKoW2W2iOB85IlfJcIQfkw9X
fgUvpUszzRXqV9XSKx+bjXzOarbMAjEAt4HS4TuTzxFk3AsvF9Jt1dgF5FByYmXc
pDzKYaUGmsn77cQwyXuJ4KW+Y1XmnBHj
-----END CERTIFICATE-----
    </ca>
</truststore>
```

```
</hypori-device-policy>

</hypori-configuration>
```

Chapter 7. Optional Configurations

Smart Card Authentication to the Hypori Halo Admin Console

Hypori provides access for administrators to utilize smart cards to access the Hypori Halo Admin Console.

Configuring Admin Console Access from an External Source

In situations where Hypori Halo Admin Console access is needed from an external IP address, the HAProxy, provisioning, and management servers must be modified.

1. SSH to the HAProxy server. Run:

```
ssh <account_name>@<HAProxy_server's_IP_address>
```

2. Elevate privileges. Run:

```
sudo su -
```

3. Reference the following file and identify the name of the `.pem` file that is in `/etc/haproxy/certs/internal`. Run:

```
cat /etc/opt/rh/rh-haproxy18/haproxy/haproxy.cfg
```

4. Locate the file identified in step 3 and create a backup copy of the file.

```
cd /etc/haproxy/certs/internal/

cp  <certname>.pem <certname>.pem.backup
```

5. Move the full chain cert file that you have created to the `/etc/haproxy/certs/internal/` folder.

```
mv <path_to_the_full_chain_cert_file> /etc/haproxy/certs/internal/
```

6. Add the full chain cert to the bottom of the original file. Run:

```
cat <certname>.pem <full_chain_cert>.pem >> <certname>.pem.new
```

7. Delete the original cert and replace it with the new cert. Run:

```
rm -f <certname>.pem

mv <certname>.pem.new <certname>.pem
```

8. Restart the HAProxy service. Run:

```
systemctl restart rh-haproxy18-haproxy.service
```

Enabling Admin Console Access using a Hard Token or Smart Card

1. SSH to the provisioning server. Run:

```
ssh <account_name>@<provisioning_server's_IP_address>
```

2. Elevate privileges. Run:

```
sudo su -
```

3. Create a backup of the original `ca.crt` file. Run:

```
cd /etc/puppet/environments/production/modules/hypori-bincache/files/mgmt/nginx/certs/

cp ca.crt ca.crt.backup
```

4. Copy the new full chain cert to the nginx certs folder. Run:

```
mv

 <path_to_full_chain_cert_file> /

etc/puppet/environments/production/modules/hypori-bincache/files/mgmt/nginx/certs/
```

5. Modify the original file to include the same full chain cert file. Run:

```
cat <full_chain_cert>.pem ca.crt >> ca.crt.new
```

6. Delete the original cert and replace it with the new cert. Run:

```
rm -f ca.crt

mv ca.crt.new ca.crt
```

7. Perform a manual Puppet update on the management server.

    a. SSH to the management server. Run:

    ```
    ssh <account_name>@<targeted_node's_IP_address>
    ```

    b. Elevate privileges. Run:

    ```
    sudo su -
    ```

    c. Instruct the server to conduct a manual Puppet update. Run:

    ```
    puppet agent -tv
    ```

8. Verify the full chain cert was added to the management server after the puppet update. Run:

