You can find the most up-to-date technical documentation on the VMware website at:
https://docs.vmware.com/
If you have comments about this documentation, submit your feedback to
docfeedback@vmware.com
About VMware Horizon Cloud on IBM Cloud Administration

This guide provides information on how to create, deploy, and administer virtual desktops and applications using Horizon Cloud.

Intended Audience

This document is intended for experienced IT system administrators who are familiar with virtual machine technology and datacenter operations.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.
The Horizon Cloud Administration Console

The Horizon Cloud Administration Console is the tenant administration interface for Horizon Cloud. The topics in this section provide general information about the Administration Console.

This chapter includes the following topics:
- Using the Console’s Search Feature
- Using the Filter Field in the Administration Console
- The User Card in the Horizon Cloud Administration Console
- Terms Used in the Administration Console

Using the Console’s Search Feature

Use the Horizon Cloud Administration Console’s search feature to locate a specific user or virtual machine (VM) by name in your environment.

Note In this release, the VM search is applicable only for VMs located in pods in Microsoft Azure.

You open the search box by clicking the magnifying glass icon ( ) in the header portion of the Administration Console. Then you can select to search within either users or VMs. When you have typed at least three (3) characters in the search field, names that begin with those characters are displayed. You can continue typing in more characters to narrow down the results.
Note With the VMs search, you can search for RDS server VMs in farms and VDI desktop VMs that are located in your Horizon Cloud inventory.

When you see the one you are searching for, you can click it to get more details about the user or VM. The screen that is displayed depends on whether you clicked on a user or a VM:

- For a user, the card for that user is displayed. For details, see The User Card in the Horizon Cloud Administration Console.

- For a VM, the system displays the screen on which you can locate that VM. For example, if you click on a VM in the results list that is an RDS server VM in a farm, the system displays the Servers tab of that farm’s details page.

Using the Filter Field in the Administration Console

Various pages in the Horizon Cloud Administration Console provide a filter field to filter the information that is displayed on those pages.
When a page has a filter field, as you type characters into the field, the system displays only the subset of the displayed records that contain characters that match that pattern.

**Note**  The system begins matching the pattern and filtering the records displayed in the page after you have typed three (3) characters into the filter field.

**On-Screen Filtering in the Reports Pages**

In the tabs of the Administration Console's Reports page, the filtering field works on the number of items that are displayed on the user interface itself and not on the total set of system records for that item. These pages support displaying up to 500 items. Therefore, if the system contains more than 500 records for an item, up to 500 items only are displayed in the user interface page. Using the filter field only filters the 500 displayed records. The filter is not applied to the full set. Here is an example to illustrate:

- You have 2000 users assigned to a VDI floating desktop assignment.
- The user names range from vdiuser-1 to vdiuser-2000, such as vdiuser-500, vdiuser-501, vdiuser-502, and so on up to vdiuser-2000.
- Over the course of a day, all 2000 users log in and use a desktop from that assignment.
- When you navigate to Monitor > Reports > Desktop Mapping, a displayed message states the report has more than 500 items.
- When you type vdiuser-54 into the filter to see the records for users vdiuser-54, vdiuser-540, vdiuser-541 up to vdiuser-549, you expect to see 11 rows displayed.

However, instead of displaying the expected 11 rows filtered out of the full 2000 set, the Desktop Mapping page displays only the subset of the originally displayed 500 rows that match the filter pattern. To see the full data set, use the export feature ( ![ ] ).

The following screenshot is an example of the Desktop Mapping page where the system has more than 500 records and the pattern entered in the filter field displays the subset of the displayed records.
The User Card in the Horizon Cloud Administration Console

Use the Horizon Cloud Administration Console’s user card feature as a dashboard to work with a specific user’s assigned resources, such as that user’s desktops.

You use the Administration Console’s search feature to display the card for a specific user. See Using the Console’s Search Feature for how to search for a user. When you click on a user in the search results, that user’s card is displayed.

Use the tabs at the top of the user card to work with those items in your environment that are related to that user.
### User Card Tabs

<table>
<thead>
<tr>
<th>Sessions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Lists current and historical user sessions, aggregated from all of your cloud-connected pods. Provides actions you can perform on the listed sessions. For details about these actions, see Actions You Can Take on Sessions.</td>
</tr>
<tr>
<td></td>
<td>- By default, only current sessions are shown.</td>
</tr>
<tr>
<td></td>
<td>- For sessions provisioned from pods in Microsoft Azure, you can use the drop-down on the left to show historical data for up to seven days.</td>
</tr>
</tbody>
</table>

**Note** Since by default current sessions are shown, the Sessions tab will show a value of 0 at the top when there is no current session. When you adjust the display to show historical data, this number is updated to the number of sessions in the selected period.

Click on a session to open its dashboard. From a session's dashboard, you can monitor the user session for troubleshooting. See Working with the Session Dashboard.

#### Assignments

<table>
<thead>
<tr>
<th>Assignments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Lists the user's assignments.</td>
</tr>
</tbody>
</table>

**Note** URL redirection customization assignments are not listed in the user card.

**Note** When a user is entitled to a dedicated VDI desktop assignment, but has not yet launched the desktop for the first time, that assignment appears on the Assignments tab. However, after the user's first launch of the desktop, the system removes it from the Assignments tab's list and displays it on the Desktops tab.

### Desktops

<table>
<thead>
<tr>
<th>Desktops</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Lists the user's:</td>
</tr>
<tr>
<td></td>
<td>- Active sessions to VDI floating desktops</td>
</tr>
<tr>
<td></td>
<td>- Active sessions to RDSH session desktops</td>
</tr>
<tr>
<td></td>
<td>- VDI dedicated desktops that have been assigned to this user, even when the user does not have an active session to that desktop.</td>
</tr>
</tbody>
</table>

**Note** The system assigns a VDI dedicated desktop to a user in one of two ways:

- You explicitly assign that specific dedicated desktop to this particular user, using the Assign action in the VDI dedicated desktop assignment's page
- The user claims the desktop from the set that is defined by the VDI dedicated desktop assignment to which that user is entitled. You can entitle a user to a VDI dedicated desktop assignment without explicitly assigning a specific dedicated desktop to that user. You entitle users using the assignment's Users/Groups area. Then when an entitled user launches a desktop from the set of desktops in that assignment for the first time, that user has claimed that VDI dedicated desktop, and the system permanently assigns that VDI dedicated desktop to that user.

On this tab, you can use the standard virtual machine (VM) action buttons to perform actions on the desktops' underlying virtual machines.

### Applications

<table>
<thead>
<tr>
<th>Applications</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Lists the user's entitled remote applications.</td>
</tr>
</tbody>
</table>

### Activity

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Displays the user's activity for selected time periods.</td>
</tr>
</tbody>
</table>

### Actions You Can Take on Sessions

The available actions you can take on a listed session vary based on the type of session and the permissions of the administrator.
<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>VDI Desktop</th>
<th>Session-based Desktop</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Message</td>
<td>Send a message to the logged-in user. When sent, the message appears on the user's screen.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote Assistance</td>
<td>Initiate a remote assistance session.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Restart</td>
<td>Restart the VM.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Disconnect</td>
<td>Disconnect the session.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Logoff</td>
<td>Log the user off the session.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Reset</td>
<td>Reset the VM.</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

**Working with the Session Dashboard**

When you click on one of the active sessions listed on the user card's Sessions tab, the dashboard for that session is displayed. This dashboard has tabs Details and Processes.

**Details tab**

The Details tab provides data about various session-related details that can be used to monitor the end user's session for troubleshooting purposes, such as CPU usage, memory usage, network latency, disk performance, and so on. Scroll through the dashboard and use the Less and More links to change how many details are displayed on the screen.

The following screenshot shows an example of some of the types of data and actions that are available in the session dashboard.
The User Experience Metrics area of the Details tab displays performance data and provides actions that super administrators and help desk administrators can use to troubleshoot issues in the session.

Processes

The Processes tab lists the processes and applications that are running in the session and provides an End Task button to end a troublesome process or application.

When the Help Desk Feature is Not Installed in the Desktop or Farm VM

When a VDI desktop VM or farm server VM is based on an image that does not have the Help Desk feature installed, an information alert is displayed when you open the dashboard for a session connected to that VM.

In this case, the VM's data is not reported to Horizon Cloud. Because the usual data is not available, some of the dashboard areas appear blank or empty for such sessions, such as:

- Most of the data about the client and VM is unavailable.
- The User Experience metrics and charts are empty.
- The Processes tab is empty.
- Refresh icons are not clickable.
- Some of the action buttons, such as the **End task** button, are not displayed.

**Terms Used in the Administration Console**

The Horizon Cloud Administration Console replaced the Enterprise Center, and some of the terms used in the interface are different.

The table below shows common Enterprise Center terms and their equivalents in the Horizon Cloud Administration Console.

<table>
<thead>
<tr>
<th>Enterprise Center</th>
<th>Horizon Cloud Administration Console</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop Manager</td>
<td>Pod</td>
</tr>
<tr>
<td>User Activity</td>
<td>Activity</td>
</tr>
<tr>
<td>Task and Events</td>
<td>Activity</td>
</tr>
<tr>
<td>Pool</td>
<td>Assignment</td>
</tr>
<tr>
<td>Session-based Pool (Desktop-only)</td>
<td>Session Desktop Assignment</td>
</tr>
<tr>
<td>Session-based Pool (Application-only)</td>
<td>Remote Application Assignment</td>
</tr>
<tr>
<td>Static Pool</td>
<td>Dedicated Desktop Assignment</td>
</tr>
<tr>
<td>Dynamic Pool</td>
<td>Floating Desktop Assignment</td>
</tr>
<tr>
<td>Mapped</td>
<td>Assigned User</td>
</tr>
<tr>
<td>Dynamic Pool Refresh</td>
<td>Push Updates</td>
</tr>
<tr>
<td>Gold Pattern</td>
<td>Image</td>
</tr>
<tr>
<td>Sealed Gold Pattern</td>
<td>Published Image</td>
</tr>
<tr>
<td>Unsealed Gold Pattern</td>
<td>Offline Image</td>
</tr>
</tbody>
</table>
The Getting Started wizard displays by default when you open the user interface, showing the tasks necessary to set up your Horizon Cloud system. The wizard provides a high-level overview of the work that you have done, and what you still need to do. You can access this page at any time by clicking the 'play' icon at the top of the page.

It is recommended that you perform the tasks in the order shown.

**Note** When you log in for the first time, you must register the Active Directory before you can start using the system. See below under General Setup.
## General Setup

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>Includes tasks related to general settings.</td>
</tr>
</tbody>
</table>
| To add first AD domain: | - Click the Add button under Active Directory.  
|                       |   - Follow steps in Register Your First Active Directory Domain. |
| To edit the AD domain: | - Click the Edit button under Active Directory.  
|                       |   - Follow steps in Edit an Active Directory Domain. |
| Roles and Permissions | To edit roles and permissions:  
|                       |   - Click the Edit button under Roles & Permissions.  
|                       |   - Follow the steps in Edit Roles and Permissions. |
| User Session Information | This feature allows user and domain data to be used by the Cloud Monitoring Service (CMS) for reports on the Reports page. If it is disabled, the following are not provided:  
|                       |   - The Unique User Summary feature of the Utilization report  
|                       |   - The Session History report  
|                       |   - Click the Edit button under User Session Information.  
|                       |   - To keep the feature enabled, leave the default setting (YES) and click Save. To disable, switch the setting to NO and click Save. |
| Note                  | The agents on the virtual machines (RDSH and VDI) need outbound Internet access so they can send the data to Horizon Cloud. |

## Desktop Assignment

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
</table>
| To import a VM for image creation: | - Click the New button under Import VM.  
|                       |   - Follow the steps for importing a VM in Chapter 11 Imported VMs. |
| To create an image from a VM: | - Click the New button under Create Image.  
|                       |   - Follow the steps in Create an Image. |
| To create a desktop farm: | - Click the New button under Create Desktop Farm.  
|                       |   - Follow the steps in Create a Farm. |
| To create a desktop assignment: | - Click the New button under Create New Desktop Assignment.  
|                       |   - Follow the steps in Create a Dedicated or Floating VDI Desktop Assignment or Create an RDSH Session Desktop Assignment, depending on the type of desktop assignment you want to create. For more information, see Types of Assignments. |

## Application Assignment

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
</table>
| To create an RDSH image: | - Click the Configure button under Create RDSH Image.  
<p>|                       |   - Follow the steps in Create an RDSH Image. |
| To create an application farm: | - Click the New button under Create Application Farm. |</p>
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Follow the steps in <a href="#">Create a Farm</a>.</td>
</tr>
<tr>
<td></td>
<td>To review application inventory:</td>
</tr>
<tr>
<td></td>
<td>Click the <strong>Go</strong> button under Application Inventory.</td>
</tr>
<tr>
<td></td>
<td>Review and edit applications on the Applications page as described in <a href="#">Chapter 7 Applications</a>.</td>
</tr>
<tr>
<td></td>
<td>To create a new application assignment:</td>
</tr>
<tr>
<td></td>
<td>Click the <strong>New</strong> button under Create New Application Assignment.</td>
</tr>
<tr>
<td></td>
<td>Follow the steps in <a href="#">Create an Application Assignment</a>.</td>
</tr>
</tbody>
</table>

At the bottom of the page, use the slider to indicate if you want the Getting Started page to appear at startup.
Join or Leave the Customer Experience Improvement Program

The VMware Customer Experience Improvement Program (CEIP) provides information that VMware uses to improve its products and services, to fix problems, and to advise you on how best to deploy and use VMware products.

Horizon Cloud participates in the VMware CEIP. Information about the data collected through CEIP and how VMware uses it are in the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html.

The CEIP appears the first time you start Horizon Cloud after completing the domain join. You must then make a selection. You can change your selection at any time after that.

Procedure

1. Start the Horizon Cloud Administration Console.

2. Select Help > CEIP.

3. Move the slider next to Join Customer Experience Improvement Program to No to leave CEIP or Yes to join. The default is Yes.

4. Click Save.
Monitoring

Use the Monitor icon to access desktop information, administrator and user activity, view reports detailing user and desktop mapping, and check notifications.

There are four selections available from the Monitor icon.

<table>
<thead>
<tr>
<th>Selection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>Displays details on desktop connections, connection states, and capacity allocation.</td>
</tr>
<tr>
<td>Activity</td>
<td>Displays activity details for Administrators and Users.</td>
</tr>
<tr>
<td>Reports</td>
<td>Provides mapping details for Users and Desktops</td>
</tr>
<tr>
<td>Notifications</td>
<td>Displays a list of current notifications.</td>
</tr>
</tbody>
</table>

This chapter includes the following topics:

- Dashboard Page
- Activity Page
- Reports Page
- Notifications Page

Dashboard Page

This page is available from the Monitor icon and displays information about your overall environment.

The system refreshes the information every few minutes and displays a message indicating the amount of time remaining until the next refresh. You can also refresh the page manually.
<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capacity</td>
<td>The allocated capacity. To see a chart of historical capacity usage, roll over the square. By default, the chart shows the last seven days of data. One point corresponds to one day. Data is averaged over the tenants in your environment within those seven days, on a daily basis.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you have multiple desktop models, the value displayed here is the percentage allocated of the total capacity of all desktop models. For example, if DM-1 has 50 out of 100 allocated (50%) and DM-2 has 0 out of 25 allocated (0%), the total is 50 out of 125 allocated and the value displayed will be 40%. To see the information for the individual desktop models, roll over the graphic and click <strong>More</strong>.</td>
</tr>
<tr>
<td>Utilization</td>
<td>Utilization of allocated RDS desktops and remote applications. The system's definition of utilization is the number of active sessions divided by the maximum possible number of sessions. To see a chart of historical utilization data, roll over the square. By default, the chart shows the last seven days of data. One point corresponds to one hour. Data is averaged over the desktop assignments/farms and application farms in your environment within those seven days, on an hourly basis.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Data for this report are updated at the beginning of each hour, but not in between. For example, any user activity from 2:01 PM to 2:59 PM would not be included in the report until 3:00 PM.</td>
</tr>
<tr>
<td>Activity</td>
<td>Desktop, application, and peak activity. Click on the labels to filter the displayed information.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Data for this report are updated at the beginning of each hour, but not in between. For example, any user activity from 2:01 PM to 2:59 PM would not be included in the report until 3:00 PM.</td>
</tr>
<tr>
<td>Top Location by Users</td>
<td>Reflects the usage according to your named locations.</td>
</tr>
</tbody>
</table>

**Activity Page**

The Activity page shows data regarding current and past events in the system.