```
openssl crl2pkcs7 -nocrl -certfile /etc/nginx/certs/ca.crt | openssl pkcs7 -print_certs -noout
```

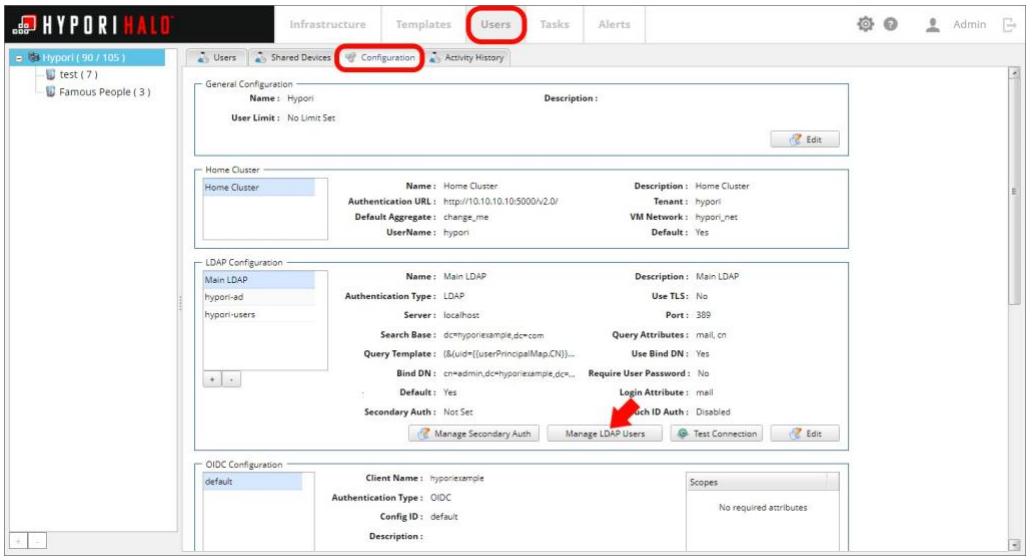
Configuring Smart Card Authentication in the Admin Console

There are situations that require administrators be able to use a smart card or CAC card to access the Hypori Halo Admin Console.

Note:
This feature requires Hypori version 4.9 with the February 2021 patch (or later) installed.

Note:
Prior to completing the steps below, ensure that you have completed adding the appropriate CA chains to the Hypori Halo management server and TLS server, if you require access from an external IP address.

1. Open the Hypori Halo Admin Console.
2. Add the Organizational Unit (OU) that will be used in new Authentication Configuration.
    a. Click **Users**.
    b. Click the **Configuration** tab.
    c. Click **Manage LDAP Users**.



    d. Click **Add User to LDAP**.
    e. Fill out the 'Add New User to Main LDAP' pop-up with the following information:

    Parent DN: `ou=scadmin,dc=(your domain,dc=(your domain)`

First Name: Provide the user's first name.

Last Name: Provide the user's last name.

CN: Configure your CN to equal your user's SAN.

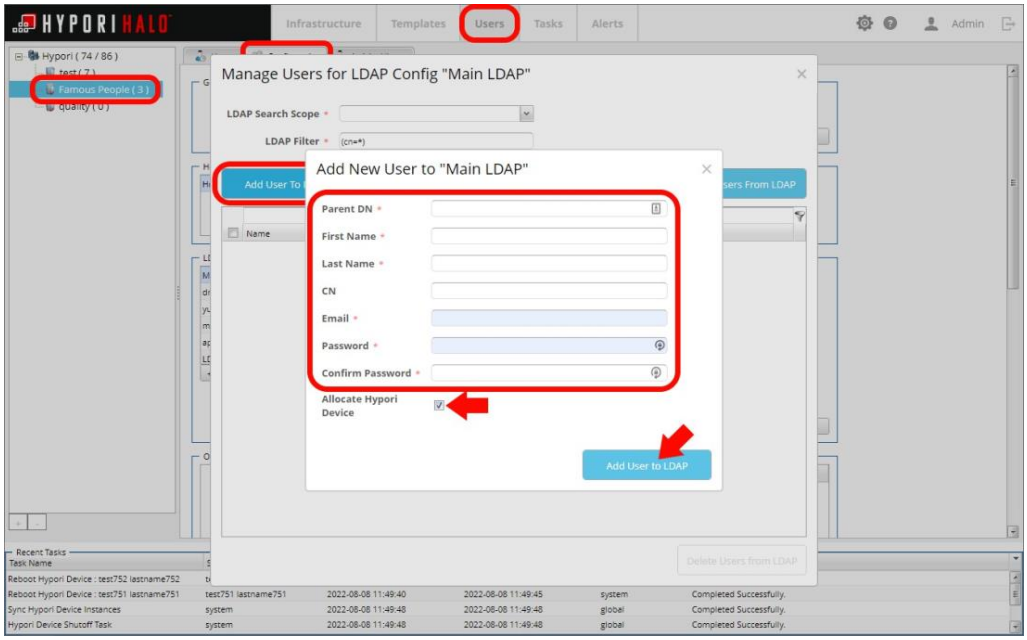
Email: Provide the same SAN email address that matches the CN.

Password: Provide a password for the user.

Confirm Password: Repeat the password entered above.

f. Uncheck the **Allocate Hypori Device** box.

g. Click **Add User to LDAP**.

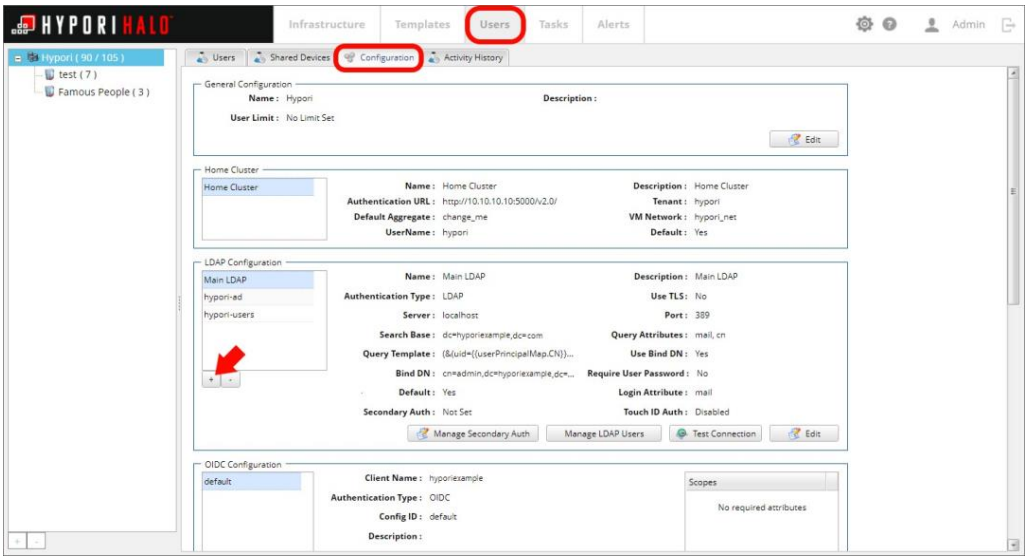


3. Add a new Authentication Configuration.

a. Click **Users**.

b. Click the **Configuration** tab.

c. Under LDAP Configuration, click the **add** (**+**) icon.



d. Fill out the "Add New LDAP Configuration" box with the following information:

   Name: SC Admins

   Server: localhost

   Port: 389

   Search Base: `ou=scadmin,dc=(your domain,dc=(your domain)`

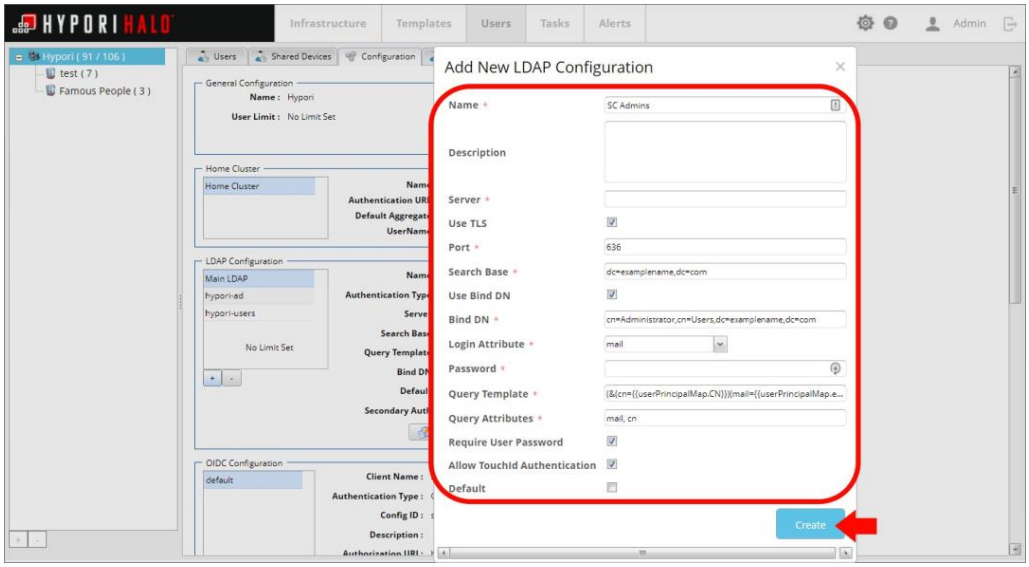
   Bind DN: `ou=admin,dc=(your domain,dc=(your domain)`

   Password: password retrieved from management server (`/etc/openldap/slapd.conf`)

   Query Template: `(cn={{userPrincipalMap.UPNAltName}})`

e. Deselect the bottom 3 boxes.

f. Click **Create**.

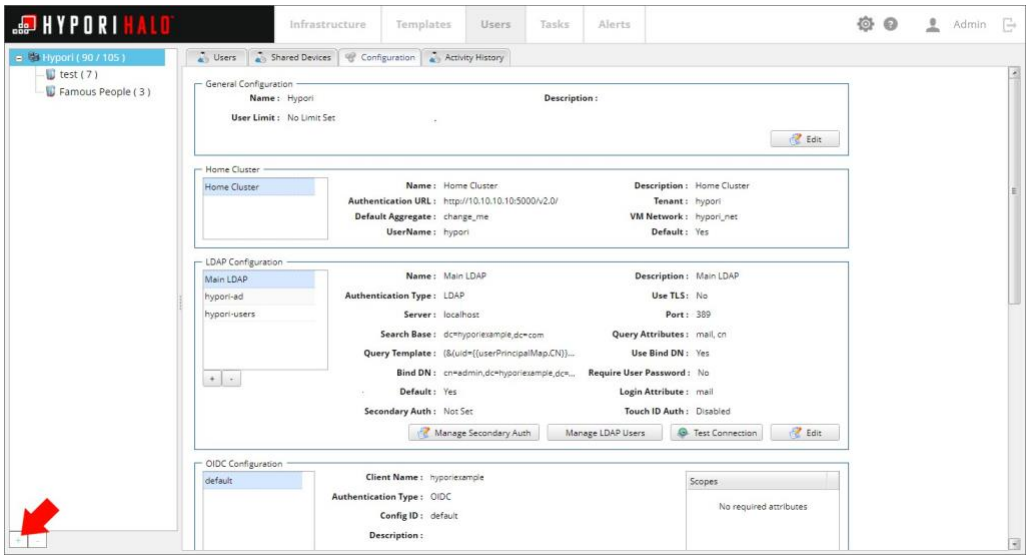


4. Add a new 'SC Admins' domain.

a. Click **Users**.

b. Click the **Configuration** tab.

c. Click the **add** (**+**) icon in the bottom left corner of the navigation pane.



d. Fill out the General Configuration box with the following information:

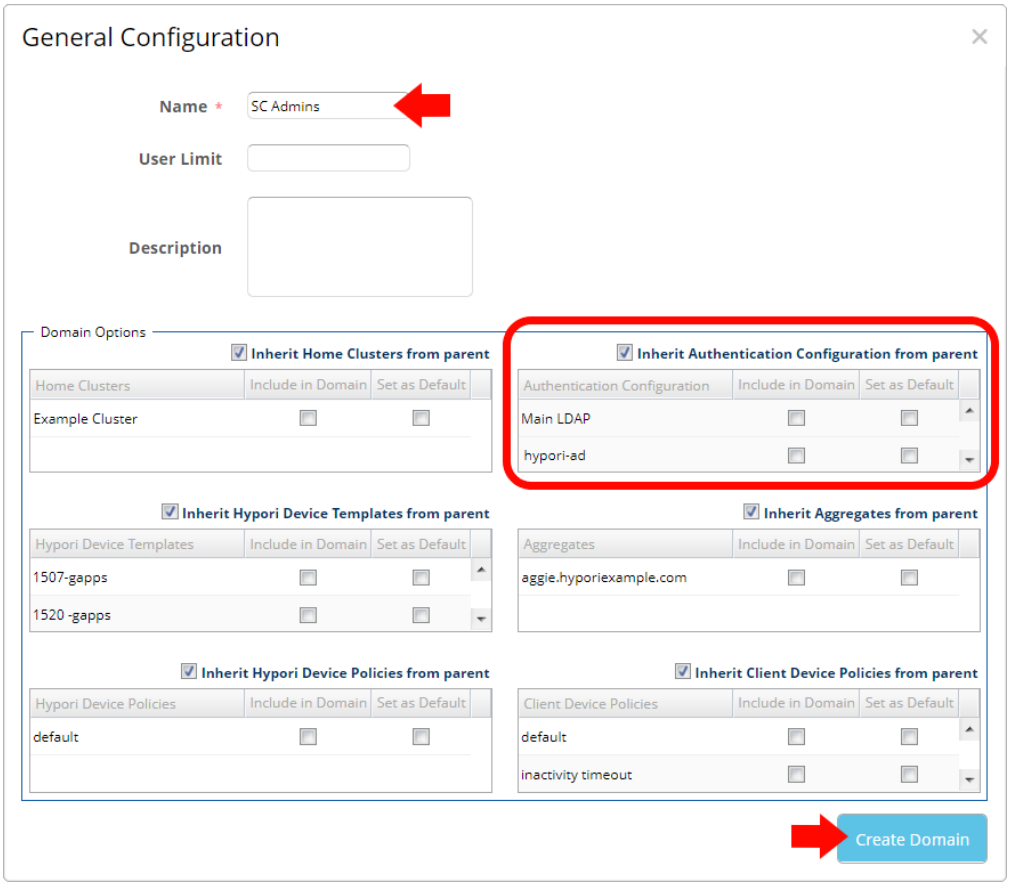
Name: SC Admins

e. Uncheck the **Inherit Authentication Configuration from parent** box.

f. Under Authentication Configuration, scroll down and select the configuration created in the previous section.

g. Check the **Include in Domain** and **Set as Default** boxes next to your configuration.

h. Click **Create Domain**.