The Activity page is available from the Monitor icon. It contains tabs for administrator and user events.

**Admins Tab**

The Admins tab displays administrator events with information for each action. You can perform these tasks.

- Use the Show filter to display events for only a certain period of time.
- View the total number of events.
- Use the Filter box to filter events.
- Refresh the list.
- Download information in the list in .xlsx format with the Export feature.
- Expand an event to view details and subtasks for that event.
<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Details regarding the event.</td>
</tr>
<tr>
<td>Status</td>
<td>Successful indicates an event was performed in its entirety. Failed indicates an event was either partially performed or not performed at all.</td>
</tr>
<tr>
<td>% Completion</td>
<td>Current percentage of event completed.</td>
</tr>
<tr>
<td>Time</td>
<td>Time that the event was logged.</td>
</tr>
</tbody>
</table>

- You can cancel some tasks before they complete by selecting the task in the list and clicking the **Cancel Tasks** button.
- Before attempting to select a task for cancellation, refresh the view to update the status for the tasks displayed.
- If a task is currently able to be cancelled, you will be able to select the corresponding check box in the task list. If you select the 'select all' check box at the top of the list, all tasks that can currently be cancelled are selected.

The table below shows tasks that you can cancel.

<table>
<thead>
<tr>
<th>Task</th>
<th>Cancel When Task is in Queued State</th>
<th>Cancel When Task is in Running State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Farm Expansion</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When the system has automatically created an expansion task for an RDSH farm, the farm must be offline before you can cancel that task.</td>
<td><strong>Note</strong> When the system has automatically created an expansion task for an RDSH farm, the farm must be offline before you can cancel that task.</td>
</tr>
<tr>
<td>Assignment Expansion</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When the system has automatically created an expansion task for a VDI desktop assignment, the assignment must be offline before you can cancel that task.</td>
<td><strong>Note</strong> When the system has automatically created an expansion task for a VDI desktop assignment, the assignment must be offline before you can cancel that task.</td>
</tr>
<tr>
<td>Convert VM to Image</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you cancel this task, and wish to retry it, first confirm that the VM is in a state where it can be converted. If you are not sure, power off and then power on the VM.</td>
<td><strong>Note</strong> If you cancel this task, and wish to retry it, first confirm that the VM is in a state where it can be converted. If you are not sure, power off and then power on the VM.</td>
</tr>
<tr>
<td>Rebuild VM</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Push Updates</td>
<td>Supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>

**Users Tab**

The Users tab displays user events with information for each event. You can perform these tasks.

- Use the Show filter to display events for only a certain period of time.
- View the total number of events.
- Use the Filter box to filter events.
- Refresh the list.
- Download information in the list in .xlsx format with the Export feature.
- Expand an event to view details and subtasks for that event.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Details regarding the event.</td>
</tr>
<tr>
<td>Time</td>
<td>Time that the event was logged.</td>
</tr>
</tbody>
</table>

**Reports Page**

Use the Reports page to access various reports related to end users' desktop and application sessions.

**Important** The Desktop Health, Utilization, Session History, Concurrency, and Top Applications reports do not reflect user-related data until an hour has passed from the time you enabled monitoring user session information.

Select Monitor > Reports to open the Reports page, where you can view detailed information for the following categories. You can also manually refresh this page, filter your search, and export data to a Microsoft Excel worksheet.

**Note** If you have disabled monitoring user session information for utilization, trending, and historical analysis, the reports associated with that type of data are disabled and not visible on the Reports page. When that monitoring feature is disabled, the system collects such user session information for a limited period of time and hashes the username to enable real time administration while disabling historical and aggregated viewing of that user information. As a result, the reports that would display historical and aggregated viewing of that data, such as the Session History report, are not available.

The **Enable User Session Information** toggle for enabling or disabling monitoring user session information is located on the General Settings page (Settings > General Settings).
<table>
<thead>
<tr>
<th>Report Type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Mapping</td>
<td>View details and sort by various categories, such as User name, Domain, Desktop Name, Desktop Model, Farm, and Mapping Type (User or Group).</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This report is populated only for users that have at least one direct assignment to a desktop. In the Administration Console, you can choose individual users or user groups when making a desktop assignment. If a user has at least one assignment done as an individual user and zero or more assignments done as being part of the assigned group, this report reports all of that user's desktop assignments. However, if all of the user's desktop assignments are done using groups, that user's assignments are not reported in this report. If the user is mapped to a desktop as an individual user, the Group Name column is blank. If the user is mapped to a desktop from being a member of a group that is entitled to the desktop assignment, the Group Name column displays the entitled group's name.</td>
</tr>
<tr>
<td>Desktop Mapping</td>
<td>View details and sort by various categories, such as Desktop Name, Model, Assignment Name, Type, Farm, Active User, Mapped Users, and Mapped User Groups.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> In this report, the Mapped Users column is populated only for dedicated VDI desktop assignments, because for such assignments, each user gets mapped to a specific VDI desktop and returns to that same desktop at each login. That mapped user is the user assigned to that desktop. However, for floating VDI desktop assignments and session desktop assignments that are served by farms, users do not get mapped to specific desktop VMs. As a result, there is not data in the Mapped Users column for those desktop assignment types.</td>
</tr>
<tr>
<td>Desktop Health</td>
<td>View list of desktops, which can be filtered by assignment or error status. Click on a desktop to view its real-time desktop health report.</td>
</tr>
<tr>
<td></td>
<td>- For RDS desktops, the report includes CPU usage %, memory usage %, disk IOPS, and active/disconnected sessions.</td>
</tr>
<tr>
<td></td>
<td>- For VDI desktops, the report includes CPU usage %, memory usage %, disk IOPS, duration, bandwidth, and latency.</td>
</tr>
<tr>
<td></td>
<td>- For all desktops, a Desktop Health alert displays when one or more of the following parameters is at or above a set threshold value: CPU usage %, memory usage %, and disk latency.</td>
</tr>
<tr>
<td></td>
<td>- Threshold values are 90% for CPU, 80% for memory usage, and 100ms for disk latency.</td>
</tr>
<tr>
<td></td>
<td>- These parameters are checked every minute, and the alert is triggered when the measurement is at or above the threshold value for 10 consecutive minutes.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This report's data is updated every minute by the data from the backend reporting system.</td>
</tr>
<tr>
<td>Report Type</td>
<td>Details</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Utilization</td>
<td>View graphs for user and session trends, protocol and client usage, access type (internal or external), session duration, and service type. Can be filtered by assignment and time period.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When Enable User Session Information is turned off for your environment, the Unique User Summary feature of this report is not provided. The Enable User Session Information is set in the General Settings page.</td>
</tr>
<tr>
<td></td>
<td>The backend reporting system sends the data for this report at a specific UTC time:</td>
</tr>
<tr>
<td></td>
<td>■ For the selected periods <strong>Last 24 hours</strong> or <strong>Last 1 week</strong>, the data is updated hourly. The update starts at 5 minutes past the hour UTC and takes about 15 minutes to complete.</td>
</tr>
<tr>
<td></td>
<td>■ For the other time periods, the data is updated daily. The update starts at 2am UTC and takes about 15 minutes to complete.</td>
</tr>
<tr>
<td>Session History</td>
<td>View session information by user, including last login time, session duration, weekly average use, and average session length. Can be filtered by time period.</td>
</tr>
<tr>
<td></td>
<td>The backend reporting system sends the data for this report daily at a specific UTC time. The update starts at 2:10am UTC and takes about 15 minutes to complete. Due to that update timing, data for sessions that take place after the 2am UTC time point are not reflected in this report until the next day.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This report is not provided when Enable User Session Information is turned off for your environment, as set in the General Settings page.</td>
</tr>
<tr>
<td>Concurrency</td>
<td>View per-assignment data for capacity, number of concurrent users, peak concurrency, and applications in use. Can be filtered by time period.</td>
</tr>
<tr>
<td></td>
<td>The backend reporting system sends the data for this report daily at a specific UTC time. Due to that update timing, data for sessions that take place after the 2am UTC time point are not reflected in this report until the next day.</td>
</tr>
<tr>
<td>Top Applications</td>
<td>View a list of applications that end users have used in VDI desktops and each application's total usage duration. Can be filtered by assignment and by time period.</td>
</tr>
<tr>
<td></td>
<td>This data can help you see which are the most used applications in a particular VDI desktop assignment.</td>
</tr>
<tr>
<td></td>
<td>The backend reporting system sends the data for this report at a specific UTC time:</td>
</tr>
<tr>
<td></td>
<td>■ For the selected period <strong>Last 24 hours</strong>, the data is updated hourly. The update starts at 20 minutes past the hour UTC and takes about 15 minutes to complete.</td>
</tr>
<tr>
<td></td>
<td>■ For the other time periods, the data is updated daily. The update starts at 2:30am UTC and takes about 15 minutes to complete.</td>
</tr>
<tr>
<td>URL Configurations</td>
<td>View information for currently configured URL redirects. For more information, see Create a URL Redirection Customization and Assign it to Users.</td>
</tr>
<tr>
<td>Agent Versions</td>
<td>View current versions of agents and VMware Tools for each VM. Select a pod in the Pod drop-down at the top left of the page to show information for that pod. You can also sort data on all columns, including Assignment Name.</td>
</tr>
</tbody>
</table>

**Notifications Page**

The Notifications page shows information regarding system notifications.
The Notifications page is available from the Monitor icon. You can perform these tasks.

- Use the Show filter to display notifications for only a certain period of time.
- View the total number of notifications.
- Use the Filter box to filter notifications.
- Refresh the list.
- Download information in the list in .xlsx format with the Export feature.

The Notifications page displays notifications with information for each one.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Icon indicates the type of notification.</td>
</tr>
<tr>
<td></td>
<td>- Blue &quot;i&quot; icon - information</td>
</tr>
<tr>
<td></td>
<td>- Yellow &quot;!&quot; icon - warning</td>
</tr>
<tr>
<td></td>
<td>- Red &quot;x&quot; icon - critical issue</td>
</tr>
<tr>
<td>Notification</td>
<td>Text of the notification.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the notification. For example, Active or Dismissed,</td>
</tr>
<tr>
<td>Date</td>
<td>Date of notification.</td>
</tr>
</tbody>
</table>

**Note** Notifications also appear in an abbreviated list format when you select the notifications icon ("bell" shape) at the top of the user interface page. You can double-click on a notification to view it on the Notifications page or select Show All to navigate to the Notifications page.
Assignments

On the Assignments page, you can create, edit, and delete assignments, and also update agent software for dedicated desktop assignments.

Click the Assign icon to access the Assignments page, where you can take these actions.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Create a new application, desktop, or customization assignment.</td>
</tr>
<tr>
<td>Edit</td>
<td>Select an assignment to make changes, or drill down to view summary and sessions information.</td>
</tr>
<tr>
<td>Take Offline</td>
<td>For specific types of desktops assignments, allows you to take them off line for maintenance. For active customization assignments, allows you to make them inactive.</td>
</tr>
<tr>
<td>Update Agent</td>
<td>Update agents for dedicated desktop assignments.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete an assignment.</td>
</tr>
<tr>
<td>Recover</td>
<td>[Instant Clone desktops only] Recover desktops that encountered an error during a previous image update.</td>
</tr>
<tr>
<td>Bring Online</td>
<td>Bring an offline desktop assignment online again. For inactive customization assignments, allows you to make them active.</td>
</tr>
</tbody>
</table>

Clicking on an assignment in the list opens a detail page showing summary information for the assignment. For some types of assignments, there are other tabs in addition to the Summary tab:

- Desksops - displays for dedicated and floating desktop assignments. See Manage Desktops in a Dedicated or Floating Desktop Assignment.
- System Activity and User Activity - display for dedicated and floating desktop assignments. See View Activity or Cancel Tasks for Assignments.
- Sessions - displays for native application assignments. See View Activity or Cancel Tasks for Assignments

The following topics provide additional information about data shown on the Assignments page:

- Types of Assignments - Describes values that display in the Type column.
- Capacity and Users Values for VDI Desktop Assignments - Describes values that display in the Capacity and Users columns.
This chapter includes the following topics:

- Types of Assignments
- Capacity and Users Values for VDI Desktop Assignments
- Create an Application Assignment
- Create a Dedicated or Floating VDI Desktop Assignment
- Create an RDSH Session Desktop Assignment
- Edit an Assignment
- Create a URL Redirection Customization and Assign it to Users
- Edit Assignment Mode
- Update Agent Software for an Assignment
- Delete an Assignment
- Recover an Assignment
- Manage Desktops in a Dedicated or Floating Desktop Assignment
- View Activity or Cancel Tasks for Assignments
- Working with Nested Organizational Units

**Types of Assignments**

There are several types of assignments, as described in the table below. The type for each assignment appears in the Type column of the assignment list.
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Use application assignments to assign Windows applications to groups. See Create an Application Assignment. Type displayed can be:</td>
</tr>
<tr>
<td></td>
<td>- Remote Applications - Assignment includes applications from servers in RDSH farms.</td>
</tr>
<tr>
<td></td>
<td>- Native Applications - Assignment includes AppStacks.</td>
</tr>
<tr>
<td>Desktops</td>
<td>Use desktop assignments to assign dedicated, floating, or RDSH-based virtual desktops to users and groups. See Create a Dedicated or Floating VDI Desktop Assignment and Create an RDSH Session Desktop Assignment. Type displayed can be:</td>
</tr>
<tr>
<td></td>
<td>- Dedicated Desktop - Traditional Clone</td>
</tr>
<tr>
<td></td>
<td>- Dedicated Desktop - Instant Clone</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Dedicated Desktop - Instant Clone assignments can only be created in certain unusual configurations, and are not recommended. If you wish to create this type of assignment, consult your VMware representative first to confirm that you will be able to do so.</td>
</tr>
<tr>
<td></td>
<td>- Floating Desktop - Traditional Clone</td>
</tr>
<tr>
<td></td>
<td>- Floating Desktop - Instant Clone</td>
</tr>
<tr>
<td></td>
<td>- Session Desktop</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Because a session desktop uses the traditional type of cloning by default, the Assignments page displays Session Desktop in the Type column for such assignments. Definitions are as follows.</td>
</tr>
<tr>
<td></td>
<td>- Dedicated Desktop - In a dedicated desktop assignment, each user is assigned a specific remote desktop and returns to the same desktop at each login. Dedicated assignments require a one-to-one desktop-to-user relationship and should be sized based on the total user population. The primary use for dedicated desktop assignments is to ensure that the hostname of the desktop VM remains the same between sessions. Certain software packages might require this use for licensing.</td>
</tr>
<tr>
<td></td>
<td>- Floating Desktop - In a floating desktop assignment, a user might receive a different VM with a different machine name and/or hostname with each login. With floating desktop assignments, you can create desktops that shifts of users can use. Sizings should be based on the maximum number of concurrent users.</td>
</tr>
<tr>
<td></td>
<td>- Session Desktop - In a session desktop assignment, an RDSH-published desktop experience is shared across multiple users, that is, terminal services.</td>
</tr>
<tr>
<td></td>
<td>- Traditional Clone and Instant Clone - Type of cloning used for desktops. The option for selecting clone type is available while creating an image. The image selected for creating a desktop defines the desktop clone type. See Create an Image.</td>
</tr>
<tr>
<td></td>
<td>Note the following:</td>
</tr>
<tr>
<td></td>
<td>- A desktop can have multiple users assigned to it, but it can be used by only one user at a time.</td>
</tr>
<tr>
<td></td>
<td>- Desktops in floating desktop assignments do not provide persistence. You can configure persistence as part of an application assignment.</td>
</tr>
<tr>
<td></td>
<td>- Where possible, use floating desktop assignments because they cost less than dedicated desktop assignments and do not dedicate VM resources for each user.</td>
</tr>
<tr>
<td>Customization - URL Redirection</td>
<td>Use these assignments to assign URL handling rules to users. See Create a URL Redirection Customization and Assign it to Users.</td>
</tr>
</tbody>
</table>
Capacity and Users Values for VDI Desktop Assignments

For dedicated and floating VDI desktop assignments, the capacity and user values shown in the respective columns on the Assignments page are calculated as described below.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capacity</td>
<td>Capacity represents the number of desktops involved in that dedicated or floating desktop assignment.</td>
</tr>
<tr>
<td>Users or user groups</td>
<td>Number of users or user groups currently mapped to the assignment. The actual number that is displayed depends on whether the assignment is mapped to a set of individual users, to a group or multiple groups, or to a combination of both.</td>
</tr>
</tbody>
</table>

**Note** For session desktop assignments and application assignments, the Assignment page's Capacity column shows NA by default.