5. Add new admin(s) to the newly created domain:

a. Click **Users**.

b. Click the **Configuration** tab.

c. Click the newly created **SC Admin** domain from the navigation pane.

d. Click **Add**.

e. Fill out the General Configuration box with the following attributes:

Authentication Configuration: Use the drop-down to select 'entry'.

LDAP Search Scope: Use the drop-down to select 'entry'.

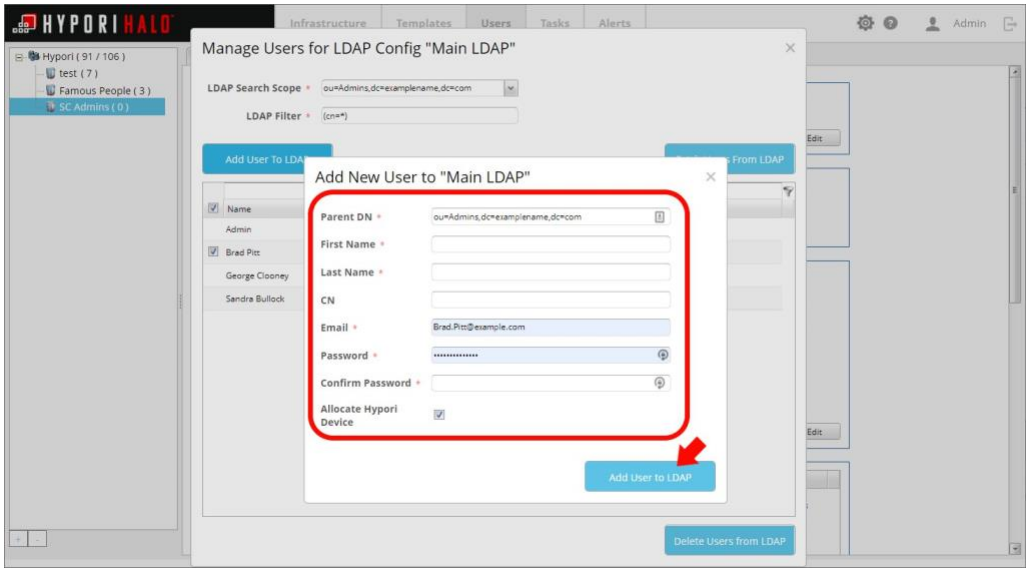
User role: Check the Administrator box

f. Uncheck all boxes.

g. Accept the default choices for all other items.

a. Click **Fetch Users From LDAP**.

b. Click the check box next to your desired user, then click **Add User** in bottom right corner. Confirm your user add when prompted.



6. Verify your ability to log in using your smart card.

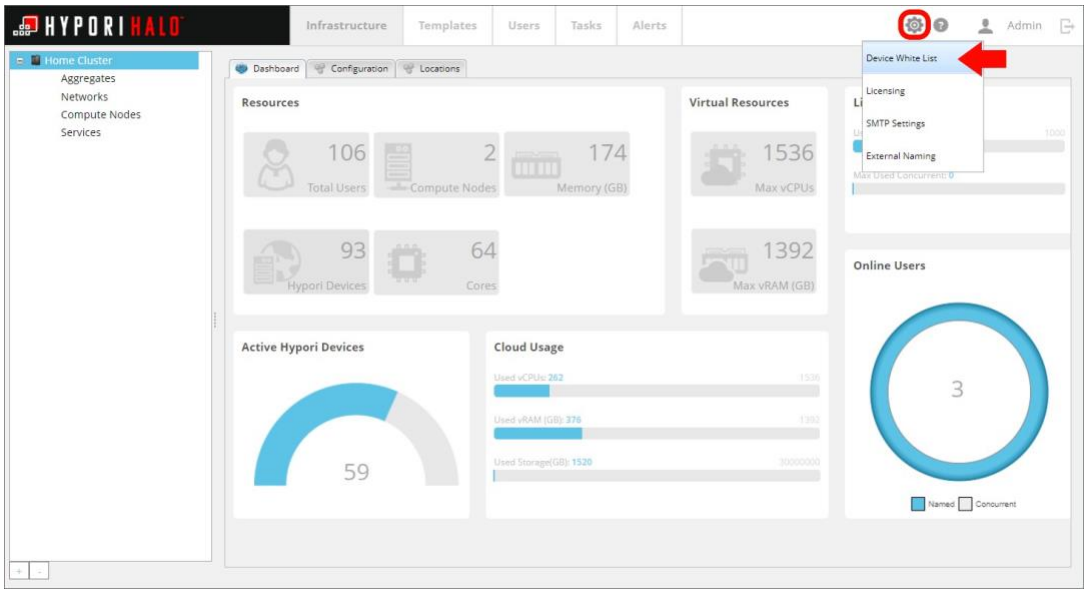
Using a Device Whitelist

Using a device whitelist allows the Hypori Halo Administrator to grant users permission to access their virtual workspace using only the models of smartphones/tablets and operating system versions the administrator has specified.

Note:
This is specifically useful for organizations that are buying specific models (e.g., Galaxy S22) of smartphones/tablets and then issuing them to their employees or ensuring that OS upgrades occur in a timely manner.

1. Open the Hypori Halo Admin Console.
2. In the menu, click the **Settings** icon.

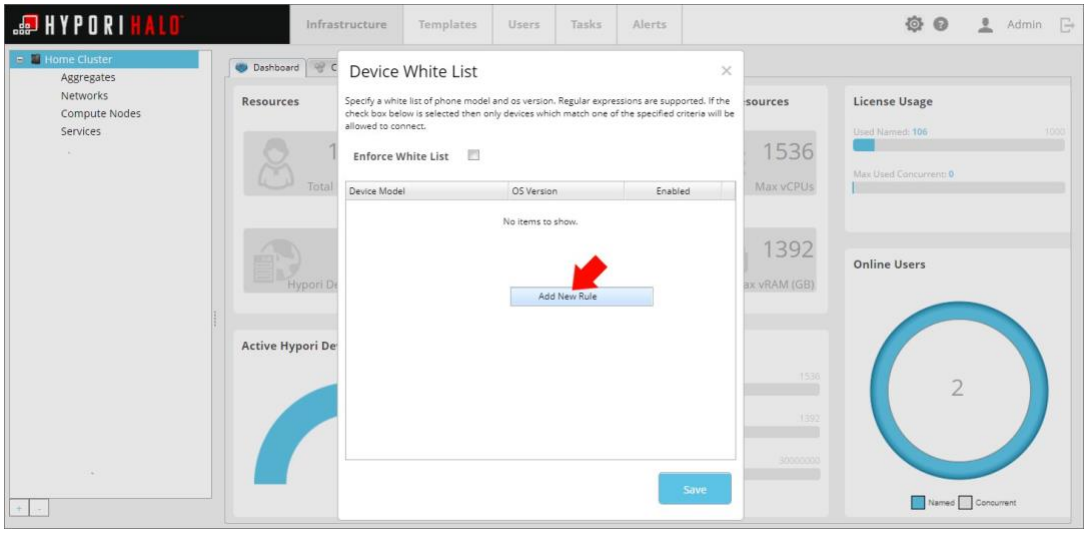
3. Click **Device White List**.



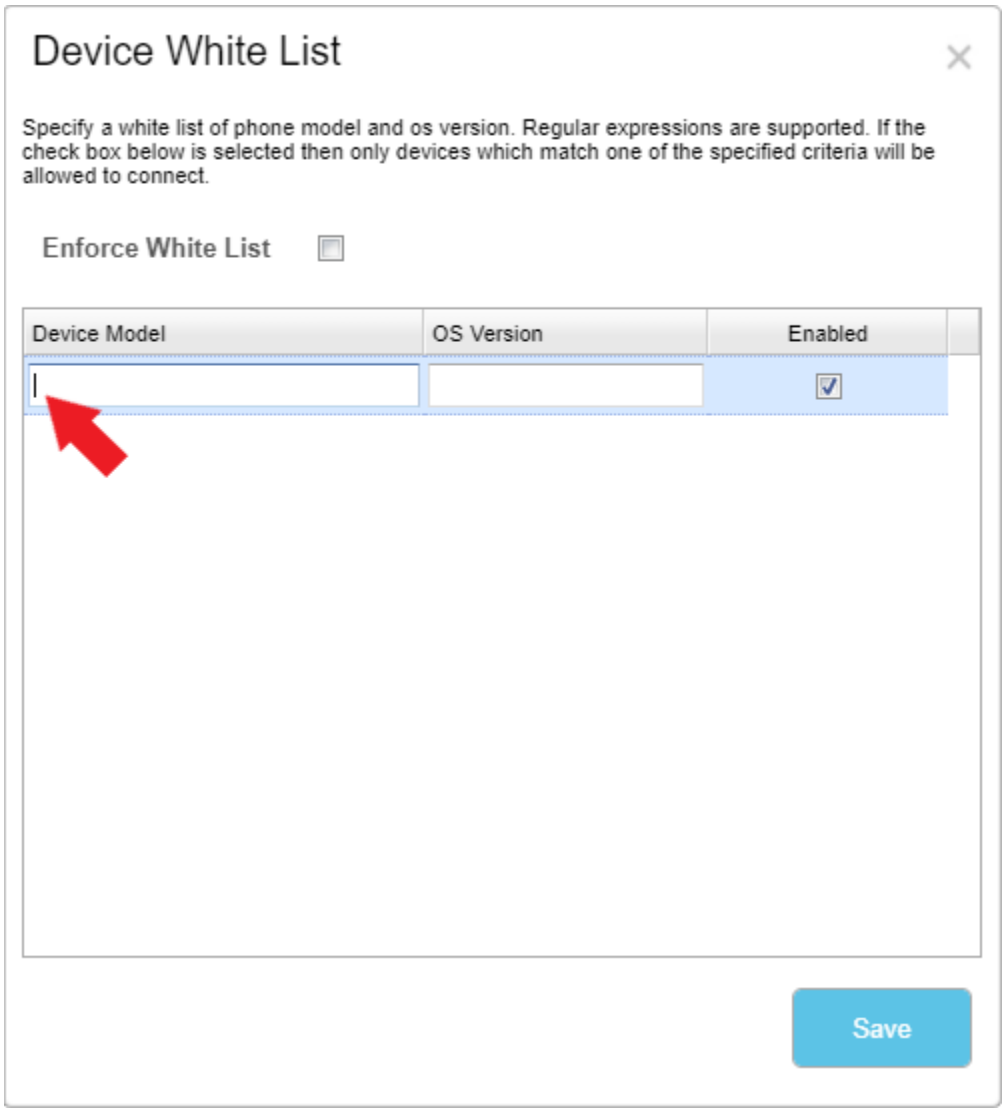
4. Right-click the mouse anywhere in the box to bring up the Add New Rule link.

Note:

Mac users will press <CTRL> when clicking on the mouse button.



5. Click **Add New Rule** to make a new line appear.
6. Click the new line under Device Model to prompt for a cursor.



7. Enter the Device Model identification and OS Version information for the device type being whitelisted in the indicated fields, then press <Enter>.

Tip:
The Enabled box will be automatically checked. Uncheck the box if you do not want that device model currently enabled.

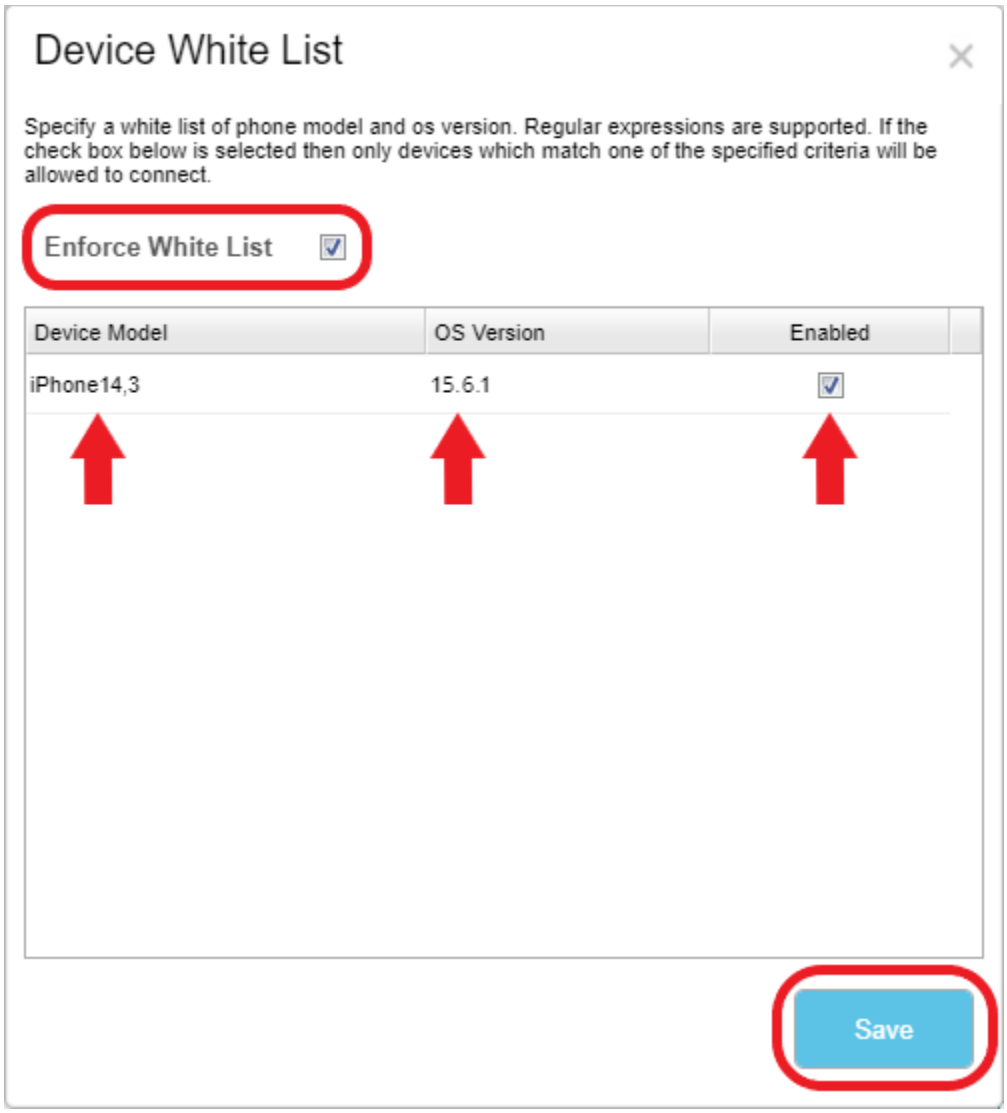
Important:
To determine the correct information used to populate the Device Model field, refer to the following URLs:

- **Android:** https://tech-latest.com/android-device-codenames/
- **iOS:** https://github.com/pluwen/apple-device-model-list

Note:

The OS Version is the numerical version ID of the OS being whitelisted.

8. When all the devices being whitelisted have been added, verify the **Enforce White List** box is checked to activate the whitelist.



9. Click **Save**.

Disabling Website Provisioning

There are situations that require users be denied the option to provision their devices with a QR code on the User Onboarding webpage.

To disable website provisioning of Hypori Halo devices:

1. SSH to the management server. Run:

```
ssh <account_name>@<management_server's_IP_address>
```

2. Elevate privileges. Run:

```
sudo su -
```

3. Back up the existing user provisioning webpage. Run:

```
mv /usr/share/nginx/html/userprov/index.html
/usr/share/nginx/html/userprov/index.html.backup
```

4. Modify the permission of the file to prevent users from accessing it. Run:

```
chmod 600 /usr/share/nginx/html/userprov/index.html.backup
```

5. Create a new, empty index.html which will load a blank page for end-users, should they access the userprov site. Run:

```
touch /usr/share/nginx/html/userprov/index.html
```

6. SSH to the provisioning server. Run:

```
ssh <account_name>@<provisioning_server's_IP_address>
```

7. Elevate privileges. Run:

```
sudo su -
```

8. Modify the `services.yml.erb` file to disable self-provisioning. Run:

```
vi /usr/share/openstack-puppet/modules/profile/templates/mgmt/services.yml.erb
```

9. Locate the `allowSelfProvisioning` parameter and using a text editor, change its the value to `false`.

> **Note:**
> This prevents anyone from invoking rest APIs to get an OTP using port 9443.

Disabling the Ability to Sideload Apps

Administrators can use virtual workspace policy to manage the ability of their users to install apps using the sideload method. For older Android 9 virtual workspaces, the mechanism is via a user restriction in the Device Policy configuration.

Policy settings for Android 9 Virtual Workspaces

- Android 9 ships with all current Hypori Halo versions.
- Android 9 virtual workspaces run the Android P operating system
- To disable the ability to sideload apps, insert the following code into the Device Policy configuration:

```
    <user-restriction-settings>
        <user-restriction name="no_install_unknown_sources"/>

        <!--
            The following provide greater control over installing apps. These will disable all
installs/updates,
            disable the ability to disable/enable apps, and disable app removals/uninstalls.

        <user-restriction name="DISALLOW_UNINSTALL_APPS"/>
        <user-restriction name="DISALLOW_APPS_CONTROL"/>
        <user-restriction name="DISALLOW_INSTALL_APPS"/>
        <user-restriction name="DISALLOW_INSTALL_UNKNOWN_SOURCES"/>
        -->
    </user-restriction-settings>
```

Client Certificate Provisioning Using an Offline Registration Authority (RA)

Hypori Halo makes use of client certificates as the first layer of security when Hypori Halo clients connect to their backend services (virtual workspaces, policies, notifications etc.). Hypori Halo has previously supported issuance of the client certificates from three sources:

- Internal Hypori managed CA
- NDES compliant external CA
- ADCS compliant external CA

An additional method has been added to issue User Certificates, enabling administrators to enable the User Certificates to be signed in an offline fashion. This method allows for environments whose CA/RA systems are not connected by API or are air-gapped for security reasons.

The Offline RA process still retains the ability to auto-provision user certificates onto the Hypori Halo Client onboard end users using manual One-Time Password (OTP) entry or by scanning a QR Code. In addition, there is support on the client to manually renew a certificate using the OTP.

Note:
Before configuring the Hypori Halo Admin Console, Offline RA must be enabled on the management server. To perform that step, the appropriate entries must be inserted into the `hostinfo.yaml` file and then Puppet must be run on the management server. See *"Management Server Parameters"* in the *Hypori Halo Server Installation Guide* for more information and then the `step2` script must be run again on the provisioning server.

Once Offline RA has been enabled on the management server, certificate issuance consists of nine parts:

1. Modify the Hypori Halo servers to support Full Chain client certificates.
2. Update the SPICE bundle.
3. Update the management server values to support NSS.
4. Create a new Authentication Configuration.
5. Generate a CSR for the user.
6. Use the CSR that was generated to create a signed certificate by the CA.
7. Import the signed certificate into Hypori.
8. Generate an OTP for the user.
9. Supply the OTP to the user (via email, phone call, etc.).

The end user can then employ the OTP to claim the certificate.

Modifying Hypori Halo Servers to Support Full Chain Client Certs

The HAProxy, provisioning, and management servers must be modified to support the externally generated `ca.pem` and full chain certs.

1. SSH to the HAProxy server. Run:

```
ssh <account_name>@<HAProxy_server's_IP_address>
```

2. Elevate privileges. Run:

```
sudo su -
```

3. Determine the location of the CA file being used by the HAProxy. Run:

```
# grep bind <haproxy cfg file> | awk ' { print $8 " " $9 } '
```

The output should resemble:

```
[root@tlsproxy ~]# grep bind /etc/opt/rh/rh-haproxy18/haproxy/haproxy.cfg | awk
' { print $8 " " $9 }'


ca-file /etc/haproxy/certs/internal/ca.pem
ca-file /etc/haproxy/certs/internal/ca.pem
ca-file /etc/haproxy/certs/internal/ca.pem
ca-file /etc/haproxy/certs/internal/ca.pem

[root@tlsproxy ~]#
```

4. Locate the file identified in step 3 and create a backup copy of the file.

```
cd /etc/haproxy/certs/internal/

cp <certname>.pem <certname>.pem.backup
```

5. Install new ca file by using one of the following methods:
   a. Move a full chain cert file or a complete ca file including intermediate and root certs to the `/etc/haproxy/certs/internal/` folder. Run:

```
# mv <path_to_the_cert_file> /etc/haproxy/certs/internal/
```

   - or -

   b. Append the full chain cert to the bottom of the original file. Run:

```
#cat <certname>.pem.backup <full_chain_cert>.pem >> <certname>.pem.new
```

6. Verify the permissions and context on the certificate file. Run:

```
# ls -lZ /etc/haproxy/certs/internal/<certname>.pem
```

The output should resemble:

```
[root@tlsproxy internal]# ls -lZ /etc/haproxy/certs/internal/ca.pem
-rw-------. root root system_u:object_r:etc_t:s0       /etc/haproxy/certs/internal/ca.pem
[root@tlsproxy internal]#
```

Note:

If the permissions or context are not correct use the following to update:

```
chcon system_u:object_r:etc_t:s0 /etc/haproxy/internal/<certname>.pem

chmod 600 /etc/haproxy/internal/<certname>.pem

chown root:root /etc/haproxy/internal/<certname>.pem
```

7. Restart the HAProxy service. Run:

```
systemctl restart rh-haproxy18-haproxy.service
```

Updating the Spice Certificate Bundle

Note:
This section should only be performed by a Hypori Halo integrator.

To update the Spice certificate bundle, perform these steps:

1. Log into the provisioning server as the root user. Run:

```
ssh <account_name>@<provisioning_server's_IP_address>
```

2. Elevate privileges. Run:

```
sudo su -
```

3. Unzip the `spice_certs.tgz` file. Run:

```
# cd /etc/puppet/environments/production/modules/hypori-bincache/files/

# tar xvf spice_certs.tgz
```

4. Create a new client CA file and populate the contents of the file with the contents of the `ca.pem` file along with the intermediate certs, followed by the root certificate.

```
# cd 3.0

# cat ca.pem <intermediate cert> <root_cert> >> client-ca-cert.pem
```

5. Validate the certificate. Run:

```
# openssl crl2pkcs7 -nocrl -certfile client-ca-cert.pem | openssl pkcs7 -print_certs -noout
```

6. Verify the permission / context of the certificate file. Run:

```
# ls -lZ
```

The output should resemble:

```
[root@provo]# ls -lZ
/etc/puppet/environments/production/modules/hypori-bincache/files/3.0
[root@provo]# ls -lZ
-rw-r--r--. root root unconfined_u:object_r:puppet_etc_t:s0 auth-cert.pem
-rw-r--r--. root root unconfined_u:object_r:puppet_etc_t:s0 ca-cert.pem
-rw-r--r--. root root unconfined_u:object_r:puppet_etc_t:s0 client-ca-cert.pem
-rw-r--r--. root root unconfined_u:object_r:puppet_etc_t:s0 server-cert.pem
-rw-r--r--. root root unconfined_u:object_r:puppet_etc_t:s0 server-key.pem
[root@provo]#
```

If permission / context does not match the image above, run the following commands:

```
# chcon unconfined_u:object_r:puppet_etc_t:s0 client-ca-cert.pem

# chmod 644 client-ca-cert.pem

# chown root:root client-ca-cert.pem
```

7. Re-Zip the spice folder. Run:

```
# cd ..