Create an Application Assignment

You can create an application assignment on the Assignments page.

**Procedure**

1. Click the **Assign** icon.
   - The Assignments page displays.
2. Click **New**.
3. Click the **Get Started** button under Applications.
4. On the Definition tab, select a type for the assignment.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote</td>
<td>Assignment includes applications from your RDSH farms.</td>
</tr>
<tr>
<td>Native</td>
<td>Assignment includes AppStacks.</td>
</tr>
</tbody>
</table>

**Note** The fields displayed on this tab will differ depending on the type you select.
If you selected Native, enter information in the fields as described below, click **Next**, and then proceed to Step 9 below.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignment Name</td>
<td>Unique name for the assignment.</td>
</tr>
<tr>
<td>OS</td>
<td>Select the correct OS from the drop-down menu. This OS must be the same OS as the OS used to capture the applications.</td>
</tr>
<tr>
<td>Computer Name Prefix</td>
<td>(Optional) Enter a prefix. Entering a prefix limits access to the application assignment to authorized users who log in to a desktop assignment that has the same prefix at the beginning of its name. If you leave this option blank, all authorized users can access the new application assignment regardless of the desktop assignments they are logged in to.</td>
</tr>
</tbody>
</table>

If you selected Remote, enter a unique name for the assignment and then proceed to the next step.

On the Applications tab, select the remote applications or AppStacks to include in the assignment, and click **Next**.

The displayed list reflects whether you selected **Remote** or **Native** for the application type in the previous steps. If you had selected **Remote** for the application type, the applications you select here can be from different farms.

On the Users tab, start typing the name of a user or group in the text box, and then click the name in the list to select it.

(Optional) Repeat the previous step to select additional users or groups.

Click **Next**.

On the Summary tab, review the information on and if it is correct, click **Submit**. If not, click **Back** to return to previous tabs and edit your information.

### Create a Dedicated or Floating VDI Desktop Assignment

You create VDI desktop assignments from the Assignments page.

Use these steps to assign a dedicated or floating VDI desktop to your end users. To assign a session-based (RDSH) desktop, see the steps in **Create an RDSH Session Desktop Assignment**.

**Procedure**

1. Click the **Assign** icon.

   The Assignments page displays.

2. Click **New**.

3. Click the **Get Started** button under Desktops.

   The Assign Desksop dialog displays.
4 Select either Dedicated or Floating to create an assignment for a VDI desktop. For information on types of desktop assignments see Types of Assignments. For the steps on creating a session-based desktop, see Create an RDSH Session Desktop Assignment.

**Note** There will be some variation in the fields displayed on the screen, depending on the type of desktop assignment you are creating. These variations are noted in the following steps.

5 Enter information for Fixed Attributes.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pod</td>
<td>This option only displays if the data center is configured with multiple pods. You can only create assignments from images in the same pod.</td>
</tr>
<tr>
<td>Desktop Model</td>
<td>Select model from the drop-down list.</td>
</tr>
<tr>
<td>Domain</td>
<td>[Traditional Clone images only] Select domain from the drop-down list.</td>
</tr>
<tr>
<td>Join Domain</td>
<td>[Traditional Clone images only] Leave default setting (Yes).</td>
</tr>
</tbody>
</table>

6 Enter information for the Flexible Attributes displayed.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Image        | Select an image from the list.  
- In the list, the acronym for the image type appears at the beginning of the image name. For example, '[IC] image1' is an Instant clone image and '[TC] image 2' is a Traditional Clone image.  
- For dedicated desktop assignments, Instant Clone images will not display for most users. It is not recommended to create this type of assignment, but if you wish to do so, consult your VMware representative first to confirm that your system is configured to allow this.  
- For dedicated and floating desktop assignments, RDSH role-enabled images will not be listed, since there is no reason that users would want to create dedicated or floating desktop assignments from those images. RDSH role-enabled images are used for session desktop assignments. |
| Assignment Name | A unique name for the new assignment. |
| VM Names      | Name for all virtual machines or guest desktops in this assignment, which will have a number appended to it, for example, win7-1, win7-2, win7-Floating. The name must start with a letter and can contain only letters, dashes, and numbers. This value is prefilled based on the assignment name. |
| Default Protocol | Select Blast (HTML Access) or PCoIP. |
| Preferred Client Type | Select Browser or Horizon Client. |
| Capacity      | Number of desktops in the assignment. Capacity remaining is indicated to the right of the field.  
**Note** If the remaining capacity displayed appears to be too low, it may be because the default limit of 2,000 desktops per pod has been reached. This includes VMs created in earlier versions of the product, but does not include Utility or Imported desktops. For more information, contact your VMware representative. |
7 Under Flexible Attributes, expand Advanced Properties and enter required information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer OU</td>
<td>Active Directory (AD) Organizational Unit where VMs are located. For example, OU=NestedOrgName,OU=RootOrgName,DC=DomainComponent,DC=eng, and so on. The entries must be comma-separated with no spaces in between. For more information about Active Directory, see Working with Nested Organizational Units.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> For traditional clones, if the Computer OU is set to 'CN=Computers' the system uses the default Active Directory 'Computers' container for VMs. Note that this default container may have been redirected to an organizational unit class container.</td>
</tr>
<tr>
<td>Run Once Script</td>
<td>(Optional) Location of scripts that should run after system preparation completes.</td>
</tr>
<tr>
<td>Session Timeout Interval</td>
<td>The timeout value for end user sessions to the desktops. The default is seven days (10,080 minutes). The maximum value is 99,999 minutes, approximately 69 days.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If no user activity occurs before the timeout interval is reached, a message indicates that the user will be logged off if they do not click OK in the next 30 seconds. If the logoff occurs, any unsaved documents are lost.</td>
</tr>
<tr>
<td></td>
<td>If you are assigning a timeout value for dedicated desktops, you can specify the maximum value. If you have a large timeout interval set for floating desktops, the desktops do not reset as quickly if they are not in use. This configuration might result in the pool of available desktops running out, and users seeing failure messages.</td>
</tr>
<tr>
<td>Enable Windows Hot Plug</td>
<td>This setting enables/disables the HotPlug functionality for desktops in an assignment. When this is set to No (default setting), network adapters do not appear in the Quick Add/Remove area. This makes it more difficult for users to put their VMs into an unusable state.</td>
</tr>
</tbody>
</table>

8 Click **Next**.

9 On the Users step, select tenant from the drop-down list and then start typing the name of a user or group from your Active Directory.

10 Select a user or group from the list.

11 (Optional) Search for and select additional users or groups, and click **Next**.

   If you assign a dedicated desktop to more than one user, a warning message appears to verify if this is the intended configuration. The configuration is supported, but the users would share the desktop and only one can use it at any one time.

12 On the Summary step, confirm that the displayed information is correct and click **Submit**.

13 Click the **Assign** icon to see your new assignment.

**Create an RDSH Session Desktop Assignment**

You create session desktop assignments using the Assignments page.

For general information about desktop assignments, see **Types of Assignments**.
Prerequisites

Verify you have the following items:

- The Farms page lists at least one farm of remote desktops type. Only farms configured to deliver remote desktops can be used for a session desktop assignment.
- The farm you want to use is in the pod from which you want to deliver the session desktops.
- The farm is not already used in an assignment. A farm configured to deliver remote desktops cannot be used in more than one session desktop assignment. To verify whether the farm you want to use is already used in a session desktop assignment, look in the Assignment page’s Farms column and see if the farm is listed. If it is listed, then it is already being used in a session desktop assignment and you will have to create a new farm.

Procedure

1. Start the New Assignment workflow by clicking Assign and clicking New.
2. In the New Assignment start screen, click the Desktops icon.
   
   The New Desktop Assignment window opens to the first wizard step.
3. On the wizard's Definition step, click Session.
Complete the selections on the Definition step and then click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pod</td>
<td>This option only displays if your data center is configured with multiple pods. Pods contain specific assignable images and server model capacities for assignments. You can only create assignments from images in the same pod.</td>
</tr>
<tr>
<td>Farm</td>
<td>Select the farm that has the configured RDS-enabled image that you want to assign to the end users. Only farms that are in the selected pod and which not already involved in existing session desktop assignments are available for selection.</td>
</tr>
<tr>
<td>Assignment Name</td>
<td>Type a friendly name for this assignment. The end users see this name when they go to access their assigned desktop. For example, when an end user launches Horizon Client to go to an assigned desktop, this name is the one displayed in Horizon Client. The name must contain only letters, hyphens, and numbers. Spaces are not allowed. The name cannot start with a non-alphabetic character.</td>
</tr>
</tbody>
</table>

On the Users step, search for users and groups in your registered Active Directory domains, select the ones you want to give this session desktop assignment, and then click **Next**.

On the Summary step, review the configuration and then click **Submit**. The system begins the process of configuring the farm's server instances to provide session desktops to the selected users. On the Assignments page, the Status column reflects the current progress.

**Edit an Assignment**

You can change assignment settings such as capacity and assigned users.

**Procedure**

1. On the Assignments page, select the assignment to edit and click **Edit**.
2. Make your changes and click **Submit**.

   **Note**  If you edit the capacity of a desktop assignment, it takes a few minutes for the system to reflect the change.

   For instructions on filling in the fields in the wizard, see the topic for creating the type of assignment you are editing (Create an Application Assignment or Create a Dedicated or Floating VDI Desktop Assignment).
Create a URL Redirection Customization and Assign it to Users

In the Administration Console, you create customization assignments to assign settings that customize your end users' environments. One type of customization is URL redirection. You can define URL handling rules where the Horizon Client redirects URLs from the end user's client machine to a desktop or application provided by your Horizon Cloud environment. A URL redirection configuration gives the Horizon Client information about which URLs should be handled by one of the end user's assigned Horizon Cloud desktops or applications instead of being opened by the user's local system.

**Note**  The Horizon Cloud Administration Console provides a user interface for you to configure client-to-agent URL redirection. To configure agent-to-client URL redirection, you must use group policy settings as described in Configuring Agent-to-Client Redirection. The steps below are for configuring client-to-agent URL redirection.

The Horizon Client fetches an end user's assigned URL redirection rules when the user logs in to the Horizon Client on their local device. Then when that user attempts to open a link in a local document or file and the link matches a URL pattern rule in the assigned settings, Horizon Client determines the appropriate handler to use. The handlers are specified opens the user's assigned desktop or application to handle the URL link, as determined by the appropriate handler you specified in the URL redirection configuration. If the URL redirection handler specifies to use a desktop, the desktop's default application for the link's specified protocol processes the URL. If the handler specifies to use an application, the user's assigned application processes the URL. If the user is not entitled to the desktop or application specified in the handler, Horizon Client displays a message to the user, unless you have specified **Strict Match** as **No** for the handler.

In the scenario where **Strict Match** is set to **No**, the system locates a resource to use based on this fall-back behavior:

1. The system searches the user's assignments using a substring match of the target resource specified for the handler. If the system finds an assignment that matches the substring, that assigned desktop or application is used to open the link.

2. When the handler's **Resource Type** is set to **Application**, if the search for a substring match fails, the system searches the user's application assignments for an assigned application that can handle the protocol specified in the handler's **Scheme** field.

**Note**  This step in the fall-back behavior only applies for applications. If the **Resource Type** is set to **Desktops**, this step is skipped.
If the system cannot locate a resource in the user's assignments that can handle the protocol, Horizon Client displays a message to the user.

Important The user's Horizon Client must be installed with the URL_FILTERING_ENABLED=1 option to give the client the capability to handle the URL redirection feature. For details, see the Installing Horizon Client for Windows with the URL Content Redirection Feature topic in the VMware Horizon 7 documentation.

When your environment is integrated with VMware Identity Manager™, the user must have opened at least one application using Horizon Client before the URL redirection feature can work for that user. By opening at least one application using the **Open in Client** option, the user's assigned URL redirection configuration is loaded into the client device's registry where Horizon Client can get the configuration values.

A customization assignment can be turned inactive by using the **Take Offline** button on the Assignments page. A user can be assigned more than one active customization for URL redirection settings. To avoid potential conflicts between rules from different active configurations, when the user logs in to Horizon Client, the system:

- Sets only one configuration in effect, even when that user has more than one active configuration assigned.
- Uses the URL redirection configuration that is alphabetically first as the configuration in effect for the user.

**Prerequisites**

In the Administration Console, you can create a customization for URL redirection even before you have any desktops or remote applications in your Horizon Cloud inventory. However, before the URL redirection flow works for those end users specified in the customization, the following prerequisites must be met:

- The Horizon agent in the base image used by the farm was installed using the URL_FILTERING_ENABLED=1 parameter on the command line.
- Your Horizon Cloud inventory has the desktops and remote applications that you intend to use in the configuration.
- If the customization has **Strict Match** set to **Yes**, assignments must exist that entitle the specific desktops and remote applications to the end users specified in the customization.

**Procedure**

1. On the Assignments page, click **New**.
2. In the New Assignment window, click the **Customizations** icon.
   - The New Customization Assignment Assignment wizard opens to its first step.
In the Definition step, configure the general settings and then click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignment Name</td>
<td>Enter a friendly name for this assignment.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally enter a description for the configuration.</td>
</tr>
</tbody>
</table>

In the Configuration step’s Source section, create a list of URL patterns that this configuration will tell Horizon Client to intercept on the client system.

4. In the **URL Pattern** field, type a string that specifies the URL matching pattern to be intercepted. You can use wildcards to specify a URL pattern that matches multiple URLs.

   For example:
   - If you type `google.*`, all URLs that include the text `google` are intercepted.
   - If you type `.*` (period asterisk), all URLs are intercepted for all protocol schemes (matches all).
   - If you type `mailto://.*.example.com` all URLs that contain the text `mailto://.*.example.com` are intercepted.

   **Important** You should always consider that the URLs you enter in the **URL Pattern** field are case-sensitive, including the host name part like `docs.vmware.com`. The URL redirection feature behavior is sensitive to the case of the URL patterns you enter here. As an example, if you enter `DOCS.VMWARE.COM/*` as the pattern and the end user clicks a link `https://docs.vmware.com`, the URL redirection does not happen, because the host name exists actually in lowercase. For host names, enter them as lowercase. If you need to match subdirectories in the URL path, use a wildcard or enter those URLs as the path actually exists, such as `docs.vmware.com/en/VMware-Horizon-Cloud-Service/*`

   a. Press Enter to add your specified URL pattern to the list.
   b. Repeat the steps of typing in a pattern and pressing Enter to add more URL matching patterns.
5 In the Rules section, define the set of handlers that determine which target inventory resource should handle various protocols.

A handler defines which of the user's entitled desktops or applications should handle that specific protocol. For example, if the user opens a Microsoft Word document that has a mailto hypertext link and the user clicks on that link in the document, the handler defines what entitled application should handle the request, such as Microsoft Outlook or Mozilla Thunderbird.

a In the Rules section, configure the settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheme</td>
<td>Enter the protocol to which this handler applies, such as http, https, mailto, callto, and so on.</td>
</tr>
<tr>
<td>Resource Type</td>
<td>Select whether a desktop or application is to handle the specified protocol.</td>
</tr>
<tr>
<td>Target Resource</td>
<td>Enter the name of the target resource in your Horizon Cloud inventory that you want handling the protocol specified in the Scheme field.</td>
</tr>
<tr>
<td>Strict Match</td>
<td>Select Yes to force an exact match between the name specified in the Target Resource field and the names of the user's available entitled session desktops or remote applications. Select No if you want the system to use its fall-back behavior to support the situation where an end user does not have an assignment for a resource with the exact name specified in the Target Resource field. For example, when the Resource Type is set to Applications and you specify Microsoft Outlook as the target resource to handle the mailto protocol, but the user does not have an assignment for any Microsoft Outlook applications, when Strict Match is set to No, the system will search for a compatible application assigned to that user to handle the mailto protocol, such as Mozilla Thunderbird.</td>
</tr>
</tbody>
</table>

b To add more handlers, click Add a row and complete the fields.

6 Click Next to proceed to the next wizard step.

7 Search for and select the users and groups for this assignment and click Next.

8 Review the summarized information and click Submit.

**Understanding What URL Content Redirection Is**

Generally speaking, the URL content redirection feature supports redirection from a remote desktop or application to a client, and from a client to a remote desktop or application.
Redirection from a remote desktop or application to a client is called agent-to-client redirection. Redirection from a client to a remote desktop or application is called client-to-agent redirection.

**Agent-to-client redirection**

With agent-to-client redirection, Horizon Agent sends the URL to Horizon Client, which opens the default application for the protocol in the URL on the client machine. For details about configuring agent-to-client redirection in Horizon Cloud, see Configuring Agent-to-Client Redirection.

**Client-to-agent redirection**

With client-to-agent redirection, Horizon Client opens a remote desktop or remote application that you specified to handle the URL. For details about configuring client-to-agent redirection in Horizon Cloud, see Create a URL Redirection Customization and Assign it to Users.

You can redirect some URLs from a remote desktop or application to a client, and redirect other URLs from a client to a remote desktop or application. You can redirect any number of protocols, including HTTP, HTTPS, mailto, and callto.

### Configuring Agent-to-Client Redirection

With agent-to-client redirection, Horizon Agent sends the URL to Horizon Client, which opens the default application for the protocol in the URL.

To enable agent-to-client redirection, perform the following configuration tasks.

- Ensure the URL content redirection feature is enabled in Horizon Agent in the master image VM, as described in the prerequisites section in Create a URL Redirection Customization and Assign it to Users.
- Apply the URL Content Redirection group policy settings to your remote desktops and applications. See Add the URL Content Redirection ADMX Template to a GPO.
- Configure group policy settings to indicate, for each protocol, how the Horizon Agent should redirect the URL. See URL Content Redirection Group Policy Settings.

### Add the URL Content Redirection ADMX Template to a GPO

The URL Content Redirection ADMX template file, called urlRedirection.admx, contains settings that enable you to control whether a URL link is opened on the client (agent-to-client redirection) or in a remote desktop or application (client-to-agent redirection).

To apply the URL Content Redirection group policy settings to your remote desktops and applications, add the ADMX template file to GPOs on your Active Directory server. For rules regarding URL links clicked in a remote desktop or application, the GPOs must be linked to the OU that contains your virtual desktops and RDS hosts.

You can also apply the group policy settings to a GPO that is linked to the OU that contains your Windows client computers, but the preferred method for configuring client-to-agent redirection is to use the vdmutil command-line utility. Because macOS does not support GPOs, you must use vmdutil if you have Mac clients.
Prerequisites

- Verify that the URL content redirection feature is included when Horizon Agent is installed in the master image VM, as described in Create a URL Redirection Customization and Assign it to Users.
- Verify that Active Directory GPOs are created for the URL Content Redirection group policy settings.
- Verify that the MMC and the Group Policy Management Editor snap-in are available on your Active Directory server.

Procedure

1. Download the Horizon 7 GPO Bundle ZIP file from the VMware download site at my.vmware.com/web/vmware/downloads.
   The file has a name in the form VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip where x.x.x is the version and yyyyyyy is the build number. All ADMX files that provide group policy settings for the product are available in this file.

2. Unzip that ZIP file and copy the URL Content Redirection ADMX file to your Active Directory server.
   a. Copy the urlRedirection.admx file to the C:\Windows\PolicyDefinitions folder.
   b. Copy the urlRedirection.adml language resource file to the appropriate subfolder in C:\Windows\PolicyDefinitions.
      For example, for the EN locale, copy the urlRedirection.adml file to the C:\Windows\PolicyDefinitions\en-US folder.

3. On your Active Directory server, open the Group Policy Management Editor.
   The URL Content Redirection group policy settings are installed in Computer Configuration > Policies > Administrative Templates > VMware Horizon URL Redirection.

What to do next

Configure the group policy settings in your Active Directory server. For descriptions of the settings, see URL Content Redirection Group Policy Settings.

URL Content Redirection Group Policy Settings

The URL Content Redirection template file contains group policy settings that enable you to create rules for configuring the agent-to-client redirection capability for your Horizon Cloud environment. The template file contains only Computer Configuration settings. All of the settings are in the VMware Horizon URL Redirection folder in the Group Policy Management Editor.

Important Even though the URL Content Redirection template file contains group policy settings related to client-to-agent redirection, you do not use group policy settings to configure client-to-agent redirection in Horizon Cloud. In Horizon Cloud, you use the Administration Console to create the rules for client-to-agent redirection. You create rules for client-to-agent redirection when you create a URL redirection assignment in the Administration Console. For detailed steps, see Create a URL Redirection Customization and Assign it to Users.
The following table describes the group policy settings available in the URL Content Redirection template file.

**Table 6-1. URL Content Redirection Group Policy Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>IE Policy: Prevent users from changing URL Redirection plugin loading behavior</td>
<td>Determines whether users can disable the URL Content Redirection feature. This setting is not configured by default.</td>
</tr>
<tr>
<td>IE Policy: Automatically enable URL Redirection plugin</td>
<td>Determines whether newly installed Internet Explorer plug-ins are automatically activated. This setting is not configured by default.</td>
</tr>
<tr>
<td>Url Redirection Enabled</td>
<td>Determines whether the URL Content Redirection feature is enabled. You can use this setting to disable the URL Content Redirection feature even if the feature has been installed in the client or agent. This setting is not configured by default.</td>
</tr>
</tbody>
</table>
Table 6-1. URL Content Redirection Group Policy Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Properties</th>
</tr>
</thead>
</table>
| **Url Redirection Protocol 'http'** | For all URLs that use the HTTP protocol, specifies the URLs that should be redirected. This setting has the following options: ▪ brokerHostname - IP address or fully qualified name of the Connection Server host to use when redirecting URLs to a remote desktop or application. ▪ remoteItem - display name of the remote desktop or application pool that can handle the URLs specified in agentRules. ▪ clientRules - the URLs that should be redirected to the client. For example, if you set clientRules to *.mycompany.com, all URLs that include the text mycompany.com are redirected to the Windows-based client and are opened in the default browser on the client. ▪ agentRules - the URLs that should be redirected to the remote desktop or application specified in remoteItem. For example, if you set agentRules to *.mycompany.com, all URLs that include mycompany.com are redirected to the remote desktop or application. When you create agent rules, you must also use the brokerHostname option to specify the IP address or fully qualified domain name of the Connection Server host, and the remoteItem option to specify the display name of the desktop or application pool.  

**Note**  The preferred method for configuring client rules is to use the vdmutil command-line utility.  

This setting is enabled by default. |
| **Url Redirection Protocol '...']'** | Use this setting for any protocol other than HTTP, such as HTTPS, email, or callto.   
The options are the same as for Url Redirection Protocol 'http'.   
If you do not need to configure other protocols, you can delete or comment out this entry before adding the URL Content Redirection template file to Active Directory.   
As a best practice, configure the same redirection settings for the HTTP and HTTPS protocols. That way, if a user types a partial URL into Internet Explorer, such as mycompany.com, and that site automatically redirects from HTTP to HTTPS, the URL Content Redirection feature will work as expected.   
In this example, if you set a rule for HTTPS but do not set the same redirection setting for HTTP, the partial URL that the user types is not redirected.  
This setting is not configured by default. |

Edit Assignment Mode

You can take assignments offline for maintenance and bring them back online using the Edit Assignment Mode setting. Setting an Assignment to offline mode will prevent users from logging into the assignment desktops/applications. The setting also allows you to configure a custom maintenance notice for the assignment.
You can perform the following tasks using the Edit Assignment Mode setting.

- Take an assignment offline:
  a. On the Assignments page, select the assignment and click the **Edit Assignment Mode** button at the top of the page.
     
     The Edit Assignment Mode dialog appears.
  b. Change the Assignment Mode setting to Offline.
  c. Click **Save**.

- Bring an assignment online:
  a. On the Assignments page, select the assignment and click the **Edit Assignment Mode** button at the top of the page.
     
     The Edit Assignment Mode dialog appears.
  b. Change the Assignment Mode setting to Online.
  c. Click **Save**.

### Update Agent Software for an Assignment

Use the Update Agent Software feature to update the Horizon Agent Installer for Dedicated Desktop - Traditional Clone assignments.

**Note** You can also update agent software for a Dedicated Desktop - Instant Clone assignment by updating the image and pushing changes to the assignment. This process is described in Update Agent Software for an Image.

At a high level, the system's agent update capability works as follows:

- The system makes regular contact with the VMware CDS software distribution network to see if a new version of the Horizon Agents Installer is available. It downloads the new version to a file share that you have set up on a local machine. The update file is then automatically imported into the system and made available to assignments.

- After a new version is downloaded, the Assignments page reflects that an update is available. A visual indicator is displayed for those dedicated VDI desktop assignments that have the agent-related software at a level prior to the new version.
You select the dedicated VDI assignment and start the agent update wizard. Besides selecting the agent version, in the agent update wizard, you can optionally specify the following items.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available VMs to Users</td>
<td>Use this field to specify a percentage of the assignment's VMs to keep available for users during the update.</td>
</tr>
<tr>
<td></td>
<td>By default, the system marks all of the desktops for maintenance as the update starts. You can use this field to ensure a higher percentage of a small-sized pool is available as the system goes through and updates the desktops. Setting a higher availability percentage results in an adjustment to the number of desktops currently marked for maintenance.</td>
</tr>
<tr>
<td>Skip VMs with Logged-In User</td>
<td>Have the system skip updating VMs that have a logged-in user, a session that is either active or disconnected. This setting avoids the system's default behavior of forcing end users off their desktop when the update process starts on that desktop.</td>
</tr>
<tr>
<td>Retry Skipped VMs and Job Timeout</td>
<td>When you have the system skip updating VMs that have a logged-in user, you can optionally specify whether to have the system automatically retry updating any skipped VMs. In this case, after the system has gone through the assignment's desktop VMs and updated those VMs without logged-in users, the system:</td>
</tr>
<tr>
<td></td>
<td>1 Checks the ones that it initially skipped to see if those VMs have logged-in users.</td>
</tr>
<tr>
<td></td>
<td>2 Updates any of the skipped VMs which have no logged-in users.</td>
</tr>
<tr>
<td></td>
<td>3 Periodically repeats steps 1 and 2 until the time specified in the Job Timeout field has elapsed.</td>
</tr>
<tr>
<td></td>
<td>If you do not have the system automatically retry the skipped VMs, you can manually take care of those VMs later.</td>
</tr>
<tr>
<td></td>
<td>Important VMs that encounter an error during the update process are not retried. For a failed update, the VM rolls back to the agent version that it had before the update process started.</td>
</tr>
</tbody>
</table>

After you submit the update task in the wizard’s last step, the system begins updating the desktops in the assignment. When updating the assignment, the system updates a batch of VMs in parallel. By default, the system uses 30 VMs for each batch until the remaining number of VMs to update is less than 30. At that point, that final set is for updating those remaining VMs. It takes approximately 30 minutes to fully update a VM. The batch size cannot be larger than 30. If the assignment has 30 or fewer desktops, all desktops in the assignment are updated together. Your VMware representative can adjust the batch size if you request it.

The number of in-progress VMs depends on whether you specified to have a percentage of the VMs to be kept available during the update. When you set an availability percentage, the system adjusts the set of in-progress VMs to meet the availability percentage.

At the end of the agent update process, the assignment's summary page lists the version of the Horizon Agents Installer that is in effect.
During the time the system is updating the desktops, the desktops’ end users encounter the following behaviors:

- If a desktop has an active session and you kept No for Skip VMs with Logged-In User, that user is warned five minutes before the update occurs. This five-minute warning is to give the user time to save any in-progress work.
- If a user attempts to log in to a desktop that is being updated, the login is unsuccessful and the user receives a message that the desktop is not yet available.

Upon request, your VMware representative can make the following adjustments in your environment:

- Adjust the interval between scans for new Horizon Agents Installer versions.
- Adjust the wait time for scans after tenant startup.
- Adjust the default batch size from 30.
- Set your system to restart VMs before installing agents.

**Prerequisites**

- You must have created an Agents file share and added it to Horizon Cloud. This means that you select Agents for the file share type when you create the file share. Agents file shares are used only for importing Horizon Agents Installer files. See Managing File Shares.
- The assignment must already have DaaS Agent 17.1.0.5232563 or later and Horizon Agent 7.3.2.7161471 or later installed.

**Procedure**

1. **Click Assign.**

   The Assignments page displays, with a blue dot appearing next to the name of any assignment that has an Horizon Agents Installer update available. If you hover over a blue dot, a popup displays indicating the new version of the Horizon Agent Installer available for that assignment.

2. **Select the check boxes for one or more assignments.** By selecting multiple assignments, you can update all of them to a common Horizon Agents Installer versions.

3. **Click Update Agent Software.**

   The Agent Update dialog displays.
4 In the Software step, select the update version you want to use from the drop-down list.

5 In the Available VMs to Users field, specify the percentage of desktop VMs in the assignment that you want powered on and available to end users during the upgrade process.

   **Note** If you do not need desktops available, type a zero (0). You must specify a value for Available VMs to Users, even when you do not care about having desktop VMs available to users during the update process.

6 (Optional) To have the system skip those desktops that have logged-in users, set the Skip VMs with Logged-In User toggle to Yes.

   When that toggle is set to Yes, the Retry Skipped VMs toggle appears.

7 (Optional) To have the system automatically retry any of skipped VMs, set the Retry Skipped VMs toggle to Yes.

   When the Retry Skipped VMs toggle is set to Yes, the Job Timeout field appears.
8  (Optional) In the **Job Timeout** field, specify the time period over which you want the system to continue automatically trying to update the skipped VMs.

The Job Timeout field sets the number of minutes that the system retries updating the skipped VMs. Every 30 minutes, the system tries to update the skipped VMs until it reaches the end of this time period or until all of the assignment's desktop VMs have been updated.

You can enter a value that ranges from 240 minutes (4 hours) to 1440 minutes (24 hours). The default value is 720 minutes (12 hours).

**Note** VMs that encounter an error during the update process are not retried. For a failed update, the VM rolls back to the agent version that it had before the update process started.

9  Click **Next**.

10  (Optional) On the Command Line tab, add any command line options.

11  Click **Finish**.

- A message displays at the top of the page indicating that the update has started.
- The system updates the agent-related components on the desktop VMs in the dedicated VDI desktop assignment.
- At the end of the agent update process, the assignment's summary page lists the version of the Horizon Agents Installer that is in effect.