# pwd
```

Verify the output is: `/etc/puppet/environments/production/modules/hypori-bincache/files`, then run:

```
# cp spice_certs.tgz spice_certs.tgz.old

# tar czvf spice_certs.tgz 3.0
```

8. Verify and correct the permissions / context of the `spice_certs.tgz` file. Run:

```
# ls -lZ spice_certs.tgz
```

The output should look exactly like:

If the output does not match the image above, run:

```
# chcon unconfined_u:object_r:puppet_etc_t:s0 spice_certs.tgz

# chmod 644 spice_certs.tgz

# chown root:root spice_certs.tgz
```

9. Pull a list of the provisioned nodes:

```
hypori-admin --pass <password> list
```

10. Run a manual puppet update on each compute node.

> **Note:**
> This action will cause the compute nodes to fetch the new spice folder.

a. SSH to the targeted compute node. Run:

```
ssh <account_name>@<compute_node's_IP_address>
```

b. Elevate privileges. Run:

```
sudo su -
```

c. Instruct the compute node to perform a manual Puppet update. Run:

```
puppet agent -tv
```

d. Repeat step 10 on every compute node until they have all been successfully synchronized with the provisioning server.

11. Connect to the Hypori Halo Admin Console.
12. Stop all virtual workspaces after completing the certificate updates.
13. Start all virtual workspaces.

Updating Management Server Values to Support Network Security Services (NSS)

1. SSH to the provisioning server. Run:

```
ssh <account_name>@<provisioning_server's_IP_address>
```

2. Elevate privileges. Run:

```
sudo su -
```

3. Edit the `hostinfo.yaml` file using the text editor. Run:

```
vi /root/hypori/hostinfo.yaml
```

4. Add the following two values to the management server section:

```
profile::mgmt::user_cert_ca_type: NSS

profile::mgmt::user_cert_max_otps: 1
```

5. Run the `step2` script to re-provision the servers. Run:

```
/root/hypori/step2-autoProvision.sh <foreman_admin_password> <root_password_new_hosts>

 [bootloader_password_new_hosts]
```

where:

- *foreman_admin_password* is the password you set when you installed the provisioning server.
- *root_password_new_hosts* is the password that will be used for the `root` user on all newly provisioned hosts.

Creating a New Authentication Configuration

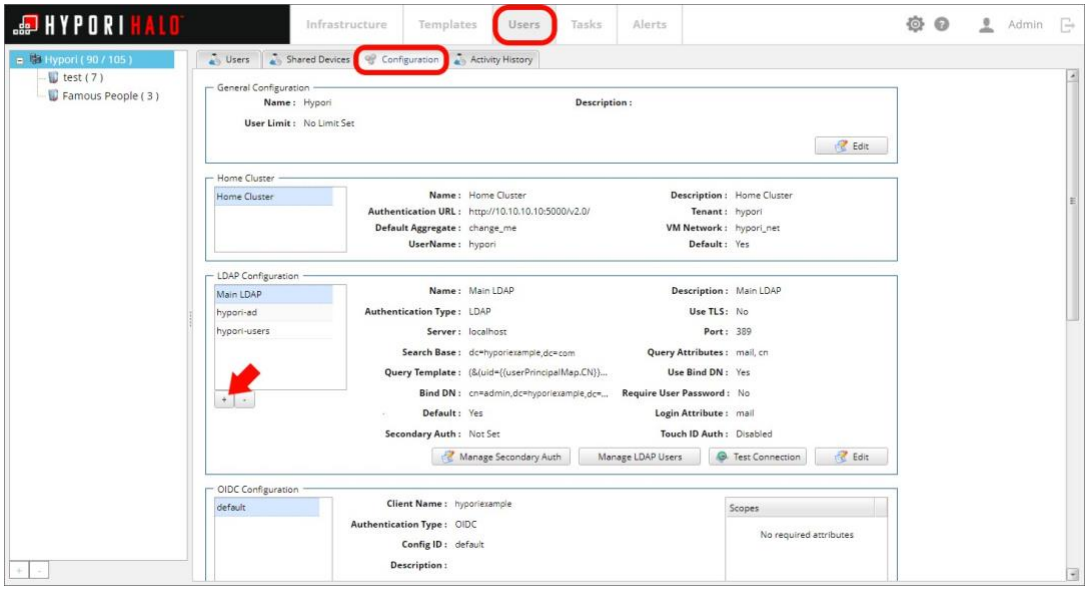
The management server makes use of the client certificate passed along by TLS proxy to extract attributes which can be used to identify the user uniquely. As a frame of reference, the query template in the Hypori Halo Admin Console is, by default: `(&(uid={{userPrincipalMap.CN}})`

`(mail={{userPrincipalMap.emailAddress}}))` which uses the CN and email from the certificate to find the user.

For instructions on creating customized authentication configurations, see Users and their Virtual Workspaces *(on page 57)*.

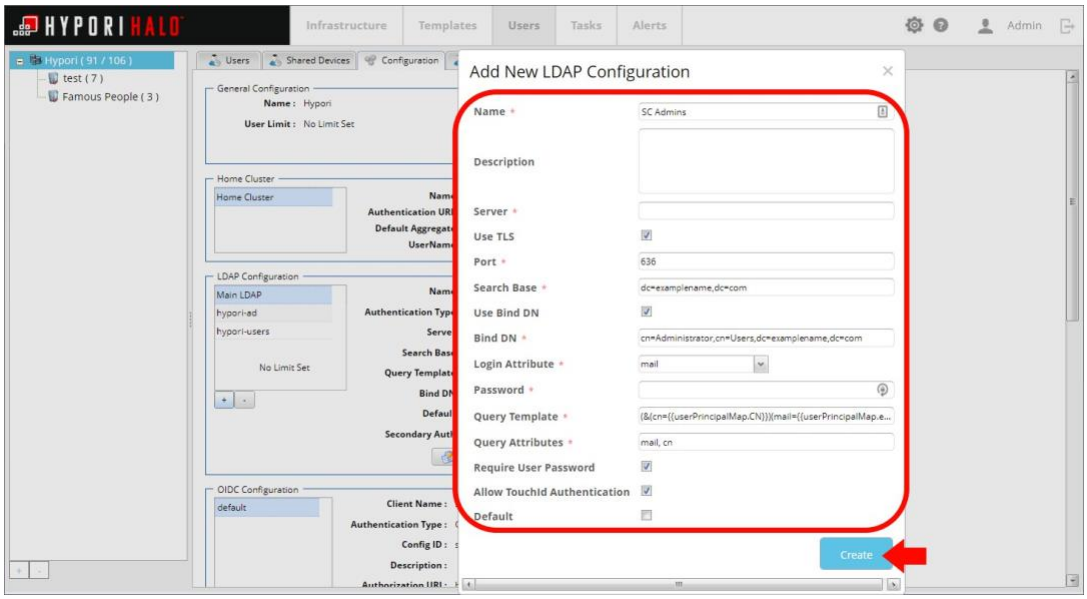
To add a second authentication configuration to the primary LDAP configuration, perform these steps:

1. Log into the Hypori Halo Admin Console.
2. Click **Users**
3. In the navigation pane, select the domain.
4. Click the **Configuration** tab.
5. Under Authentication Configuration, click the **add** (**+**) icon.



6. Match the Add New LDAP Configuration values against the Main LDAP configuration, except:
    - **Name:** (rename)
    - **Server:** localhost
    - **Use TLS:** no
    - **Port:** 389
    - **Search Base: (OPTIONAL)** Set to only search for an OU with Purebred cert users allocated. An example search base for a server with the FQDN `server.domain.com` is `dc=server.domain,dc=com`
    - **Login Attribute:** mail
    - **Password:** This value can be found in the management server's `slapd.conf` file.
        - Open the file on the Management server at `/etc/openldap/slapd.conf`.
        - search for "rootpw"

- **Query Template:** This value should be configured to search only for the UserPrincipalMap of the cert provided. `(&(uid={{userPrincipalMap.CN}}))`
- **Query Attributes:** mail, cn
- **Require User Password:** no
- **Allow TouchID Authentication:** This can be yes or no.
- **Default:** This can be yes or no.

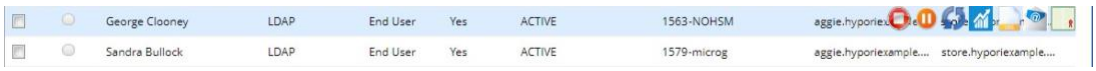


7. Click **Create**.

Generating a Certificate Signing Request (CSR)

To generate an offline certificate, perform these steps:

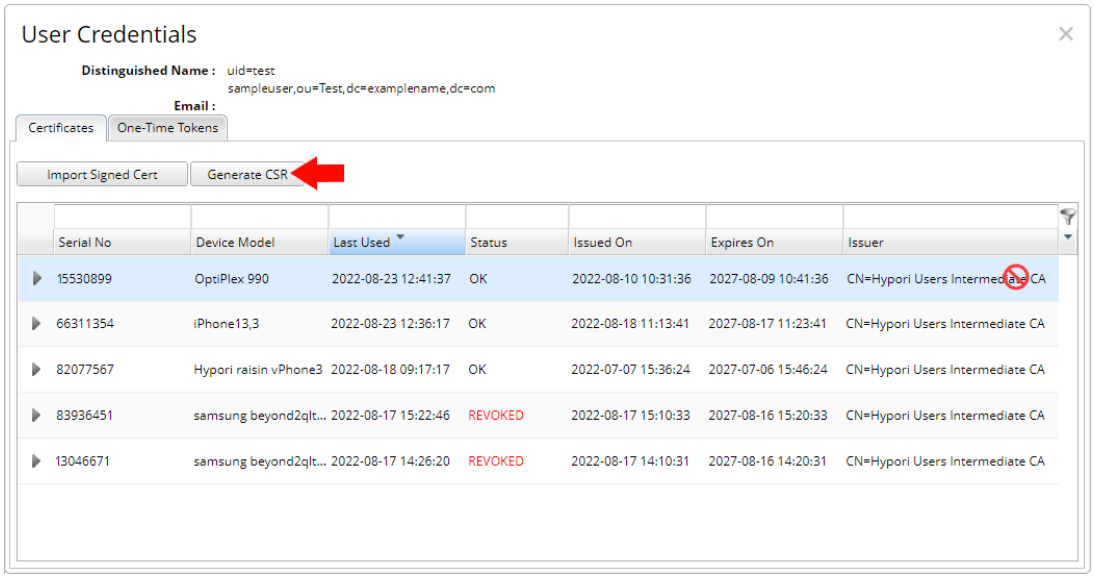
1. Open the Hypori Halo Admin Console.
2. Click **Users**.
3. In the navigation pane, select the user's domain.
4. Click the **Users** tab.
5. Hover your cursor over the user's entry that you are generating the certificate request for, to make the icons appear on the right.



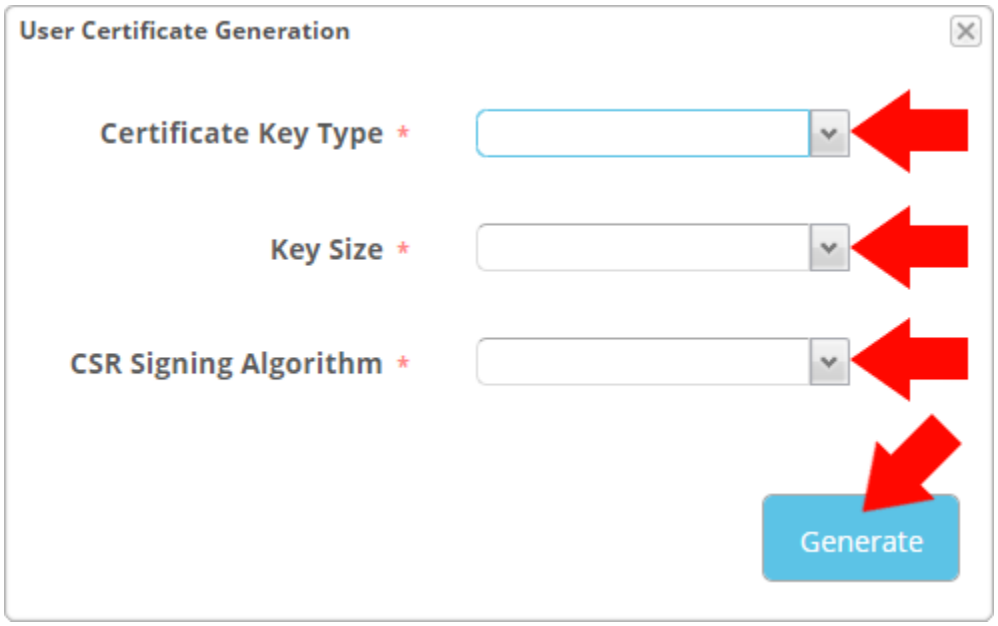
6. Click the **View Credentials** icon.

The User Credentials window will open. It shows the current certificates and OTPs of the selected user.

7. Click the **Generate CSR** button.



8. Use the drop-down to select the Key Type. The remaining field titles will automatically update, based on the certificate type that has been selected.
9. Select the appropriate settings in the remaining drop-down's fields.
10. Click **Generate**.



Use the drop-down menus to select the appropriate selections for your provisioning method.

Note:

The resultant CSR can be used to generate a signed certificate for the user.

Signing the Offline Certificate

Once the CSR has been generated, the RA uses it to generate a signed certificate for the user. You may utilize the tools and/or processes available to your organization. Once you have the user's signed certificate, you can proceed to importing the certificate.

Note:
The customer's Signing Root CA should be configured to provide required attributes. For example, under Enhanced Key Usage you may see:

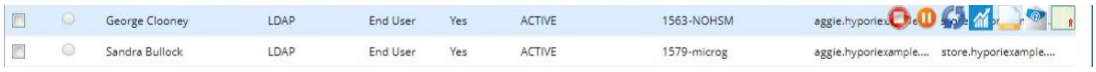
- Server Authentication
- Client Authentication
- Secure Email

Important:
If any of these values are missing, then certificate authentication will fail. Hypori Halo is looking for these values in particular the secure email value to authenticate.

Importing a Signed Certificate

To import a signed certificate, perform these steps:

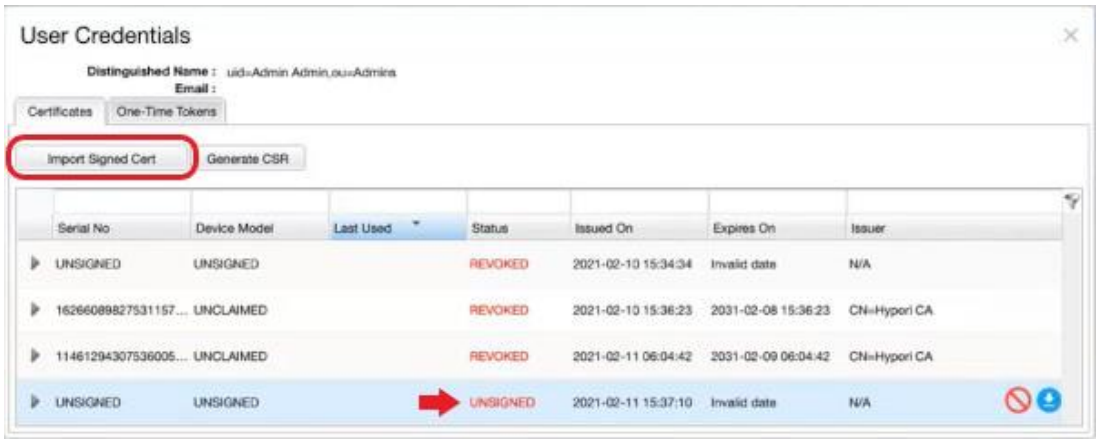
1. Open the Hypori Halo Admin Console.
2. Click **Users**.
3. In the navigation pane, select the user's domain.
4. Click the **Users** tab.
5. Hover over the name of the user (who is receiving the imported certificate) to make the icons appear on the right.



6. Click the **View Credentials** icon on the far-right side.

The User Credentials window will open, listing the current certificates and OTPs of the selected user.

7. Click the **Import Signed Cert** button.

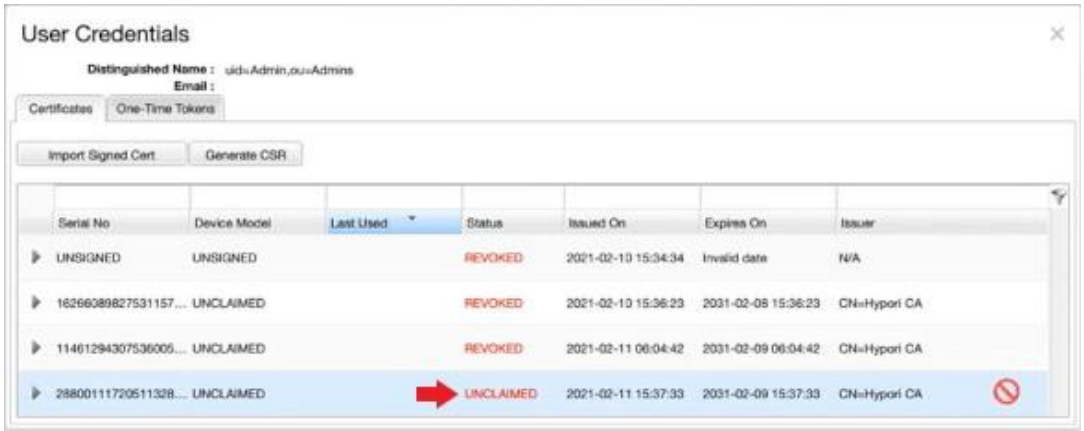


Note:

When the CSR was generated, an unsigned cert was populated on the list as a placeholder.

8. Click **Browse**, navigate to the signed cert file, then click **Open**.
9. Click **Upload**.

The unsigned cert should change to being labeled as an unclaimed cert.



> **Note:**
> Once the user has had their device provisioned, their certificate will be labeled as claimed.

10. Click the **One-Time Token** tab.
11. Click **Generate OTP**.

12. If the admin has the user's device on-hand, they can scan the QR code below to provision the device. If the device is not available, the OTP circled below can be provided to the user to provision using the OTP method. See the *Hypori Halo User Guide* for further instructions on provisioning using an OTP.

Rekeying an Expiring Offline Certificate

To rekey a user's expiring certificate, follow these steps:

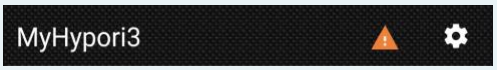
1. Generate a new CSR. For the steps needed to generate a CSR, see Generating a Certificate Signing Request (CSR) *(on page 166)*.
2. Once the CSR has been generated, you may utilize the tools and/or processes available to your organization to generate the certificate.
3. Import the signed certificate and send the user the OTP via email. For the steps required to perform this, refer to Importing a Signed Certificate *(on page 168)*.
4. When the user receives the email, they should:

    a. Open their Hypori Halo app.

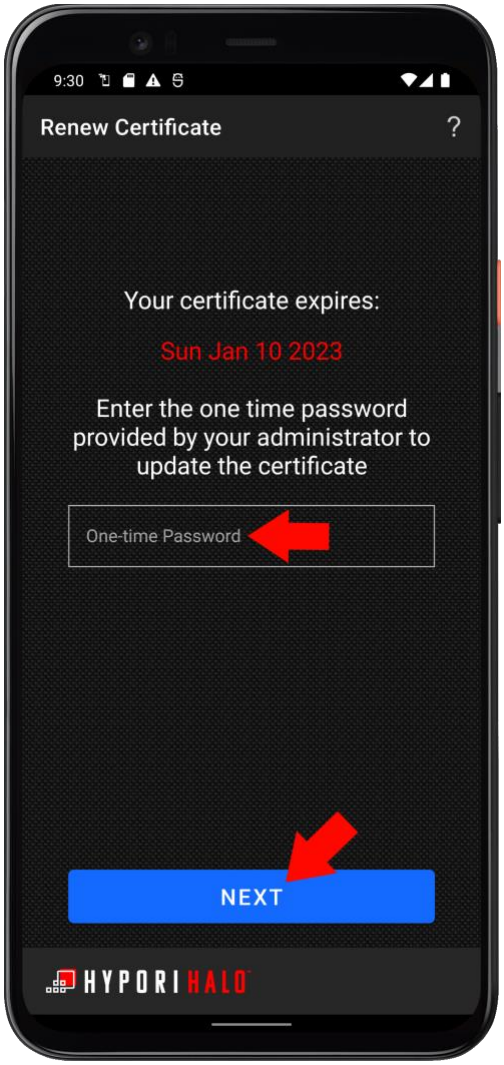
    b. Tap the **Settings** icon next to the account indicating that the certificate is expiring.

Note:

The yellow alert icon will turn into an orange warning icon shortly before the certificate expires.



c. Enter the updated OTP at the indicated field.



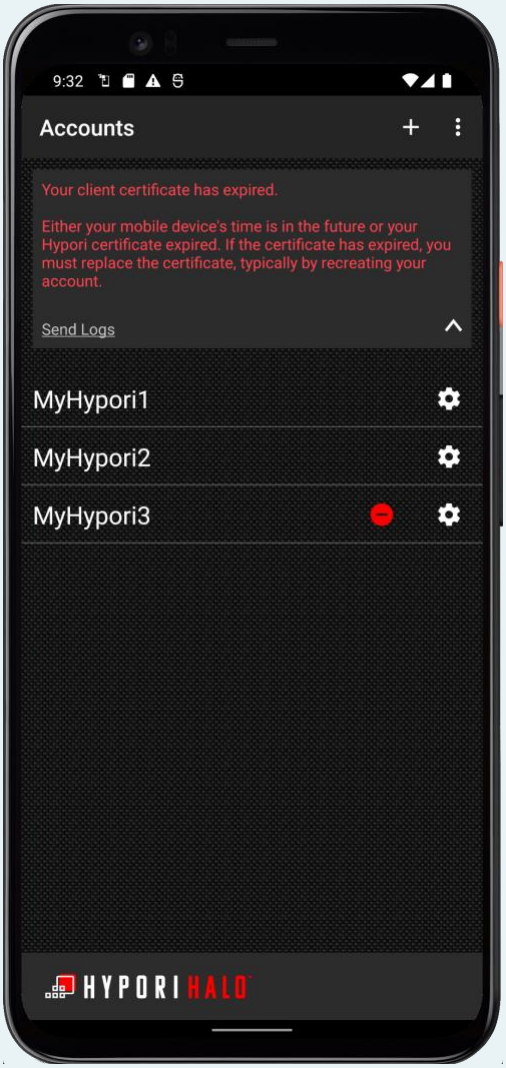
d. Tap **Next**.

The Hypori Halo Client will contact the server in the background, validate the OTP, generate the updated cert, return the cert to the Hypori Halo Client which will then import it.

5. The user can now reconnect to their virtual workspace.

Note:

If the user fails to have their certificate renewed before their client credentials expire, they will need to perform the new user onboarding steps again to create a new login before their access to their virtual workspace can be restored.



Using a Custom One-Time Password (OTP) Email Template

It is possible to customize the content of the email that is sent to end-users with their One-Time Password embedded. To accomplish this, follow these steps.

1. SSH to the management server. Run:

```
ssh <account_name>@<management_server's_IP_address>
```

2. Elevate privileges. Run:

```
sudo su -
```

3. Edit the `otpemailcontent.html` file. Run:

```
vi /usr/share/nginx/html/userprov/otpemailcontent.html
```

4. Use the text editor to perform the template modifications.
5. Save and exit the file.

Appendix A. Troubleshooting

Use the topics in this section to troubleshoot issues that can occur in your Hypori Halo environment.

Viewing Recent Tasks

To view recent tasks performed in the Hypori Halo Admin Console, select the View the Recent Tasks table at the bottom of the Hypori Halo Admin Console. This table shows:

- **Task Name:** The name that identifies the server task.
- **Started By:** The entity that initiated the task. Most tasks are system events.
- **Start Time:** The date and time when the task started.
- **End Time:** The time when the server task ended if it has been terminated.
- **Queue:** The queue associated with the task.
- **Detail:** The status of the task, such as whether it is in progress, has completed successfully, or has produced an error.

Double-click a task to see additional details.

Viewing the Hypori Halo Admin Console Task History

To view the Hypori Halo Admin Console's task history:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Tasks**.
3. Under Task History, scroll through the list of tasks. By default, the Task History table is filtered to show the last 50 tasks that occurred yesterday.
4. To filter the list, select one of the following options in the Fetch Tasks History since list:
    - **Yesterday:** Shows tasks that occurred with a timestamp one day before the current date.
    - **Last Week:** Shows tasks that occurred over the seven-day period from the previous week.
    - **Last Month:** Shows tasks that occurred in the previous calendar month.
    - **Last Year:** Shows tasks that occurred in the previous calendar year.
    - **All:** Shows all logged tasks.
5. To limit the number of records retrieved, select one of the options in the Max Records to Fetch list.

For each task, the Task History table shows:

- **Task Name:** The name of the task.
- **Started By:** The entity that initiated the task. Most tasks in the log are started by the Hypori Halo Admin Console system.
- **Start Time:** The date and time when the task was initiated.
- **End Time:** The date and time when the task completed.
- **Queue:** The queue associated with the task.
- **Detail:** Whether the task completed successfully or failed.

Double-click a task to see additional details.

You can sort the table by column. See Sorting Tables by Column *(on page 177)*.

Viewing Hypori Halo Admin Console Alerts

The Hypori Halo Admin Console uses an alerting system to notify you that system errors have occurred or that the console failed to execute a specific task. The Alerts page provides a list of alerts that can be filtered to show severity and details about the events at different periods of time.

To view the latest list of alerts in the Hypori Halo Admin Console:

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Alerts**.
3. Scroll through the list of alerts. By default, the Alerts table is filtered to show the last 50 alerts that occurred yesterday.
4. To filter the list, select one of the following options in the Fetch Alerts since list:
    - **Yesterday:** Shows alerts that occurred with a timestamp one day before the current date.
    - **Last Week:** Shows alerts that occurred over the seven-day period from the previous week.
    - **Last Month:** Shows alerts that occurred in the previous calendar month.
    - **Last Year:** Shows alerts that occurred in the previous calendar year.
    - **All:** Shows all logged alerts.
5. To limit the number of records retrieved, select one of the options in the Max Records to Fetch list.

For each entry, the Alerts table shows:

- **Category:** A categorical description for the alert.
- **Alert Type Id:** The system type ID number for the alert.
- **Severity:** The severity level for the alert.
- **Detail:** A detailed description of the issue that generated the alert.
- **Type:** The type of event that caused the alert.
- **Job Name:** The system job name associated with the event that caused the alert.
- **Time Stamp:** The date and time that the event that caused the alert was initiated.

Tip:
Double-click an alert to see additional details.

You can sort the table by column. See Sorting Tables by Column *(on page 177)*.

Sorting Tables by Column

To sort a table in the Hypori Halo Admin Console:

1. Open the Hypori Halo Admin Console.
2. Open a page that contains the table.
3. Click on the right side of the column heading and select one of the following options:
    - **Sort Ascending:** Sorts the table in ascending order.
    - **Sort Descending:** Sorts the table in descending order.
    - **Configure Sorting:** Opens the Sort box to provide additional sorting options.
    - **Autofit All Columns:** Resizes all columns to fit the data in each column.
    - **Auto Fit:** Resizes the selected column to fit the data in that column.

If you selected Configure Sorting, you can further refine your sort. In the Sort box do one or more of the following and click **Apply**:

- To add an additional level: Click **Add Level**. In the **Then By** list, select another attribute to use to sort the column. Under **Order**, click a sort order from the list. Click **Apply** to add the secondary sort level.
- To remove a sort level, select the sort level row and click **Delete Level**.
- To copy a sort level to use as a baseline for creating a new level, select the sort row that you want to copy and click **Copy Level**.
- To move a sort attribute up or down in the sorting hierarchy, select the up arrow to give the selected attribute a higher priority. Select the down arrow to reduce its priority.

Using Logcat for Troubleshooting

When an end-user is reporting performance or functionality issues, a common troubleshooting step is to enable Logcat on an end-user's device, then collect the logs that are produced by that end-user device. Follow these steps to enable Logcat on an end-user's device and to then collect the logs from that device.

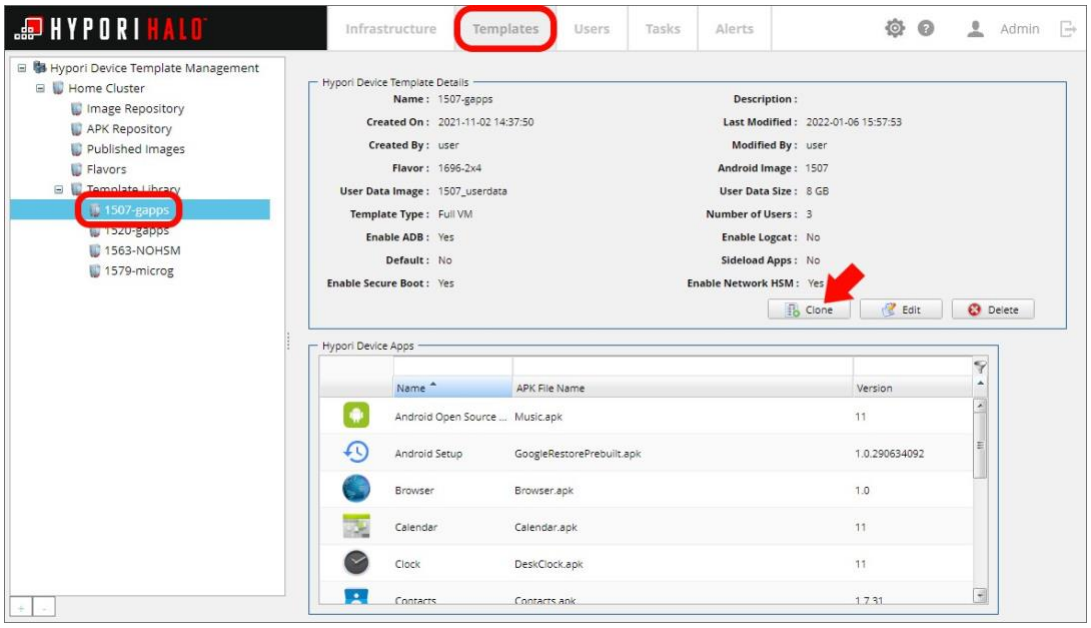
Tip:
Running Logcat is resource-expensive, so it is recommended that it only be enabled on end-user devices that are being debugged. Otherwise, do not enable Logcat.

Enabling Logcat

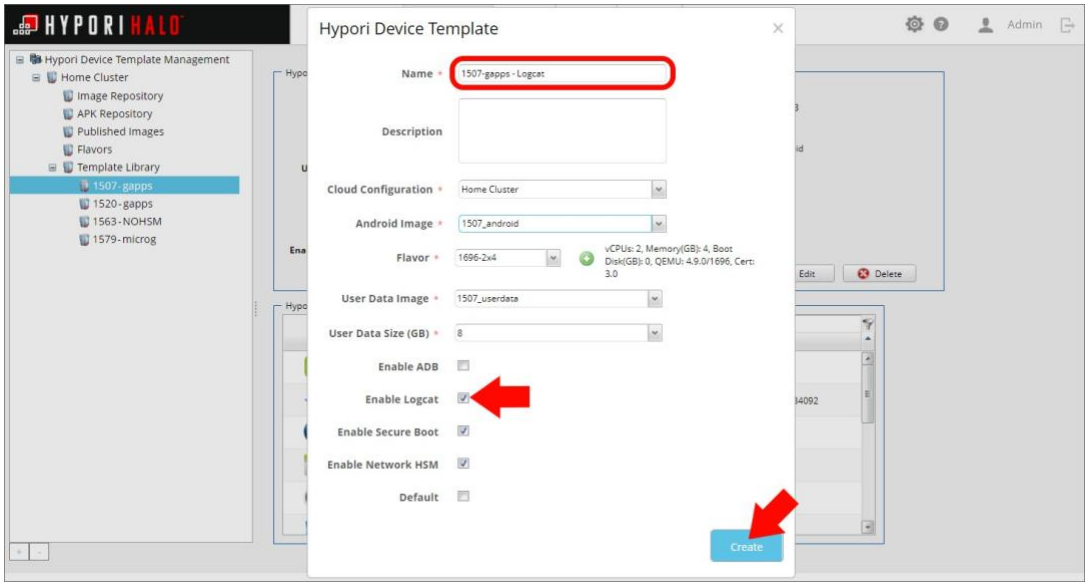
A template that is in use by the end-user's problematic device cannot be changed therefore, it is a best practice to clone the user's template, enable Logcat in the new template, and change their device to use the new template.

To enable Logcat, perform these steps:

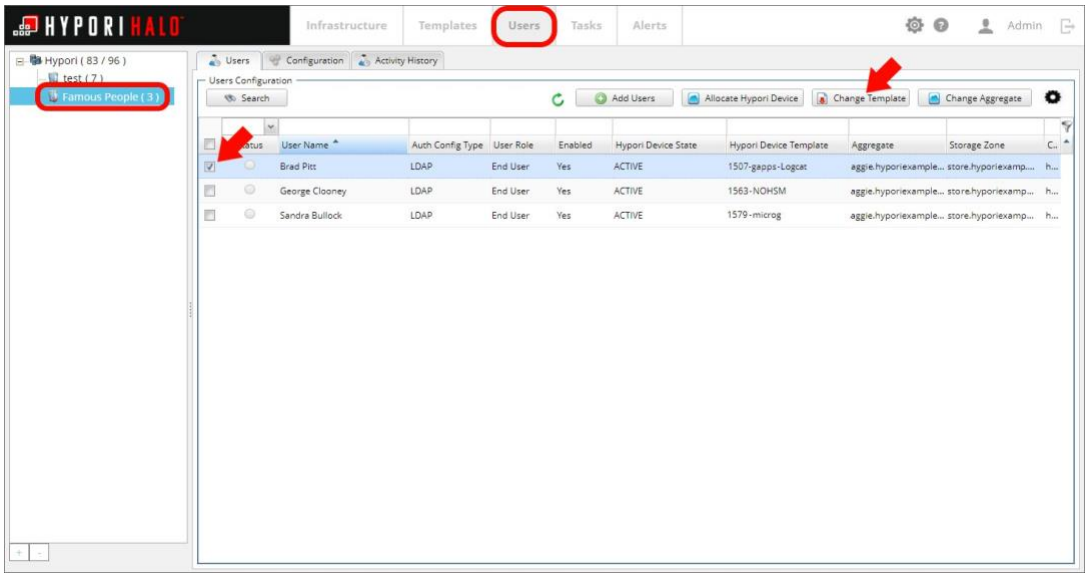
1. Open the Hypori Halo Admin Console.
2. Click **Templates**.
3. In the navigation pane, under the Template Library, select on the template that is currently deployed on the user's virtual workspace.
4. Click **Clone**.



5. Change the name to follow your naming convention.
6. Check the box next to **Enable Logcat**.
7. Click **Create**.



8. In the menu, click **Users**.
9. In the navigation pane, select the user's domain.
10. Find the user and check the box next to their name.
11. Click **Change Template**.

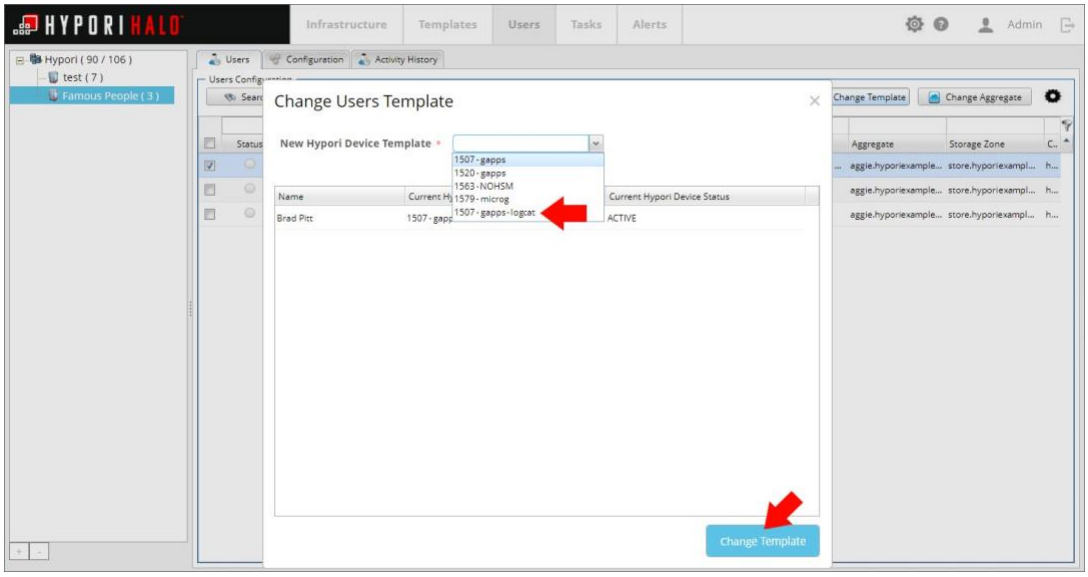


12. Select the newly created template in the drop-down list.

- If the template is not present, edit the domain so it inherits the template.

> **Note:**
> This is located under the Configurations tab for the domain. Click the **Edit** button.

13. Click **Change Template**.



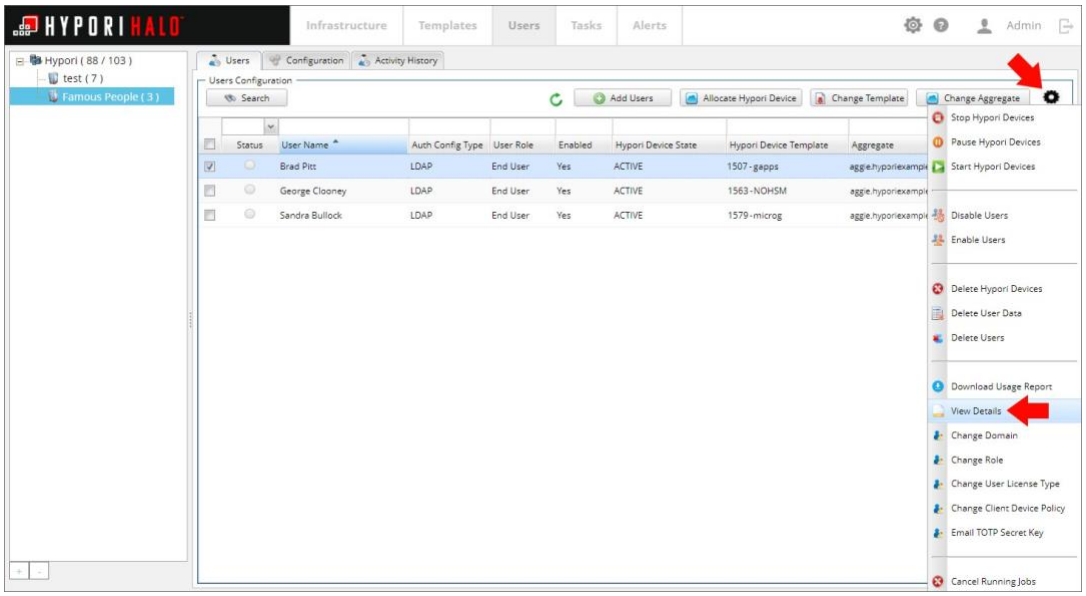
Now that the user has Logcat enabled, contact the user and have them reproduce the issue.

Locating the Logcat Files

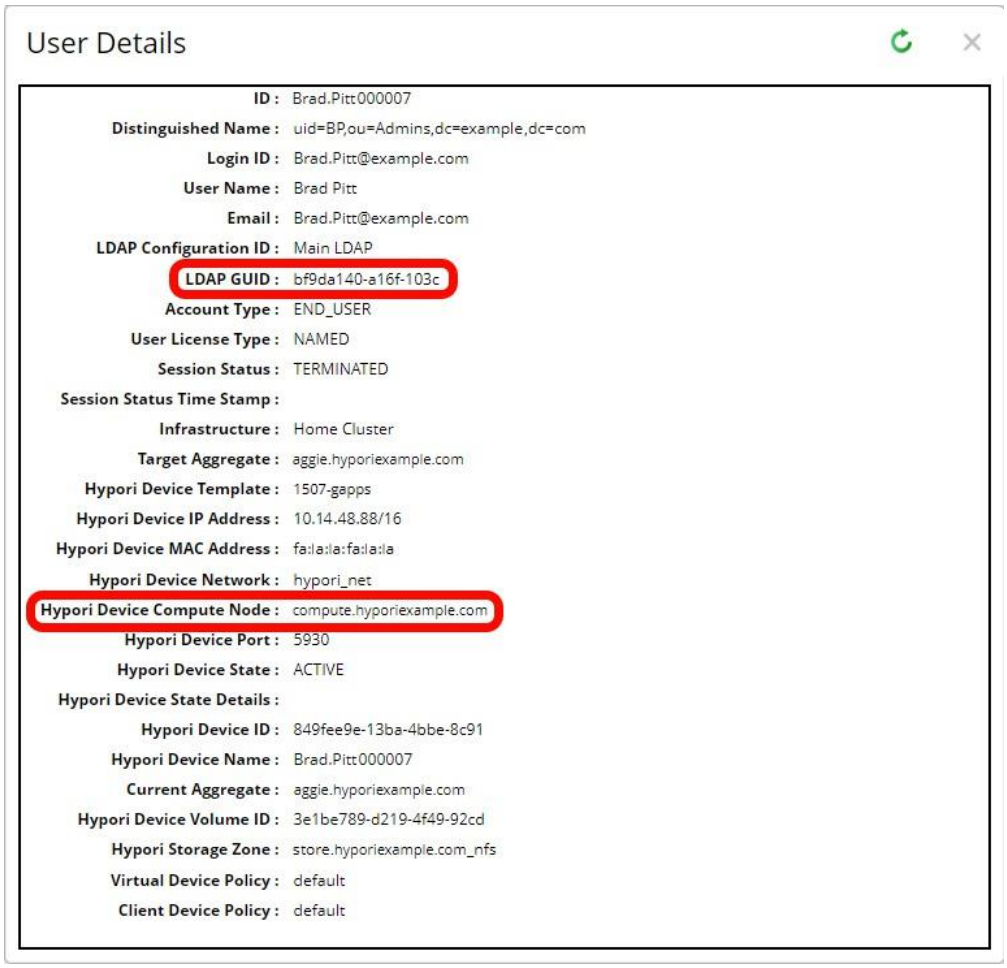
A log has now been created, and it needs to be located. The log is stored within the compute node and is labeled by their Lightweight Directory Access Protocol (LDAP) Globally Unique Identifier (GUID).

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the user's domain.
4. Click the **Users** tab.
5. Locate the user, then check the box by the user's name.
6. In the Users Configuration area, just above the table, click the **More Actions** icon.

7. Click **View Details**.



8. Write down the details for the user's LDAP GUID and Hypori Device Compute Node, you will need this information to complete the next section.



Retrieving the Logcat Files

A log has now been located, and now it needs to be retrieved so it may be examined.

1. Log into the virtual workspace's compute node. Run:

   ```
   ssh <account_name>@<IP_address_of_the_virtual_workspace's_compute_node>
   ```

   Enter the admin's password.
2. Elevate Privileges. Run:

   ```
   sudo su -
   ```
3. Go to the directory that holds the Logcat files. Run:

   ```
   cd /var/log/hypori/logcat
   ```
4. Create a temp directory under the Logcat directory. Run:

   ```
   mkdir temp
   ```
5. Display a list of the files. Run:

   ```
   ls -l
   ```
6. Verify there is an entry that matches the LDAP GUID.

   Note:
   There should be multiple entries that contain that GUID, some files ending with .Z and some without. The files with the .Z extension are the relevant log files. If multiple .Z files exist, the most recently created on will have the most recent logging, but you might need to grab more than one if the relevant logging spans across two or more files.
7. While in the Logcat directory, find the user's LDAP GUID, then move all the files over to the temp directory. Run:

   ```
   mv abc123* temp/
   ```

   Note:
   The wildcard will move the matching LDAP GUID and all the adjoining extensions over to the temp directory
8. Go to the temp directory and unzip all the .Z files.

   ```
   cd temp/