You can view the progress of the update task by selecting **Monitor > Activity**. The task description indicates the update being performed and the assignment on which it is being performed. If the task is not completed successfully within 24 hours, and the retry and job timeout options are not in effect, the update task is shown in failure status.

If any VMs are skipped in the update task, the update task has Partial Success status on the Activity page. In the Activity page, you can see how many VMs are skipped in the update task. If you have a number of skipped VMs at the end of the update task even though the retry option was set to **Yes**, either the Job Timeout value was not long enough for the system to get to all of the skipped VMs or the end users never logged out of those VMs.

### Delete an Assignment

You can delete assignments if they are no longer needed.
Prerequisites

An assignment can be deleted only if it contains no virtual machines.

- To delete a dedicated desktop assignment, first delete the virtual machines from the Assignment page.
- To delete any other type of assignment, first set the assignment size to zero.

Procedure

1. Select the assignment to delete and click Delete.
2. Click Delete in the confirmation dialog box to permanently delete the assignment.

Recover an Assignment

You can recover desktops that encountered an error during a previous image update.

**Note** This operation is available for Instant Clone desktops only.

Procedure

1. Select the assignment to recover.
2. Click Recover.

Manage Desktops in a Dedicated or Floating Desktop Assignment

You can manage desktops in dedicated and floating desktop assignments.

**Note** For session desktop assignments, the assignments are only used for entitling access to the RDS-based desktop, and not for management of the desktops. To manage session desktops, you manage the servers and sessions in the underlying farm. See Managing Farms in Horizon Cloud.

Procedure

1. Click the Assign icon.
   
   The Assignments page displays.
2. Click the name of an assignment on the list.
   
   The assignments details page displays.
3. Click Desktops at the top of the page.
   
   The Desktops tab displays, showing a list of desktops for the assignment. You can filter, refresh, and export the list using the controls to the top right of the page.
   
   You can perform the following actions by clicking one of the buttons at the top of the page.

   **Note** Desktop status must be green to perform these actions.
Option | Description
---|---
Shutdown | Shuts down the desktop(s).
- You can select more than one desktop at a time.
- You can only shut down VMs that do not have active user sessions.

Restart | Performs a ‘graceful’ restart of the VM(s). You can select more than one desktop at a time.
If this does not work, it may be necessary to use the Reset option (see below).

Assign | [Dedicated desktop only] Assigns dedicated desktop to a particular user. Click the button and then search for the user in the Active Directory.

You can perform the following actions by clicking the "..." button and making a selection from the drop-down menu.

Option | Description
---|---
Migrate VM(s) | [Dedicated desktop only] Migrates VM(s) to another dedicated desktop assignment.
- Selected VM(s) must meet the following requirements:
  - Have all users logged off.
  - Be domain joined.
  - Have no tasks running.
  - Have the same domain, OU, and graphics settings as the target assignment.
- To rename the VM, select the Rename VM option. During migration VM will be renamed as per target pool naming convention.
- View migration progress and status in Monitor > Activity.
- In case of a post relocate customization task failure (during VM migration across DMs), select the VM and choose the ‘Rectify’ option from the dropdown to fix a VM in an inconsistent state.
- VM can be located either on the Imported VMs page or under the target assignment.
Note the following:
- VMs can be moved between dedicated assignments on same or different Desktop Managers.
- VMs cannot be moved between assignments on different vCenters.

Rename | [Dedicated desktop only] Renames the selected desktop.

Unassign | [Dedicated desktop only] Unassigns the selected desktop from user.

Delete | [Dedicated desktop only] Deletes the selected desktop.

Suspend | Suspends the selected desktop(s). You can select more than one desktop at a time.

Resume | Resumes operation of the selected desktop(s). You can select more than one desktop at a time.

Power On | [Traditional clone only] Powers on the selected desktop(s). You can select more than one desktop at a time.

Power Off | [Traditional clone only] Powers off the selected desktop(s). You can select more than one desktop at a time.

Reset Agent Pairing | Repairs the agent pairing state when pairing failure has occurred.
- You can select multiple VMs. The action will only be applied to those selected VMs that are currently powered on.
- You can view progress on the Monitor > Activity page or on the System Activity tab of the assignment's detail page.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Launch Console</td>
<td>Launches a console for the selected desktop. This option is disabled if the VM is powered off or if more than one VM is selected.</td>
</tr>
<tr>
<td>Reset</td>
<td>Performs a hard reset of the VM(s). You can select more than one server at a time. In the case of a hung VM, it is recommended that you first try using the Restart option (see above).</td>
</tr>
<tr>
<td>Log Off</td>
<td>Logs the currently connected user off the selected desktop.</td>
</tr>
<tr>
<td>Disconnect</td>
<td>Disconnects the currently connected user from the selected desktop.</td>
</tr>
<tr>
<td>Rectify</td>
<td>[Floating desktop traditional clone only] Deletes and recreates the selected desktop. Use this option for desktop VMs that have become corrupted or otherwise non-operational.</td>
</tr>
<tr>
<td>Convert to Image</td>
<td>Converts the selected desktop to an image.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You cannot convert a VM to an image if it is currently being used as an appliance.</td>
</tr>
<tr>
<td>Generate Logs</td>
<td>Generates logs for the image VM. If you have configured a VMs file share, the system places log files in that file share. For more information, see Managing File Shares.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This feature requires Horizon Agent Installer 19.1 or higher.</td>
</tr>
</tbody>
</table>

**View Activity or Cancel Tasks for Assignments**

You can use an assignment's details page to view system or user activity for dedicated and floating desktop assignments. You can also view session activity for a native application assignment.

Use these steps to view system or user activity for dedicated desktop and floating desktop assignments, and session activity for native application assignments.

**Note** For session desktop assignments, you view the system and user activity using the details page for the underlying farm. See Managing Farms in Horizon Cloud for details.

**Procedure**

1. Click the **Assign** icon.

   The Assignments page displays.

2. Click the name of an assignment on the list.

   The assignments details page displays.

3. Click one of the options, depending on whether the assignment is a dedicated desktop, floating desktop, or a native application assignment.

   - For a dedicated desktop or floating desktop assignment, click **System Activity** or **User Activity**.

     The activity tab displays, showing a list of recent activity for the assignment. You can select from the Shown drop-down menu to adjust the time frame for the list, or filter, refresh, and export the list using the controls on the top right of the page.
On the System Activity tab, you can cancel assignment-related tasks before they complete by selecting the task in the list and clicking the **Cancel** button.

- Before attempting to select a task for cancellation, refresh the view to update the status for the tasks displayed.
- If a task is currently able to be cancelled, you will be able to select the corresponding check box in the task list. If you select the 'select all' check box at the top of the list, all tasks that can currently be cancelled are selected.

The table below shows tasks that you can cancel.

<table>
<thead>
<tr>
<th>Task</th>
<th>Cancel When Task is in Queued State</th>
<th>Cancel When Task is in Running State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Farm Expansion</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Assignment Expansion</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Convert VM to Image</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Rebuild VM</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Push Updates</td>
<td>Supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>

- **Note** When the system has automatically created an expansion task for an RDSH farm, the farm must be offline before you can cancel that task.
- **Note** When the system has automatically created an expansion task for a VDI desktop assignment, the assignment must be offline before you can cancel that task.
- **Note** If you cancel this task, and wish to retry it, first confirm that the VM is in a state where it can be converted. If you are not sure, power off and then power on the VM.
- **Note** If you cancel this task, and wish to retry it, first confirm that the VM is in a state where it can be converted. If you are not sure, power off and then power on the VM.

- For a native application assignment, click **Sessions**.

### Working with Nested Organizational Units

Add desktops to a nested Organization Unit (OU).

When you create a desktop assignment, you can specify a domain OU in the Computer OU field. You cannot specify a nested OU. You must locate the nested OU information, then manually enter it in the Computer OU field.

**Procedure**

1. Open **Active Directory Users and Computers**.
2. Select **View > Advanced features (Enabled Advanced features)**.
3. Navigate to the Organizational Unit where the desktops will be placed.
4 Right-click and select Properties.

5 Click the Attribute editor and select distinguishedName.

6 Click View.

7 Enter the distinguished name information in the Computer OU field on the Desktop Assignment page.
   Only the OU= part of the string is required. The DC= part is optional.
The Applications page shows all of the applications available for assignments.

Click the **Inventory** icon and select **Applications** to access the Applications page.

There are two types of applications:

- Remote applications are those imported from an RDS farm. You add third-party user applications to the RDS image before publishing that image to Horizon Cloud. You can either automatically scan your farms to add their applications to your applications inventory or manually add applications from the farm.

- Custom applications are applications in the RDS farms' servers that you manually add into the inventory by using the **New** button on the Applications page and the **Manually from Farm** choice. Even though the best practice is to use the automated way, the manual method can be useful for some unique situations, such as for adding applications that are invoked from the command prompt or which cannot be auto-detected in a Windows operating system.

You can take the following actions on the Applications page.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Add a Remote or Custom Application.</td>
</tr>
<tr>
<td>Edit</td>
<td>Select an application to make changes.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete an application.</td>
</tr>
<tr>
<td>Rename</td>
<td>Rename an application.</td>
</tr>
</tbody>
</table>

This chapter includes the following topics:

- Importing New Applications from an RDSH Farm Using Auto-Scan from Farm
- Manually Adding Custom Applications from an RDSH Farm
- Edit an Application
- Delete an Application
- Rename an Application
- Hide an Application
- Unhide an Application
Importing New Applications from an RDSH Farm Using Auto-Scan from Farm

You make remote applications available for user assignments by importing them from an RDSH applications farm.

If you have more than one applications farm in your environment, repeat these steps to import the applications you want from each of those farms.

Prerequisites

Verify that you have at least one applications farm in your inventory by navigating to Inventory > Farms.

Procedure

1. On the Applications page, click New.

2. In the start screen, click Auto-Scan from Farm.

   The wizard opens to its first step.

3. Select the applications farm and click Next to proceed to the next step.

   When you click Next, the system scans the selected farm for applications and then displays them for you to select.

4. Select the applications that you want to add to your application catalog.

   This wizard step displays the applications that the system's auto-scan process found in the RDS-enabled Windows server operating system used for the farm's RDS servers.

5. Click Next to proceed to the next wizard step.

6. (Optional) Customize some of the configurable options for the applications you selected, and then click Next to proceed to the next wizard step.

7. Review the summary and click Submit.

   The system adds the selected applications to the application catalog in your Horizon Cloud inventory.
What to do next
Repeat the steps to import the applications you want from your other farms.

Manually Adding Custom Applications from an RDSH Farm

Some applications cannot be automatically detected by scanning the farm. You can manually add those applications to your Horizon Cloud applications catalog.

If you have more than one such application, repeat these steps to add the applications you want.

Prerequisites
Verify that you have at least one applications farm in your inventory by navigating to Inventory > Farms.

Procedure
1. On the Applications page, click New.

2. In the start screen, click Manually from Farm.

3. In the Properties section, specify the following values.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the application.</td>
</tr>
<tr>
<td>Display Name</td>
<td>Name for the application that you want displayed to end users when they see the application in their clients, such as in Horizon Client or Workspace ONE.</td>
</tr>
<tr>
<td>Pod</td>
<td>This option only displays if your data center is configured with multiple pods. Select a pod to filter the set of farms displayed in the Farm list.</td>
</tr>
<tr>
<td>Farm</td>
<td>Select the farm that has the RDSH server VM from which you want to add the application.</td>
</tr>
<tr>
<td>Application Path</td>
<td>Specify the path to the application in the RDSH server VM's operating system.</td>
</tr>
<tr>
<td>Icon File</td>
<td>Optional: Upload a PNG file (32 x 32 pixels) to use as the application's icon.</td>
</tr>
</tbody>
</table>
4 In the Advanced Properties section, specify these optional settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application available on Farm</td>
<td>Select Yes to have the system validate the application path. If the application is not located on the farm at that path, select No so that the system does not attempt to look for the application. For example, if an application is stored in the local directory in the server VM, you would select No so that the system does not try to find the application there.</td>
</tr>
<tr>
<td>Version</td>
<td>Optional: Version number of the application</td>
</tr>
<tr>
<td>Publisher</td>
<td>Optional: Publisher of the application</td>
</tr>
<tr>
<td>Start Folder</td>
<td>Specify the location in the RDS server VM's Windows operating system that you want the remote application to use as its start folder.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you specify a LNK file in the Application Path that specifies its own start directory, the system does not use the location specified here.</td>
</tr>
<tr>
<td>Parameters</td>
<td>Specify any command line parameters you want used when the remote application is launched.</td>
</tr>
</tbody>
</table>

5 Click Submit.

The system adds an entry for the application to the Applications page.

**What to do next**

Repeat the steps for any applications you want from your other farms.

### Edit an Application

You can use the following procedure to edit an application.

**Procedure**

1 Select an application on the Applications page and click the Edit button at the top of the page.

   The Edit Application dialog appears.

2 Edit information as described below.

   **Note** Some items are not editable.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the application</td>
</tr>
<tr>
<td>Display Name</td>
<td>Name for the application that you want displayed to end users when they see the application in their clients, such as in Horizon Client or the browser using Horizon HTML Access.</td>
</tr>
<tr>
<td>Pod</td>
<td>This option only displays if your data center is configured with multiple pods. Displays the name of the pod where the farm is located.</td>
</tr>
<tr>
<td>Farm</td>
<td>The farm that was specified when the application was added into your inventory.</td>
</tr>
</tbody>
</table>
**Field** | **Description**
--- | ---
**Application Path** | Location of the application executable on the VM (for example, Z:\Customapps\app.exe) or UNC-specified path (for example, \fileserver.accounting.com\vol1\software\app.exe)
**Icon File** | .png file (32 x 32 pixels) to use as application’s icon. [optional] Click Choose File to browse for file.
**Application available on Farm** | This option reflects the choice that was specified when the application was added into your inventory.
**Version** | Version number of application [optional]
**Publisher** | Publisher of application [optional]
**Start Folder** | Specify the location in the RDS server VM’s Windows operating system that you want the remote application to use as its start folder.
*Note* | If you specify a LNK file in the Application Path that specifies its own start directory, the system does not use the location specified here.
**Parameters** | Specify any command line parameters you want used when the remote application is launched.

3 Click **Save**.

**Delete an Application**

You can use the following procedure to delete an application.

**Procedure**

1 Select an application on the Applications page and click the Delete button at the top of the page.

   The confirmation dialog appears.

2 Click **OK** to confirm delete.

**Rename an Application**

You can use the following procedure to rename an application.

**Procedure**

1 On the Applications page, select an application and click the **Rename** button at the top of the page.

   The Rename dialog appears.

2 Enter the new name and click **Save**.

   The new application name appears in the list.
Hide an Application
You can use the following procedure to hide (disable) an application on the Applications page.

**Note**  This does not delete the application from the system, but only disables it. The application is moved from the list of visible (enabled) to the list of hidden (disabled) applications. To delete an application, use the Delete function.

**Procedure**
1. Select an application on the Applications page.
2. Click the **Hide** button at the top of the page.
   - The application is disabled and is moved to the hidden applications list.

Unhide an Application
You can use the following procedure to unhide (re-enable) an application on the Applications page.

**Procedure**
1. Select **Hidden** in the Show filter at the top of the Applications list.
   - The view switches from a list of visible (enabled) to a list of hidden (disabled) applications.
2. Select the application and click **Unhide**.
   - The application is re-enabled and moved to the visible (enabled) applications list.
Images

Images are patterns that you use to create assignments.

About Images

Images are created from template VMs that are configured for the needs of various types of users. You can:

- Receive a pre-packaged image from VMware.
- Create an image from a template you receive from VMware.
- Create an image from your own template.

Image Types

There are two types of images, as described below.

<table>
<thead>
<tr>
<th>Image Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instant Clone</td>
<td>Image type that uses VMware's NGVC technology to create VMs instantly for an assignment.</td>
</tr>
<tr>
<td>Traditional Clone</td>
<td>Proprietary image type that does full image cloning when creating assignments</td>
</tr>
</tbody>
</table>

The image type is selected when the image is first created.

The Images Page

To view images currently in your system, select Inventory > Images to display the Images page.

This chapter includes the following topics:

- Managing Images
- Create an Image
- Update Agent Software for an Image
- Build Your Own Template

Managing Images

The Images page lists all images currently in the system. The actions you can perform on this page are described below.
There are two ways to perform actions on images.

- Select the check box for an image in the list and use the buttons and menu selections at the top of the page as described below.
- Click on an image to view the image detail page and use the buttons and menu selections at the top of that page. Only some of the options below are available on the image detail page, and they appear in different order.

The image detail page also has options to perform a rollback or delete a backup. See Backup Now below for more information.

You can perform the following actions using buttons at the top of the Images page.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Begin the image creation process. See Create an Image.</td>
</tr>
<tr>
<td>Rename</td>
<td>Renames the selected image.</td>
</tr>
<tr>
<td>Duplicate</td>
<td>Creates a duplicate of the selected image. The duplicate image will appear in Imported VMs when complete.</td>
</tr>
<tr>
<td>Update Agent</td>
<td>Updates agent(s) for a selected image. See Update Agent Software for an Image.</td>
</tr>
</tbody>
</table>

You can perform the following actions by clicking the "..." button at the top of the Images page and making a selection from the drop-down menu.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Now</td>
<td>[Traditional Clone images only] Creates a backup of the selected image. After you create and name the backup, it appears under Backups on the image detail page. Next to each backup shown on the image detail page there are options to roll back to that backup or to delete it from your system. Note If a backup that was previously listed on the image detail page does not appear, and you have not deleted it, contact your VMware representative to remedy this issue.</td>
</tr>
<tr>
<td>Delete</td>
<td>Permanently deletes the selected image.</td>
</tr>
<tr>
<td>Publish</td>
<td>Publishes the selected image. Note Graphics settings for Instant Clone images and VMs should be made before publishing the image. This includes number of displays, video RAM size, and enabling 3D support.</td>
</tr>
<tr>
<td>Convert to Desktop</td>
<td>Converts the selected image to a desktop.</td>
</tr>
<tr>
<td>Assign Image</td>
<td>[Instant Clone images only] Pushes updates to dedicated desktop and floating desktop assignments using the selected image. Select the assignment(s) from the list and click OK to push the updates.</td>
</tr>
<tr>
<td>Bulk Assign Image</td>
<td>Assigns the image to multiple assignments/farms of the immediate parent image (the image from which the selected image was duplicated/updated). In the Bulk Assign Image dialog, select assignments/farms in the list and click Update. Note This option is only available for images created using the Duplicate operation and images updated to newer agent versions using the Update Agent operation.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Take Offline</td>
<td>Takes the selected image offline. The image cannot be used to make new assignments or to provision new desktops or servers for existing assignments. If you take an image offline, you must republish it to make it available for assignments.</td>
</tr>
<tr>
<td>Push Updates</td>
<td>Pushes updates to assignments using the selected image.</td>
</tr>
<tr>
<td></td>
<td>- Desktop images - Click <strong>Push Updates</strong>, select the assignment(s) from the list and click <strong>OK</strong> to push the updates.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Before you push updates to your existing assignments, it is recommended that you first create a test assignment and push updates to it in order to confirm that all features are working as expected.</td>
</tr>
<tr>
<td></td>
<td>- RDS images</td>
</tr>
<tr>
<td></td>
<td>- If you updated the image using the Update Agent Software function, click <strong>Push Updates</strong>, select the farm from the list and click <strong>OK</strong> to push the updates.</td>
</tr>
<tr>
<td></td>
<td>- If you updated the image but did not use the Update Agent Software function, no action is needed. The updates are pushed automatically when you re-publish an updated image.</td>
</tr>
<tr>
<td>Reset Agent Pairing</td>
<td>Repairs the agent pairing state when pairing failure has occurred. This option is enabled when the image is in an error or offline state.</td>
</tr>
<tr>
<td>Launch Console</td>
<td>Launches a console for the VM associated with the selected image. This option is disabled if the VM is powered off or if more than one image is selected.</td>
</tr>
<tr>
<td>Generate Logs</td>
<td>Generates logs for the image VM. If you have configured a VMs file share, the system places log files in that file share. For more information, see Managing File Shares.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This feature requires Horizon Agent Installer 19.1 or higher.</td>
</tr>
<tr>
<td>Download Bootstrap</td>
<td>Downloads an encrypted bootstrap file for you to deploy to your image(s).</td>
</tr>
<tr>
<td></td>
<td>You will be prompted to enter a password of 8-20 ASCII characters containing at least one each of the following: lowercase letter, uppercase letter, number, and symbol (!@#$%^&amp;*). Do not use non-ASCII characters in the password.</td>
</tr>
<tr>
<td>Refresh Password</td>
<td>Creates a new default password to be used for bootstrapping images.</td>
</tr>
<tr>
<td></td>
<td>If you do this after having downloaded a bootstrap file but before applying the bootstrap file using keytool, then the resultant agents will not be able to pair. Therefore, it is recommended that you download the bootstrap file again after refreshing the password.</td>
</tr>
</tbody>
</table>

### Update an Instant Clone Image

You can update an Instant Clone image and the assignments based on the image.

Unlike a Traditional Clone image that can be updated after being published (take offline, make changes, and republish), an Instant Clone image must be duplicated and the new image updated and added to the relevant assignments.

**Note** Graphics settings for Instant Clone images and VMs should be made before publishing the image. This includes number of displays, video RAM size, and enabling 3D support.

**Procedure**

1. Select **Inventory > Images** from the menu to open the Images page.
2. Select the check box for the image, click the "..." button, and select **Duplicate** from the drop-down menu.

   The system creates a duplicate of the image.

   **Note**  This process can take some time, so plan accordingly.

3. Make the necessary changes to the duplicate image and publish it.

4. When the new image has been published, edit each of the assignments based on the original image so that they use the duplicate image instead. See **Edit an Assignment**.

   As users log out of their sessions, the VMs in each assignment will be synced with the new image.

5. [Optional] Delete the original image by selecting it on the Images page, clicking the "..." button, and selecting **Delete** from the drop-down menu.

### Automatically Sync Images Across Desktop Managers

If you have multiple Desktop Managers registered to a Tenant within the same Data Center, the Image Sync option can automatically sync images across the desktop managers.

Image Sync is disabled by default, and can be enabled/disabled for each Tenant by your VMware representative.

When enabled, Image Sync automatically does the following.

- Duplicates new images across Desktop Managers, so you do not have to manually clone and import the images.

- Syncs changes to images across Desktop Managers, so you do not have to make the changes on all copies.

**Note** the following:

- Images that you created before Image Sync is enabled will not be automatically synced. You will have to take them offline and then republish them for the sync to occur.

- If you have synced images and then have the feature disabled, for each of the synced images an additional image will appear in the list with a name similar to the synced image.

### Create an Image

Create a new desktop image from the Images page.

**Note**  This process takes approximately 30 minutes. Be sure you allow sufficient time to complete it before you begin.

#### Procedure

1. Select **Inventory > Images**.

   The Images page displays.
2 Click **New**.

The New Image dialog displays.

3 In the Desktop field, start typing the first few letters of the template name.

All desktops that can be converted to an image will display. Note that it takes approximately five minutes after the template import for the inventory to display.

4 Select the desktop name when it appears.

   **Note** Make sure that the desktop is powered on prior to conversion.

5 Confirm that the Agent Status has changed to Active, indicating that agent pairing has occurred. This should happen within approximately 30 seconds.

   **Note** You must have the most recent agents installed for agent pairing to succeed. If you are using older versions of the agents, ensure that the DaaS Agent is manually configured and bootstrapped for agent pairing to complete.

6 For Instant Clone, select **Yes** to create an Instant Clone image or **No** to create a Traditional Clone image. For information about types of images, see Chapter 8 Images.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instant Clone</td>
<td>Image type that uses VMware's NGVC technology to create VMs instantly for an assignment.</td>
</tr>
</tbody>
</table>

   **Note** Windows Server operating systems are not supported for Instant Clone assignments, so you should not create Instant Clone images from Windows Server template VMs. Although the image can be created with the Instant Clone Agent installed and desktops can be provisioned from it, the desktops will not launch successfully for users.

| Traditional Clone | Proprietary image type that does full image cloning when creating assignments. |

7 Enter the required information as described below.

The image type you selected above affects the fields that display.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Name</td>
<td>Name for the new image</td>
</tr>
<tr>
<td>Domain</td>
<td>[Instant Clone only] Select domain from the drop-down list</td>
</tr>
<tr>
<td>Company Name</td>
<td>Your company name</td>
</tr>
<tr>
<td>TimeZone</td>
<td>Your time zone</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Username</td>
<td>Admin user for required desktop domain</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This field displays for Instant Clone images only if your VMware representative has enabled the Image Sync feature.</td>
</tr>
<tr>
<td>Password/Verify Password</td>
<td>Password for the Admin user.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This field displays for Instant Clone images only if your VMware representative has enabled the Image Sync feature.</td>
</tr>
</tbody>
</table>

The publishing process includes running the Microsoft Windows Sysprep process. When the template VM is a Microsoft Windows server operating system, the Sysprep process will reset the built-in administrator account password to this password that you type here. This password reset is done to secure the built-in administrator account after the Sysprep process has completed. The built-in administrator password is reset to the password you type here whether you specify the built-in administrator account or a non-built-in administrator account in this step.

8 Click **Publish**.

The publishing process takes approximately 40 minutes to complete. If successful, the Image task shows as Complete.

**Note** Do not restore a VM to a snapshot taken prior to the bootstrapping process. If the agent has been already boot-strapped, this will prevent the agent from communicating as it should.

9 If the publish operation fails:
   a Select **Monitor > Activity** and locate the failed job.
   b Correct the problem that caused the failure.
   c Select **Inventory > Images** and select the check box next to the image.
   d Click ... and select **Convert to Desktop**.
   e Repeat the steps above to re-publish the image.

## Update Agent Software for an Image

Use the agent update feature to update the Horizon Agent Installer for an image and push updates to assignments.

**Note** This topic describes how to update agents using the agent update feature. To perform a manual update, see [Manually Update Agents for an Image](#).

Note the following prerequisites.

- You must have created an Agents file share and added it to Horizon Cloud. This means that you select Agents for the file share type when you create the file share. Agents file shares are used only for importing Horizon Agent Installer files. See [Managing File Shares](#).
The image must already have DaaS Agent 17.1.0.5232563 or higher and Horizon Agent 7.3.2.7161471 or higher installed.

The agent update feature functions as described below.

- The system makes regular contact with the VMware CDS software distribution network to see if a new version of the Horizon Agent Installer is available. It downloads the new version to a file share that you have set up on a local machine. The update file is then automatically imported into the system and made available to images.

- The availability of an update is indicated on the Images page, where you can apply it to images.

- Upon request, your VMware representative can do the following:
  - Adjust the interval between scans for new Horizon Agents Installer versions.
  - Adjust the wait time for scans after tenant startup.
  - Set your system to skip updating VMs with users currently logged in.
  - Set your system to restart VMs before installing agents.

Procedure

1. Click **Inventory > Images**.
   - The Images page displays, with a blue dot appearing next to the name of any image that has an Horizon Agent Installer update available. If you hover over a blue dot, a popup displays indicating the new version of the Horizon Agent Installer available for that image.

2. Select the check box an image. You can only update agents for one image at a time.

3. Click **Update Agent**.
   - The Agent Update dialog displays.

4. On the Software tab, select the Horizon Agent Installer version to update and click **Next**.

5. (Optional) On the Command Line tab, add any command line options.

6. Click **Finish**.
   - A message displays at the top of the page indicating that the update has started.
   - The system creates a clone of the image and updates the agent(s) on the clone image.

Note the following:

- Desktops are updated in batches, which cannot be larger than 30. If the assignment has 30 or fewer desktops, all desktops in the assignment will be updated together. Your VMware representative can adjust the batch size if you request it.

- If a desktop has an active session, the user will be warned five minutes before the update occurs.

- If a user attempts to login into a desktop that is being updated, the login will be unsuccessful and the user will receive a message that the desktop is not available.

You can view the progress of the update task by selecting **Monitor > Activity**. If the task is not successful within 24 hours, it fails.
7 Push updates based on the clone image. For more information, see Managing Images.
8 (Optional) Delete the original image and rename the clone image with the original image name.

Manually Update Agents for an Image
You can update agents for an image using a manual process.

Note This topic describes how to update agents manually. To using the agent update feature, see Update Agent Software for an Image.

Procedure
1 On the Images page, select the image and select Take Offline from the "..." drop-down menu.
2 Select Convert to Desktop from the "..." drop-down menu.
3 On the Imported VMs page, select the desktop VM and select Launch Console from the More menu.
4 In the console, update the agent(s) on the desktop VM.
5 On the Imported VMs page, select the desktop VM and select Convert to Image from the More menu.
6 Set up and publish the image as desired.

Build Your Own Template
Before you create an image, you must first prepare the desktop template.

The process of building the template includes the following:
- Run the Horizon Agent Installer
- Configure VMware Horizon Smart Policies (optional)
- Set up direct connection to desktop VMs (optional)
- Optimize the display (optional)

Note When you have finished setting up the template desktop, run the following command on Windows PowerShell:

```
Get-AppxPackage | Remove-AppxPackage
```

This prevents a possible sysprep issue that leads to image publish failure.

Running the Horizon Agents Installer
After you have completed the preparation steps, you can run the Horizon Agents Installer on the template VM.
There are three possible scenarios when running the Horizon Agents Installer:

- Install on Windows desktop.
- Install on Windows server as a Personal Desktop (Non-RDSH)
- Install on Windows server as an RDSH Role

For currently supported versions of Windows, see the VMware Knowledge Base.

**Note**: Keep the following points in mind as you perform these tasks:

- Installing a version of the Horizon Agents Installer that is older than the most recent version of the Horizon Agents Installer can cause problems subsequently when you create RDS pools based on the image VM. In this situation, when you create a new RDS pool, the system can allow you to select HTML Access (Blast) as a protocol, but this selection will not be applied to the pool even though it appears to have been applied successfully.
- The Help Desk Plugin option is installed by default. If you choose not to install this option, performance-related metrics from user sessions in the desktop instances or farm server instances based on this image are not collected. As a result, some data will not be available in the user card for such sessions. For details, see The User Card in the Horizon Cloud Administration Console.
- The vRealize Operations Desktop Agent option is installed by default. If you choose not to install this option, activity-related data from user sessions in the desktop instance or farm server instances based on this image is not reported to Horizon Cloud. As a result, data from end-user activity and other types of desktop activity will not be displayed in reports in the Administration Console.

**Prepare the Template VM for Agent Installation**

Before installing the agent software required for connecting to desktops, complete the following pre-installation steps.

**Procedure**

1. Uninstall all software components related to all other protocols.
   **Important**: You must uninstall all software components related to all other protocols (e.g. HDX, RGS). If you do not uninstall these other protocol components, your template will be corrupted and you will no longer successfully boot into Windows. This warning does not apply to RDP; the presence of RDP components does not cause problems.