   gunzip *.Z
   ```

9. Go to the QEMU bin directory that holds the Logcat conversion script. Run:

```
cd /opt/hypori/qemu/<Hypori_release_number>/<Hypori_version_number>/bin
```

10. Run the `./logcat` script and output it into a text file. Run:

```
./logcat -vthreadtime /var/log/hypori/logcat/temp/* > /home/hypori/<output_file_name>.txt
```

> **Note:**
> The name of the output file should be relevant to the user.

11. Verify the log was sanitized. Run:

```
vi /home/hypori/<output_file_name>.txt
```

> **Note:**
> The file should now be human-readable.

12. Remove the temp directory.

```
cd ..

rm -rf temp/
```

13. Change the context of the file. Run:

```
chcon staff_u:object_r:user_home_t:s0<output_file_name>.txt
```

14. Now that the file has been made, there are many methods you can use to move it to your local machine.

> **Note:**
> The following sub-steps are an example how to move the file via SCP.

    a. Open a local terminal window.

    b. Run:

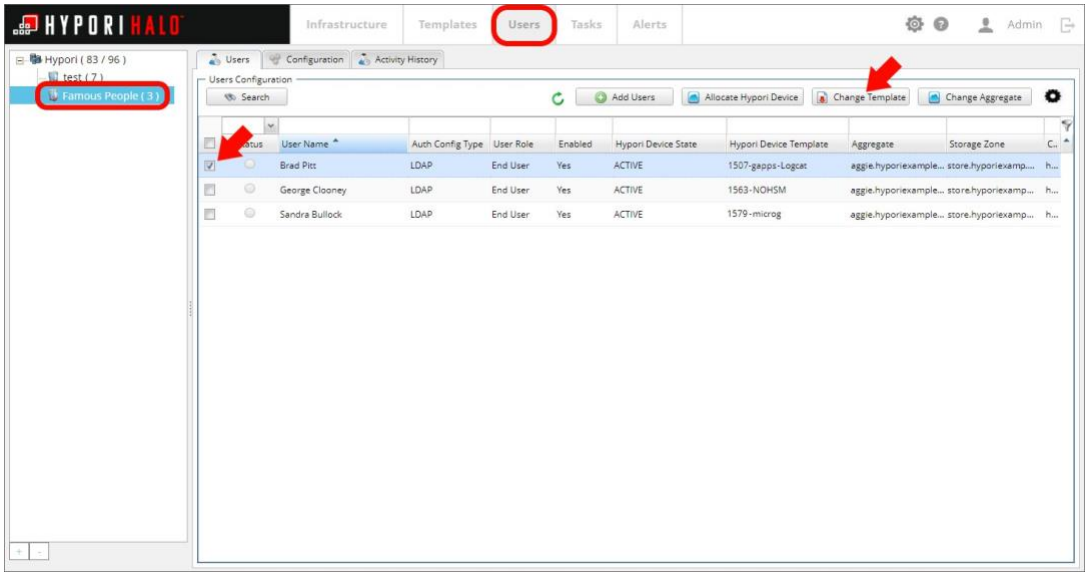
```
scp hypori@<IP_address>:/home/Hypori/logcat.txt .
```

The log file is now on your local machine. You can parse through the file yourself, or if you need additional assistance, you can reach out to support@hypori.com.

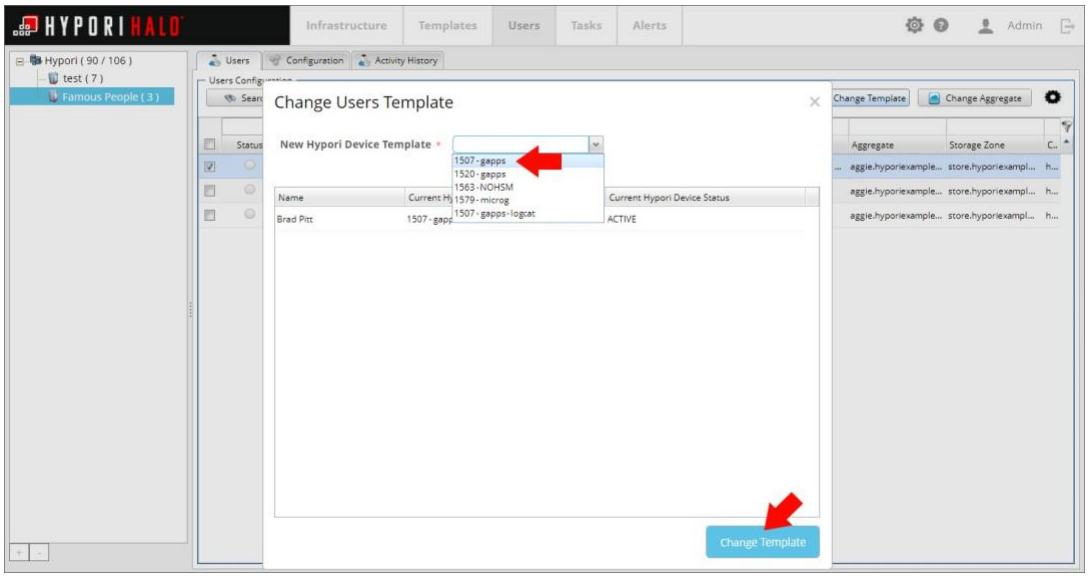
Resetting Logcat

Now that the log has been retrieved, the user's template needs to be reset.

1. Open the Hypori Halo Admin Console.
2. In the menu, click **Users**.
3. In the navigation pane, select the user's domain.
4. Click the **Users** tab.
5. Find the user and check the box next to their name.
6. Click **Change Template**.



7. Select the user's original template.
8. Click **Change Template**.



Troubleshooting Stuck VMI Instances that are Depleting Available Storage Space

You may encounter a situation where VMI instances may be stuck and depleting the amount of storage space available.

This is possibly caused by Hypori Halo consuming space somewhere in the `/var/` directory.

To troubleshoot stuck VMI instances depleting your available storage space, perform these steps:

1. Check disk space and annotating the consumption. Run:

   ```
   df -h
   ```

2. Determine what is consumed by `/var/log`.
3. Confirm there are no instances in the below path for the above. Run:

   ```
   /var/log/libvirt/qemu
   ```

   Example: This is checking for open instances that may be stuck and clogging disk space:

   ```
   [root@aushypcompute01 qemu]# lsof +L1
   COMMAND PID USER FD TYPE DEVICE SIZE/OFF NLINK NODE NAME
   ovsdb-ser 2912 root 7u REG 253,5 159 0 14 /tmp/tmpfrYjTDO (deleted)
   tuned 3796 root 8u REG 253,5 4096 0 18 /tmp/ffimXKKv5 (deleted)
   rhsmd 5086 root 4w REG 253,3 1531482 0 524374 /var/log/rhsm/rhsm.log-20200802 (deleted)
   virtlogd 6783 root 15w REG 253,3 206002 0 524367 /var/log/libvirt/qemu/instance-0000003f.log (deleted)
   virtlogd 6783 root 23w REG 253,3 25182 0 524335 /var/log/libvirt/qemu/instance-0000003e.log (deleted)
   virtlogd 6783 root 30w REG 253,3 15170 0 524339 /var/log/libvirt/qemu/instance-0000005f.log (deleted)
   virtlogd 6783 root 36w REG 253,3 93478 0 524352 /var/log/libvirt/qemu/instance-0000005c.log (deleted)
   virtlogd 6783 root 43w REG 253,3 45911 0 524385 /var/log/libvirt/qemu/instance-0000004d.log (deleted)
   virtlogd 6783 root 44w REG 253,3 106768 0 524368 /var/log/libvirt/qemu/instance-0000002d.log (deleted)
   virtlogd 6783 root 49w REG 253,3 9791 0 524372 /var/log/libvirt/qemu/instance-0000003c.log (deleted)
   virtlogd 6783 root 51w REG 253,3 119377 0 524387 /var/log/libvirt/qemu/instance-0000004f.log (deleted)
   virtlogd 6783 root 55w REG 253,3 119803 0 524389 /var/log/libvirt/qemu/instance-00000051.log (deleted)
   virtlogd 6783 root 59w REG 253,3 21252 0 524353 /var/log/libvirt/qemu/instance-00000035.log (deleted)
   virtlogd 6783 root 63w REG 253,3 101236 0 524346 /var/log/libvirt/qemu/instance-00000060.log (deleted)
   [root@aushypcompute01 qemu]# ps -ef | grep 0000004f | wc -l
   2
   [root@aushypcompute01 qemu]# ls /var/log/libvirt/qemu/
   ```

```
instance-00000045.log instance-00000046.log

[root@aushypcompute01 qemu]#
```

4. Perform a service restart. This should unstick the above open instances.