2. Update VMware Tools.

3. Make sure that port 443 is not being used by any other software, or use a non-standard port.

4. Make sure that the following ports are open to TCP and/or UDP traffic as indicated:

<table>
<thead>
<tr>
<th>Port(s)</th>
<th>Source</th>
<th>Destination</th>
<th>TCP</th>
<th>UDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>4172 (PCoIP)</td>
<td>Access Point</td>
<td>VM</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>443 (View communication)</td>
<td>Tenant Appliance</td>
<td>VM</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>Port(s)</td>
<td>Source</td>
<td>Destination</td>
<td>TCP</td>
<td>UDP</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
<td>-------------</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>32111 (PCoIP)</td>
<td>Access Point</td>
<td>VM</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>22443 (HTML Access)</td>
<td>Access Point</td>
<td>VM</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>443 (HTML Access)</td>
<td>Access Point</td>
<td>T/VM</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>8443 (HTML Access)</td>
<td>Access Point</td>
<td>VM</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>4172 (PCoIP)</td>
<td>Access Point</td>
<td>VM</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>80 (redirects to 443)</td>
<td>Access Point</td>
<td>T/VM</td>
<td>P</td>
<td></td>
</tr>
</tbody>
</table>

What to do next

Install the Horizon Agent.

Run the Horizon Agents Installer on a Windows Desktop

You can run the Horizon Agents Installer on a Windows desktop.

**Note** Keep the following points in mind as you perform these tasks:

- Installing a version of the Horizon Agents Installer that is older than the most recent version of the Horizon Agents Installer can cause problems subsequently when you create RDS pools based on the image VM. In this situation, when you create a new RDS pool, the system can allow you to select HTML Access (Blast) as a protocol, but this selection will not be applied to the pool even though it appears to have been applied successfully.

- The Help Desk Plugin option is installed by default. If you choose not to install this option, performance-related metrics from user sessions in the desktop instances or farm server instances based on this image are not collected. As a result, some data will not be available in the user card for such sessions. For details, see The User Card in the Horizon Cloud Administration Console.

- The vRealize Operations Desktop Agent option is installed by default. If you choose not to install this option, activity-related data from user sessions in the desktop instance or farm server instances based on this image is not reported to Horizon Cloud. As a result, data from end-user activity and other types of desktop activity will not be displayed in reports in the Administration Console.

**Procedure**

1. Download the latest Horizon Agents Installer from the Myvmware download site. Note that there are separate downloads for 32-bit and 64-bit operating systems.

2. Double-click the Horizon Agents Installer file (file name is: VMware-Horizon-Agents-Installer-x.y.z-nnnnnnnn-x64.exe for the 64-bit installer).

   **Note** If you choose to perform a silent install, be aware that not all silent install options are applicable to all platforms.

3. Click **Configure** under Horizon Cloud Endpoint Desktop.
4 Make desired configuration changes as described below.

- Install paths for components
  Enter custom path or leave default.

- Cloning capability
  To enable Instant Clone, select the **Instant Clone** radio button.

  **Note**  Selecting Instant Clone disables the Horizon 7 Persona Management option below.

- Features to install
  Select features to install using the available check boxes. You can hover over each selection for more information about that feature.

5 Click the forward arrow at the bottom of the wizard to continue.

6 If you wish to save the silent install command for future use, copy it from the text box.

7 Click **Proceed with installation**.

  The wizard shows installation progress for the components.

8 When all components are installed, click **Finish**.

9 Restart the virtual machine when prompted.

**What to do next**

For improved security regarding the use of the Horizon Agent, disable weak ciphers in SSL and TLS, which requires you to edit the Group Policy Object (GPO) of the Active Directory server. See the appropriate Horizon Agent documentation for information about disabling weak ciphers in SSL/TLS, such as in the VMware Horizon 7 documentation set.
Run the Horizon Agents Installer on a Windows Server as Personal Desktop (Non-RDSH)

You can run the Horizon Agents Installer on a Windows Server as a personal desktop.

**Note**  Keep the following points in mind as you perform these tasks:

- Installing a version of the Horizon Agents Installer that is older than the most recent version of the Horizon Agents Installer can cause problems subsequently when you create RDS pools based on the image VM. In this situation, when you create a new RDS pool, the system can allow you to select HTML Access (Blast) as a protocol, but this selection will not be applied to the pool even though it appears to have been applied successfully.

- The Help Desk Plugin option is installed by default. If you choose not to install this option, performance-related metrics from user sessions in the desktop instances or farm server instances based on this image are not collected. As a result, some data will not be available in the user card for such sessions. For details, see The User Card in the Horizon Cloud Administration Console.

- The vRealize Operations Desktop Agent option is installed by default. If you choose not to install this option, activity-related data from user sessions in the desktop instance or farm server instances based on this image is not reported to Horizon Cloud. As a result, data from end-user activity and other types of desktop activity will not be displayed in reports in the Administration Console.

**Procedure**

1. Download the latest Horizon Agents Installer from the Myvmware download site. Note that there are separate downloads for 32-bit and 64-bit operating systems.

2. Double-click the Horizon Agents Installer file (file name is: VMware-Horizon-Agents-Installer-x.y.z-nnnnnnnn-x64.exe for the 64-bit installer).

   **Note** If you choose to perform a silent install, be aware that not all silent install options are applicable to all platforms.

3. Click **Configure** under Horizon Cloud Endpoint Desktop.

4. Make desired configuration changes as described below.

   - **Install paths for components**
     Enter custom path or leave default.

   - **Cloning capability**
     To enable Instant Clone, select the **Instant Clone** radio button.

     **Note** Selecting Instant Clone disables the Horizon 7 Persona Management option below.

   - **Features to install**
     Select features to install using the available check boxes. You can hover over each selection for more information about that feature.
5 Click the forward arrow at the bottom of the wizard to continue.

6 If you wish to save the silent install command for future use, copy it from the text box.

7 Click **Proceed with installation**.

   The wizard shows installation progress for the components.

8 When all components are installed, click **Finish**.

9 Restart the virtual machine when prompted.

**What to do next**

For improved security regarding the use of the Horizon Agent, disable weak ciphers in SSL and TLS, which requires you to edit the Group Policy Object (GPO) of the Active Directory server. See the appropriate Horizon Agent documentation for information about disabling weak ciphers in SSL/TLS, such as in the VMware Horizon 7 documentation set.

**Run the Horizon Agents Installer on a Windows Server as an RDSH Role**

You can run the Horizon Agents Installer on a Windows server as an RDSH role.

**Note** Keep the following points in mind as you perform these tasks:

- Installing a version of the Horizon Agents Installer that is older than the most recent version of the Horizon Agents Installer can cause problems subsequently when you create RDS pools based on the image VM. In this situation, when you create a new RDS pool, the system can allow you to select HTML Access (Blast) as a protocol, but this selection will not be applied to the pool even though it appears to have been applied successfully.

- The Help Desk Plugin option is installed by default. If you choose not to install this option, performance-related metrics from user sessions in the desktop instances or farm server instances based on this image are not collected. As a result, some data will not be available in the user card for such sessions. For details, see the User Card in the Horizon Cloud Administration Console.

- The vRealize Operations Desktop Agent option is installed by default. If you choose not to install this option, activity-related data from user sessions in the desktop instance or farm server instances based on this image is not reported to Horizon Cloud. As a result, data from end-user activity and other types of desktop activity will not be displayed in reports in the Administration Console.

**Procedure**

1 Add the Remote Desktop Services role.

   a Select **Start > Administrative Tools > Server Manager** to open the Server Manager.

   b Select **Roles** and then select **Add Roles** in the right pane.

      The Before You Begin page of the Add Roles Wizard window appears.

   c Click **Next**.

      The Select Server Roles page appears.
d Select the check box for Remote Desktop Services and click **Next**.
The Remote Desktop Services page appears.

e Click **Next**.
The Select Role Services page appears.

f Select the check box for Remote Desktop Session Host and click **Next**.
The Uninstall and Reinstall Applications for Compatibility page appears.

g Click **Next**.
The Specify Authentication Method for Remote Desktop Session Host page appears.

h Select the appropriate Authentication Level, and then click **Next**.
The Specify Licensing Mode page appears.

i Specify the licensing mode, and then click **Next**.
The Select User Groups Allowed Access To This RD Session Host Server page appears.

j Add your Users or User Groups, and then click **Next**.
The Configure Client Experience page appears.

k Make desired settings, and then click **Next**.
The Confirm Installation Selections page appears.

l Confirm your selections. If something is incorrect, click **Previous** to return to the previous steps and change the settings. Click **Install**.
The Installation Progress page appears. The installation takes a few minutes to finish. The Installation Results page appears, and asks for restart.

m Click **Close**.
A dialog appears, asking for confirmation for restart.

n Click **Yes** to restart the server.

o When the server comes back, log in again.
The Resuming Configuration page appears. It takes a few seconds to resume configuration. The Installation Results page appears.

p Click **Close** to complete the installation.
The Server Manager window appears.

q Click **Roles** and confirm that the Remote Desktop Services role is installed.

2 Download the latest Horizon Agents Installer from the Myvmware download site. Note that there are separate downloads for 32-bit and 64-bit operating systems.
3 Double-click the Horizon Agents Installer file (file name is: VMware-Horizon-Agents-Installer-x.y.z-nnnnnnnn-x64.exe for the 64-bit installer).

**Note** If you want to use the URL redirection capability with the session desktops and remote applications that will be provided by this base VM, use the command line method to launch the installer and add the `VDM_URL_FILTERING_ENABLED=1` parameter to the command.

For example:

```
VMware-Horizon-Agents-Installer-x.y.z-build-x64.exe VDM_URL_FILTERING_ENABLED=1
```

Where x.y.z and build match the numbers in the file name.

**Note** If you choose to perform a silent install, be aware that not all silent install options are applicable to all platforms.

4 Click **Configure** under Horizon Cloud Endpoint Desktop.

5 Make desired configuration changes as described below.

- **Install paths for components**
  Enter custom path or leave default.

- **Cloning capability**
  To enable Instant Clone, select the **Instant Clone** radio button.

  **Note** Selecting Instant Clone disables the Horizon 7 Persona Management option below.

- **Features to install**
  Select features to install using the available check boxes. You can hover over each selection for more information about that feature.

6 Click the forward arrow at the bottom of the wizard to continue.

7 If you wish to save the silent install command for future use, copy it from the text box.

8 Click **Proceed with installation**.

   The wizard shows installation progress for the components.

9 When all components are installed, click **Finish**.

10 Restart the virtual machine when prompted.

**What to do next**

For improved security regarding the use of the Horizon Agent, disable weak ciphers in SSL and TLS, which requires you to edit the Group Policy Object (GPO) of the Active Directory server. See the appropriate Horizon Agent documentation for information about disabling weak ciphers in SSL/TLS, such as in the VMware Horizon 7 documentation set.
Configuring VMware Horizon Smart Policies

A Horizon Cloud environment supports using VMware Horizon smart policies to control the end users' virtual desktops. These smart policies provide policy-driven control over the behavior of features such as USB redirection, virtual printing, clipboard redirection, client drive redirection, and PCoIP display protocol features on the virtual desktops. By using these smart policies, you can have policies that take effect only if certain conditions are met. For example, you can configure a policy that disables the client drive redirection feature if a user connects to a remote desktop from outside your corporate network.

For a detailed description of VMware Horizon smart policies and instructions on how to use them, see Using Smart Policies in the VMware Horizon documentation or the VMware Horizon smart policies information in the VMware Horizon document titled Configuring Remote Desktop Features in Horizon 7.

These smart policies require use of User Environment Manager software and the App Volumes Unified Agent Installer software to install the required agents. You can download the software from the VMware Downloads page. Obtain version User Environment Manager 9.1 or later. For User Environment Manager system requirements and complete installation instructions, see the User Environment Manager product documentation. For detailed information and best practices for using User Environment Manager and App Volumes with your environment, see the document titled VMware App Volumes with Horizon Cloud Application Delivery Best Practices and Operations Procedures at vmware.com.

After you have completed installation and configuration of User Environment Manager and its Management Console as described in the previously mentioned documents, to configure a smart policy on your master virtual machine (VM), you need to perform the following steps on that master VM.

- If you have not done so already, run the App Volumes Unified Agent Installer. The User Environment Manager agent is installed on the VM in that process. The User Environment Manager FlexEngine client is installed with that agent component.
- Define the VMware Horizon smart policy using the User Environment Manager Management Console.
  For descriptions of the VMware Horizon smart policy settings you can select in User Environment Manager, see Horizon Smart Policy Settings in the VMware Horizon 7 documentation.
- Add conditions that must be met for the policy to take effect, as described in Adding Conditions to Horizon Smart Policy Definitions in the VMware Horizon documentation.

For examples of using Horizon smart policies, see Reviewer's Guide for View in VMware Horizon 7: Smart Policies document at vmware.com.

Adding Conditions to Horizon Smart Policy Definitions describes the use of Horizon Client property conditions in the smart policies. Predefined Horizon Client properties correspond to ViewClient_[registry keys]. Not all of the predefined properties used in Horizon 7 are applicable in a Horizon Cloud environment. The properties that are not applicable are:

- ViewClient_Broker_Pool_Tags
- ViewClient_Broker_Tags
- **ViewClient_Launch_Matched_Tags**
- **ViewClient_Broker_DNS_Name**

In a Horizon Cloud environment configured using Unified Access Gateway, the broker sets the following gateway-related properties by default to these values as follows:

- If your Unified Access Gateway is external, then the **ViewClient_Broker_GatewayLocation** property is set to External and **ViewClient_Broker_GatewayType** property is set to AP.
- If your Unified Access Gateway is internal, then the **ViewClient_Broker_GatewayLocation** property is set based on the Internal Networks list and the **ViewClient_Broker_GatewayType** property is set to AP.

**Note** The Internal Networks list is created by your service provider and is displayed on the General Settings page.

Using a Unified Access Gateway with your Horizon Cloud environment is a best practice. However, if you do not have a Unified Access Gateway, the broker sets the **ViewClient_Broker_GatewayLocation** property based on the Internal Networks list and sets the **ViewClient_Broker_GatewayType** property to None.

**Optimizing the Display**

Perform the tasks linked below to optimize the display on the template VM.

**Add the PCoIP Group Policy Settings**

You can add the PCoIP Group Policy Settings to the local computer policy environment.

To configure the group policies, you must first add the .adm template file to the Local Computer Policy configuration on this VM.

**Procedure**

1. On the template VM, click **Start > Run**.
2. Type `gpedit.msc` and click **OK**.
   
   The Local Group Policy Editor console opens.
3. Confirm that you can connect to the View Connection Server from this VM.
4. In the navigation pane, select **Local Computer Policy > Computer Configuration**.
5. Right-click **Administrative Templates**.

   **Note** Do not select Administrative Templates under User Configuration.

6. Select **Add/Remove Templates**.
7. In the Add/Remove Templates dialog, click **Add**.
8. Download the pcoip_policies.adm file from the Horizon DaaS Library on salesforce.com.
9 Click Open.

10 Close the Add/Remove Templates window.

The PCoIP group policy settings are added to the Local Computer Policy environment on the desktop system and are available for configuration.

**Add the HTML Access (Blast) Group Policy Settings**

You can add the HTML Access (Blast) Group Policy Settings to the local computer policy environment

**Procedure**

1 Download the View GPO Bundle .zip file from the VMware Horizon download site.

   The file is named VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyyy.zip, where x.x.x is the version and yyyyyyyy is the build number. All ADM and ADMX files that provide group policy settings for View are available in this file.

2 Copy the file to your Active Directory server and unzip the file.

   The HTML Access GPOs are included in the Blast-enUS.adm ADM Template file.

3 On the Active Directory server, edit the GPO.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
   | Windows 2008 or 2012  | a Select Start > Administrative Tools > Group Policy Management.  
                         | b Expand your domain, right-click the GPO that you created for the group policy settings, and select Edit.  
   | Windows 2003          | a Select Start > All Programs > Administrative Tools > Active Directory Users and Computers.  
                         | b Right-click the OU that contains your View desktops and select Properties.  
                         | c On the Group Policy tab, click Open to open the Group Policy Management plug-in.  
                         | d In the right pane, right-click the GPO that you created for the group policy settings and select Edit.  

   The Group Policy Object Editor window appears.