```
service virtlogd status

service virtlogd restart

service virtlogd status
```

Note:

These commands are non-invasive

5. Check disk space again to determine if it was cleared by the service restart. Run:

```
df -h
```

Appendix B. Security Information

When running security scans, one or more security alerts may occur.

The entries detailed in this Appendix contain additional information about these security alerts.

Version Alert - Postgres

When running a security scan, the following security alert may occur:

- Path: `/usr/bin/postgres` (via package manager)
- Installed version: 9.2.24 (postgresql-9.2.24-7.el7_9.x86_64)
- Fixed version: 9.3.23

A review of this alert within CVE-2018-1115 indicates it is a 'false positive'.

Note:

Red Hat indicates that this finding is not applicable to the base `postgresql` that ships with Red Hat Enterprise Linux 7, which is utilized as part of Hypori Halo packages.

For additional information, see page 2 in Affected Packages and Issued Red Hat Security Errata found in the Red Hat Customer Portal. Red Hat Enterprise Linux 7 shows that CVE-2018-1115 does not apply or is "not affected" by CVE-2018-1115.

Red Hat is still updating 6.2.24 versions and `postgresql-9.2.24-7.el7_9.x86_64` is the current version. This version addresses RHSA-2021:2397 - Security Advisory found in the Red Hat Customer Portal. Hypori will change the version of `postgresql` used in future revisions of product to clear this false positive from showing during OSCAP or security scans.

Version Alert - Cloud-init

When running a security scan, the following alert may occur:

- Rule ID: `xccdf_org.ssgproject.content_rule_rpm_verify_permissions`
- Node(s) Impacted: Compute, Controller, Storage, Management, TLS Proxy
- Package: `cloud-init`
- File(s): `/run/cloud-init`

A review of this alert indicates it is a 'false positive.'

As part of the managed Hypori Halo system hardening of Linux and Hypori Halo software, Hypori's build settings elevate the permissions of specific configuration files to be more restrictive than the settings defined in the stock rpm package.

By removing unneeded access to the file, Hypori enables more robust security controls to prevent subversion of Hypori Halo subsystem controls and critical processes.

Version Alert - Yum

When running a security scan, the following alert may occur:

- Rule ID: `xccdf_org.ssgproject.content_rule_rpm_verify_permissions`
- Node(s) Impacted: Compute, Controller, Storage, Management
- Package: `yum`
- File(s): `/var/cache/yum`

A review of this alert indicates it is a 'false positive.'

As part of the managed Hypori Halo system hardening of Linux and Hypori Halo software, Hypori's build settings elevate the permissions of specific configuration files to be more restrictive than the settings defined in the stock rpm package.

By removing unneeded access to the file, Hypori enables more robust security controls to prevent subversion of Hypori Halo subsystem controls and critical processes.

Appendix C. Components and Ports

Some Hypori Halo hosts have multiple components and ports. You may need to reference this information as you install or administer your Hypori Halo environment.

Compute Node Components and Ports

The compute node contains the following software components:

- Monit agent
- Nova Compute service components
- Puppet agent

The compute node uses the following ports:

Port Type	Port Number
SSH	22/tcp
Public network SPICE	5900-7500 [1,2]
Puppet kick interface	8139
Nova Compute service components	8774

[1] These ports must be allowed in from the outside.

[2] If Single Port Access is enabled, then port 433 is the only port that will be used.

Controller Node Components and Ports

The controller node contains the following software components:

- check_mk Nagios agent
- Cinder Volume service components
- Glance Image service components
- Horizon UI service components
- Keystone OS authentication components
- Monit agent

- MySQL DB components
- Neutron Network service components
- Nova Compute service components
- Puppet agent
- RabbitMQ

The controller node uses the following ports (none of which should be available externally):

Port Type	Port Number
SSH	22/tcp
Horizon UI service components	80/443
Monit agent	2812
MySQL DB components	3306
Keystone OS authen-tication components	5000/35357
RabbitMQ	5672
check_mk Nagios agent	6556
Puppet kick interface	8139
Puppet agent	8410
Nova Compute service components	8774
Cinder Volume service components	8776
Glance Image service components	9292
Neutron Network service components	9696

Management Server Components and Ports

The management server contains the following software components:

- Authentication server
- check_mk Nagios agent
- Management server
- MongoDB

- Monit agent
- nginx
- OpenLDAP
- Puppet agent

The management server uses the following ports:

Port Type	Port Number
SSH	22/tcp
Authentica- tion server TLS	443*
Monit agent	2812
check_mk Nagios agent	6556
OpenLDAP	8410
Puppet agent	8410
User setup server TLS	9443**
MongoDB	27017

* These ports must be allowed in from the outside.

** This port is optional from the outside.

Provisioning Server Components and Ports

The provisioning server contains the following software components:

- Foreman server
- Hypori repository
- Puppet master

The provisioning server uses the following ports:

Port Type	Port Number
SSH	22/tcp
http/httpd Redirect to 443	80/tcp

Port Type	Port Number
https/httpdForeman UI	443/tcp
DHCP OMAPI	7911/tcp
https/httpd Puppet master	8140/tcp
http/httpd Yum repositories	8240/tcp
https/ruby Foreman smart proxy	8443/tcp

Storage Node Components and Ports

The storage node contains the following software components:

- Cinder storage service
- Monit agent
- Puppet agent

The storage node uses the following port:

Port Type	Port Number
SSH	22/tcp
Puppet agent	8410
Cinder service	8776

Appendix D. Glossary

Acropolis

The Operating System used by Nutanix. Acropolis is based on Linux Kernel-based Virtual Machine (KVM).

ADCS

Acronym for **Active Directory Certificate Services**. An ADCS is an Active Directory tool that lets administrators customize services to issue and manage public key certificates.

Aggregate

Hypori Halo's infrastructure framework that distributes virtual workspaces across the designated compute nodes.

AHV

Acronym for **Acropolis HyperVisor**. AHV is a license-free virtualization solution included with the Nutanix/Acropolis system and is an alternative to VMware vSphere (ESXi) or Microsoft Hyper-V.

APK

Acronym for **Android Package Kit**. APK files are used to distribute and install mobile apps on Android based devices. In Hypori Halo, an APK must be included in a Published Image before being used in a Template.

ARP

Acronym for **Address Resolution Protocol**. This is a protocol for mapping an IP address to a physical machine address recognized in the local network.

Authentication Service

The Hypori Halo service running on the management server that handles authentication for the Hypori Halo clients.

Bivio

A U.S. government validated commercial hardware appliance that serves as TLS Proxy/ terminator. See **HAProxy**.

Bluetooth

Bluetooth is a short distance wireless technology standard (using short-wavelength UHF radio waves in the ISM band from 2.400 to 2.485 GHz) from fixed and mobile devices and building personal area networks (PANs).

CA

Acronym for **Certificate Authority**. This is the entity that issues digital certificates.

CentOS

CentOS is a free version of RHEL.

Cinder

Code name for the OpenStack Block Storage service. Cinder provisions and manages block devices known as Cinder volumes.

Client

Client usually refers to the app running on the end user's mobile device (iPhone, Note, etc.) but can also refer to the web console browser for the Hypori Halo Admin Console.

Client Device Policy

A series of selections which allows an administrator to determine settings such as password expiration, camera disabling, disconnect policy, etc.

Compute Node

The designation for the server hosting Hypori Halo virtual workspaces using the QEMU HyperVisor. A single compute node can host 250 virtual workspaces.

Controller Node

The designation for the server that contains the OpenStack infrastructure used to manage the compute nodes that run the (typically hundreds of) virtual workspaces.

CRT

CRT is the file type extension for a digital certificate file used with a web browser. **CRT files** are used to verify a secure website's authenticity, distributed by a **Certificate Authority (CA)**.

CSfC

Acronym for **Commercial Solutions for Classified**. A U.S. Government standards program that defines the security requirements for mobile device infrastructure that handles sensitive/classified information.

DHCP

Acronym for **Dynamic Host Configuration Protocol**. This is a client/server protocol that automatically provides a host with its IP address and other configuration information such as the default gateway and subnet mask.

DMZ

Acronym for **Demilitarized Zone**. The **DMZ** is a section of a network that exists between an intranet and the Internet. The purpose of a **DMZ** is to protect an intranet from unauthorized external access.

DNS

Acronym for **Domain Name System**. The **DNS** translates domain names to IP addresses so browsers can properly load internet resources.

DR

Acronym for **Disaster Recovery**. A proper plan for DR allows an organization to maintain or quickly resume mission-critical functions following hardware/software failure or some other external disaster.

Ethernet

Ethernet is a system for connecting multiple computer systems to form a local area network.

Extranet

Extranet is a controlled private network that allows designated intranet access to partners, vendors, suppliers, or an authorized set of customers.

FIPS

Acronym for **Federal Information Processing Standard**. **FIPS Publication 140-2** is a US government computer security standard used to approve cryptographic modules.

FIPS Mode

An enhanced "locked down" security mode that uses only cryptographic algorithms or other protocols allowed by the U.S. Federal Information Processing Standard. This option is only available for Hypori Halo.

Flavor

A flavor defines the memory, processor, and storage values for templates. Like AWS server "sizes".

Foreman

Open-source tool used for deploying and managing both physical and virtual servers. Used by Hypori Halo's provisioning server to manage the other Hypori Halo servers (e.g., controller, management, compute, and storage).

Glance

An **OpenStack** image service that provides services to store, browse, share, distribute and manage bootable disk images.

Google Play Services

A proprietary background service and set of APIs provided by Google for Android app development that provides a specific methodology for writing apps that meet Google's guidance. (Apps may still be written without these services)

HA

Acronym for **High Availability**. HA is a characteristic of a system, which aims to ensure a specific level of operational performance, for a greater than normal period.

HAProxy

An open-source software-based high availability load balancer and proxy server for TCP and HTTP-based applications that can spread requests across multiple servers. See **Bivio**.

Horizon

OpenStack component that is a web-based graphical user interface that is designed to manage **OpenStack** compute, storage, and networking services.

Image

OpenStack term for a bootable disk image. In Hypori Halo, published images are in a TGZ format and contain both an image as well as apps (APK files).

Internet

The **internet** is a global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.

Intranet

An intranet is a local or restricted communications network, especially a private network created using internet software.

IP Address

IP is an acronym for **Internet Protocol**. An **Internet Protocol Address** is a unique number assigned to all devices (such as a computer, tablet, or phone) when they connect to the internet.

Keystone

OpenStack identity service used for authentication (authN) and high-level authorization (authZ).

Logcat

A command-line tool that dumps a log of system messages, including stack traces when the device throws an error and messages that you have written from your app with the log class.

MAC Address

MAC is an acronym for **Media Access Control**. A **MAC Address** is a unique identifier assigned to a **NIC** for communications at the data link layer of a network segment. **MAC Addresses** are used as a network address for most network technologies, including **ethernet**, **Wi-Fi**, and **Bluetooth**.

Management Server

The Hypori Halo server that manages the Hypori Halo system as well as provides authentication services for Hypori Halo clients.

Monit

Open-source Linux supervision tool used for monitoring system status and recovery.

Neutron

OpenStack network service focused on delivering Networking-as-a-Service (NaaS) in virtual compute environments.

Nginx

Open-source web server used to run the Hypori Halo management server.

Nova

OpenStack component that provides on-demand access to compute resources by provisioning and managing large networks of virtual machines.

Nutanix

Software-based hyper-converged infrastructure that supports virtualization as an alternative to VMware.

OpenStack

Open-source platform for internal cloud computing. (e.g., VM deployment and management) In Hypori Halo, OpenStack spans the controller node and compute nodes.

PEM

Acronym for **Privacy Enhanced Mail**. This is a container format that may include just the public certificate (such as CA certificate files `/etc/nginx/certs`) or may include an entire certificate chain including public key, private key, and root certificates.

PFX

This is name of the combined format that holds both the private key and the certificate and is the format most modern signing utilities use. **PFX** is also known as a **PKCS12** file.

PKI

Acronym for **Public Key Infrastructure**. This is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

p12

.p12 is an alternate file extension for a **PFX** file.

Prism

The proprietary UI management module used in Nutanix Acropolis hyper-converged appliances for monitoring and managing a Nutanix system.

Provisioning Server

This is the designation for the Hypori Halo server that provisions the management server, controller node, compute nodes, and storage nodes used for deployments. It runs Foreman to deploy servers and Puppet to manage the server configurations.

Puppet

Open-source software configuration management tool used to install and manage the Hypori Halo servers/nodes.

RabbitMQ

Open-source message broker used internally by the Hypori Halo server system.

RHEL

Acronym for **Red Hat Enterprise Linux**. RHEL is an open-source operating system for physical, virtualized, and cloud-based environments that support enterprise users.

SELINUX

Acronym for **Security-Enhanced Linux**. This is a Linux kernel security module that provides a mechanism for supporting access control security policies.

Server Cert vs Client Cert

Server certificates are used to identify a server, whereas client certificates are used to authenticate the client to the server.

Sideload

A mechanism for loading an app on a phone without going to the official "app store".

SPICE

A communication protocol used between the Hypori Halo client on the user's mobile device and the back-end **virtual workspace**.

SSH

Acronym for **Secure Shell**. **SSH** is a cryptographic network protocol for operating network services securely over an unsecured network.

Template

A template defines the virtual workspace properties such as which mobile apps are included, amount of storage space allocated, and formats. Templates consist of **flavors** and **images**.

TLS

Acronym for **Transport Layer Security**. **TLS** is a cryptographic protocol designed to provide communications security over a computer network.

TLS Proxy

This is a proxy server used to handle incoming **TLS** connections, decrypting the **TLS**, and passing on the unencrypted request to the institution's other servers.

Virtual Device

An older designation for a Virtual Workspace. Some server commands and entries in the Hypori Halo Admin Console UI still use this terminology.

Virtual Workspace

A virtual workspace (sometimes referred to as a Virtual Device) is software that mimics a system that has functional hardware despite having no actual associated hardware. In Hypori Halo this is the Android-based virtual phone that the Hypori Halo client app connects to.

VyOS

Open-source network operating system based on Debian GNU/Linux that is sometimes used in Hypori Halo deployments to minimize the Hypori Halo footprint that is exposed to the enterprise network.

Wi-Fi

Wi-Fi is the popular name for wireless networking using IEEE 802.11*x* technology.

Appendix E. Change History

The following changes have been made to the *Hypori Halo Administrator's Guide*.

Version Number	Changes Made
1.0	Initial version of the *Hypori Halo Administrator's Guide*.
1.1	Resized several pictures that were not scaling properly when transformed into a PDF.
1.2	Expanded on the instructions listed in the "Importing Client Certificate" section.
1.3	Added additional entries to the virtual workspace policy section.
1.4	Updated the Product Support phone number.
1.5	Added the "Certificate Provisioning Using an Offline Registration Authority (RA)" section.
1.6	Added the "Using Logcat for Troubleshooting" section.
1.7	Added the "Troubleshooting Stuck VMI Instances" section.
1.8	Added the "Optional Configurations" chapter.
1.9	Added the "Configuring Smart Card Authentication in the Hypori Halo Admin Console" section.
1.10	Updated the "Using the ADB User Data Push" section.
1.11	Updated the "Smart Card Authentication" section.
1.12	Added the "Creating a New Admin Account" and "Disabling the Default Admin Account" sections.
1.13	Added the "Browser Requirements" section.
1.14	Minor revisions to several graphics.
1.15	Added 2 new entries to the "Security Information" Appendix as well as updated the "Changing the Default Authentication Time" section.
1.16	Corrected 2 minor typos caused by missing spaces as well as updated the Product Logo.

Version Number	Changes Made
1.17	Added the "Resetting a Screen Lock" section.
1.18	Updated all screenshots, branding and revised nearly every topic to improve consistency.