4 In the Group Policy Object Editor, right-click Administrative Templates under Computer Configuration and then select Add/Remove Templates.

5 Click Add, browse to the Blast-enUS.adm file, and click Open.

6 Click Close to apply the policy settings in the ADM Template file to the GPO.

   The VMware Blast folder appears in the left pane under Administrative Templates > Classic Administrative Templates.

7 Configure the HTML Access group policy settings.
8 Make sure your policy settings are applied to the remote desktops.
   a Run the gpupdate.exe command on the desktops.
   b Restart the desktops.

Configure Policy Settings for Display
You can configure policy settings to optimize the display on the template VM.

Make the following settings in the Overrideablepolicy group.

Procedure
1 Enable “Turn off Build-to-Lossless feature” by selecting the check box.
2 Enable “Configure PCoIP image quality levels”
   ■ Set Minimum Image Quality to 30.
   ■ Set Maximum Image Quality to 70.
   ■ Set Maximum Frame Rate to 16.

Enabling 3D Graphics
You can enable 3D graphics on a per-assignment basis.

Support for 3D graphics is provided using Soft 3D, also known as vSGA (see pages 3-4 of the VMware white paper on Graphics Acceleration for more information). In order for you to use 3D graphics feature, the following must be true:

■ Virtual hardware version must be 8 or higher.
■ Desktop must have the Windows Aero theme.
■ Servers must have appropriate hardware installed.

Note Consult the latest PCoIP recommendations when configuring desktops with this feature.
Farms in Horizon Cloud

A farm is a collection of Microsoft Remote Desktop Services (RDS) hosts that provide multiple users with session-based desktops and applications. Farms simplify the management of the RDS hosts. You can create farms to serve groups of users that vary in size or have different desktop or application requirements.

Before you can assign session-based desktops or remote applications to end users, you must create the farms to serve those desktops and applications. A farm can provide either session-based desktops or remote applications.

Use the Farms page in the Administration Console to manage your farms. You navigate to the Farms page using the Inventory icon.

This chapter includes the following topics:

- Create a Farm
- Managing Farms in Horizon Cloud
Create a Farm

You create farms using the Farms page.

**Note**  The RDS-enabled image is also called an RDS host or an RDSH (Remote Desktop Services Host) image.

**Prerequisites**

- Verify that you have at least one image listed on the Images page, that image has an RDS-enabled Windows server operating system, the Images page shows that image is in Published state, and that image is located in the pod in which you want to create the farm. You cannot create a farm in a pod without such an image available in that pod.

- Decide whether this farm will serve session-based desktops or remote applications. In this release, the same farm cannot serve both.

**Procedure**

1. In the Administration Console, navigate to **Inventory > Farms**.

2. Click **New**.

   The New Farm wizard opens.

   The New Farm wizard opens.

   The New Farm wizard opens.
3. In the wizard's Definition step, complete the fields and make your selections as appropriate and then click Next.

**Note** You might have to use the scroll bar to see all the required fields.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for this farm.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter an optional description.</td>
</tr>
<tr>
<td>VM Names</td>
<td>Base name for all of the server VMs created for this farm. The VM names will have numbers appended to this base name, for example, win2016-1, win2016-2, etc. The name must start with a letter and can contain only letters, dashes, and numbers.</td>
</tr>
<tr>
<td>Farm Type</td>
<td>Specify the type of asset this farm provides to end users:</td>
</tr>
<tr>
<td></td>
<td>Select <strong>Desktops</strong> to use this farm to provide session-based desktops.</td>
</tr>
<tr>
<td></td>
<td>Select <strong>Applications</strong> to use this farm to provide access to remote applications. After an applications farm is created, you can use the New Application workflow's <strong>Auto-scan from Farm</strong> option to import applications from the farm's servers into your application inventory.</td>
</tr>
<tr>
<td>Pod</td>
<td>This option only displays if your data center is configured with multiple pods. Pods contain specific assignable images and server model capacities for assignments. You can only create assignments from images in the same pod.</td>
</tr>
<tr>
<td>Network</td>
<td>If your data center is configured to use specific network mappings to assignments, select the network that you want this farm to use. For example, if you have a DHCP server on a specific network and your data center is configured to use that network for assignments, you might select that network. <strong>Note</strong> If Load Balance value is selected, no specific network mapping is used for the assignments using on this farm.</td>
</tr>
<tr>
<td>Image</td>
<td>Select the assignable RDSH image.</td>
</tr>
<tr>
<td>Preferred Protocol</td>
<td>Select a default display protocol you want the end-user sessions to use.</td>
</tr>
<tr>
<td></td>
<td>Circumstances might occur that cause another protocol to be used instead of the default protocol. For example, the client device does not support the default protocol or the end user overrides the default protocol selection.</td>
</tr>
<tr>
<td>Preferred Client Type</td>
<td>Select the preferred client type used when end users launch their session-based desktops from the Workspace™ ONE™ platform's portal, either a Horizon Client or a browser for HTML Access.</td>
</tr>
<tr>
<td>Domain</td>
<td>Select the Active Directory domain registered with your environment.</td>
</tr>
<tr>
<td>Join Domain</td>
<td>Select <strong>Yes</strong> so that the farm’s server instances are automatically joined the domain when they are created.</td>
</tr>
<tr>
<td>Servers</td>
<td>Specify the number of servers you want in this farm.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If the remaining capacity displayed appears to be too low, it may be because the default limit of 2,000 VMs per pod has been reached. This includes VMs created in earlier versions of the product, but does not include Utility or Imported VMs. For more information, contact your VMware representative.</td>
</tr>
<tr>
<td>Sessions per Server</td>
<td>Specify the number of concurrent end-user sessions per server that this farm will allow.</td>
</tr>
</tbody>
</table>
Optionally configure the advanced properties.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Computer OU</strong></td>
<td>Active Directory Organizational Unit where the server VMs are to be located. Enter the Active Directory Organizational Unit using the distinguished name, for example, \O=RootOrgName, DC=DomainComponent, DC=eng, and so on. The OU and each path in a nested OU can contain any combination of letters, numbers, special characters, and spaces, and can have a maximum of 64 characters. If you need to use nested Organization Units, see Working with Nested Organizational Units. <strong>Note</strong> For traditional clones, if the <strong>Computer OU</strong> is set to \CN=Computers, the system uses the default Active Directory Computers container for VMs. Note that this default container may have been redirected to an organizational unit class container.</td>
</tr>
<tr>
<td><strong>Run Once Script</strong></td>
<td>(Optional) Location of a script that you want run in the farm's server VMs after the VM creation process. <strong>Note</strong> The script should end with a reboot step to reboot the VM. A sample reboot line as a Windows command is: <code>shutdown /r /t 0</code> The script is run after the Microsoft Windows System Preparation (Sysprep) process. When the system creates a server VM for the farm, the VM starts up and completes the Sysprep process in the Windows operating system. When the Sysprep process completes, the agent in the VM reaches out to do the domain join. At the same time, the agent gets the script path you specify here. The agent sets the Windows RunOnce path (System run once) and then restarts the server VM. On the next restart, the system logs in to the Windows operating system using the local administrator account and runs the script.</td>
</tr>
<tr>
<td><strong>Enable Windows Hot-Plug</strong></td>
<td>(Optional) Keep the default No setting to prevent end users from dynamically adding or removing external devices from their virtual desktops, such as CD/DVD drives, Ethernet adapters, and similar device types. <strong>Caution</strong> Setting this toggle to Yes can result in users accidentally interfering with connectivity to the virtual desktops if the users dynamically remove the networks cards (NICs) or other operational components by mistake. Even though you might choose to enable this setting for special cases, such as supporting the use of thumb drives in your virtual desktops, be aware that the setting is enabled for all such plug-and-play devices in the resulting desktops.</td>
</tr>
</tbody>
</table>
In the wizard’s Management step, complete the fields and make your selections as appropriate and then click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rolling Maintenance</strong></td>
<td>Select the maintenance type, either according to a time cadence (<strong>Scheduled</strong>) or based on user sessions to this farm’s servers (<strong>Session</strong>). When <strong>Scheduled</strong> is selected, configure the maintenance cadence, either daily or weekly. If you choose a daily recurrence, specify the hour at which the maintenance will start. If you choose a weekly recurrence, specify both the day of the week and the hour. When <strong>Session</strong> is selected, specify the number of sessions at which the farm should begin rolling maintenance. <strong>Note</strong> Sessions which are logged off within 15 minutes are not counted for the purposes of the rolling maintenance calculations, to prevent restarting or rebuilding the servers based on a count of short running sessions. In the <strong>Concurrent Quiescing Servers</strong> field, specify the number of servers that can be in the quiescing state at the same time. When a server is in quiescing state, the server continues to work for the user sessions already connected to that server, but it does not accept any new user connections.</td>
</tr>
<tr>
<td><strong>Server Action</strong></td>
<td>Select the action that the system should perform on the servers undergoing maintenance. <strong>With Restart</strong>, the server VMs are restarted. <strong>With Rebuild</strong>, the server VMs are first deleted and then reprovisioned from their RDS desktop image.</td>
</tr>
</tbody>
</table>
### Option | Description
--- | ---
Timeout Handling  | Configure how you want the system to handle certain types of user sessions.

**Note**  | The user sessions governed by these settings are the user logins to the Windows operating system session of the RDS session desktop or application. These sessions are not the user logins in Horizon Client, Horizon HTML Access, or Workspace ONE.

The user’s session begins when the user authenticates to the Windows operating system that underlies the session-based desktop or the remote application that is served from this farm's servers.

- **Empty Session Timeout** - For applications farms, select how the system should handle idle user sessions, whether to never time out idle sessions or to time out after a specified number of minutes. Idle timeouts are based on the activity on the endpoint device, not on the session-based desktop or application. If you specify to time out an idle session, select what happens when the timeout period is up: whether to disconnect the session or log the user off. When a session is disconnected, the session is disconnected from the network and preserved in memory. When a session is logged off, the session is not preserved in memory, and any unsaved documents are lost.

- **Log Off Disconnected Sessions** - Select when the system logs the user off of a disconnected session.

- **Max Session Lifetime** - Specify the maximum number of minutes the system should allow for a single user session.

### Session Timeout Interval

This time interval is the amount of time the end users’ sessions can be idle before the system forces a log off from the session-based desktops or applications that are served by this farm. This timeout applies to the logged-in session to the underlying Windows operating system. The time you specify here is different from the timeout settings that govern the end users' Horizon Client or HTML Access logged-in session.

**Caution**  | When the system forces the log off in the underlying Windows operating system session, any unsaved data is lost. To prevent an unintended loss of data, set this interval high enough to accommodate the business needs of your end users.

**Note**  | If no user activity occurs before the timeout interval is reached, a message indicates that the user will be logged off if they do not click OK in the next 30 seconds. If the logout occurs, any unsaved user data, such as documents or files, is lost.

5  In the wizard's Summary step, review the settings and then click **Submit** to begin creating the farm.

The system starts creating the farm. You can monitor the progress using the Activity page. When the farm's status shows a green dot on the Farms page:

- If you created a desktops farm, you can use it to create a session-based desktop assignment.

- If you created an applications farm, you can use it to load applications from the servers' underlying RDS-enabled operating system into your Horizon Cloud applications catalog.
What to do next

If you created a desktops farm, you would next create a session-based desktop assignment for your end users by following the steps in Create an RDSH Session Desktop Assignment.

If you created an applications farm, you would next scan that farm to load applications into Horizon Cloud and then create an applications assignment so your end users can use the remote applications from that farm.

For more information, see Chapter 7 Applications, Importing New Applications from an RDSH Farm Using Auto-Scan from Farm, and Manually Adding Custom Applications from an RDSH Farm.

Managing Farms in Horizon Cloud

You can perform several actions on the farms listed on the Administration Console’s Farms page.

Actions You Can Perform on the Farms Page

At a page level, you can select the check box next to an existing farm and click one of the buttons to perform its associated action on the farm.

Edit

Clicking this button launches a wizard in which you can change certain settings, such as the farm’s power management settings, the minimum and maximum number of servers the farm can have, and so on. The wizard is similar to the New Farm wizard, with read-only fields for those settings that cannot be changed for an existing farm. For detailed descriptions of the fields, see Create a Farm.
Alternatively, instead of using the Edit button, you can click the farm's name and update the settings from the farm's summary page.

**Note** When you edit the farm and reduce the Sessions per Server value, any existing sessions in excess of the new lower value are not automatically logged off. You can either manually log off the excess sessions or wait until the system logs off the sessions according to the values for the farm's Timeout Handling settings (Empty Session Timeout, Log Off Disconnected Sessions, Max Session Lifetime) and Session Timeout Interval. Because those existing sessions in excess of the new lower value are not automatically logged off, the Administration Console might display server and farm utilization values higher than 100% until the excess active sessions are logged off.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Take Offline</td>
<td>Clicking this button opens a window in which you can select to take a farm offline for maintenance.</td>
</tr>
<tr>
<td>Bring Online</td>
<td>Clicking this button opens a window in which you can select to bring an offline farm back online.</td>
</tr>
<tr>
<td>Delete</td>
<td>You use this button to delete the selected farm. However, before you can delete a farm using this button, you must delete any assignments that are using the farm. You can view the assignments that are using the farm by navigating to the Assignments page and sorting on its Farms column.</td>
</tr>
</tbody>
</table>

**Note** Deleting the farm deletes all of the farm's underlying server VMs. When a farm is deleted, all of that farm's logged activity is removed from the Activity page.

### Actions You Can Perform Within a Farm's Detailed Pages

From the Farms page, you can click a farm's name to see its detailed pages. Initially the Summary page is displayed.

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary page</strong></td>
<td>The Summary page displays the farm's current settings. For each page section, you can click Edit to change those settings that the system allows to be updated for an existing farm. Some settings cannot be changed on a farm after it is created, such as its pod.</td>
</tr>
<tr>
<td><strong>Servers page</strong></td>
<td>The Servers page displays the existing server instances in the farm. The actions you can perform on a selected server are power on or off (depending on the server's current state) and delete.</td>
</tr>
</tbody>
</table>
Sessions page

The Sessions page displays the farm's existing user sessions. When you select a session, you can disconnect it or log the user off the session. When you click **Disconnect**, you force the user's session to be disconnected. No message is sent to the user that the session is disconnecting. When you click **Log Off**, a message is displayed to the user with a grace period in which the user can save documents before the session ends.

System Activity page

The System Activity page displays activity in the farm due to system actions, such as expanding the farm.

You can cancel assignment-related tasks before they complete by selecting the task in the list and clicking **Cancel Tasks**.

- Before attempting to select a task for cancellation, refresh the view to update the status for the tasks displayed.
- If a task is currently in a state where the system allows you to cancel it, you can select the check box corresponding to that cancellable task. If you select all of the listed tasks by selecting the topmost check box, only those tasks that are currently cancellable are selected.

The table below shows tasks that you can cancel.
### Manage Servers in a Farm

You can perform certain actions on the individual servers in a farm.

**Procedure**

1. Click **Inventory > Farms**.
   
   The Farms page displays.

2. Click the name of a farm on the list.
   
   The farm details page displays.

3. Click **Servers** at the top of the page.
   
   The Servers tab displays, showing a list of servers for the farm. You can filter, refresh, and export the list using the controls to the top right of the page.

   You can perform the following actions by selecting one or more servers and clicking one of the buttons at the top of the page.

   **Note**  
   Server status must be green to perform these actions.

---

<table>
<thead>
<tr>
<th>Task</th>
<th>Cancel When Task is in Queued State</th>
<th>Cancel When Task is in Running State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Farm Expansion</td>
<td>Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When the system has automatically created an expansion task for an RDSH farm, the farm must be offline before you can cancel that task.</td>
<td></td>
</tr>
<tr>
<td>Assignment Expansion</td>
<td>Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When the system has automatically created an expansion task for a VDI desktop assignment, the assignment must be offline before you can cancel that task.</td>
<td></td>
</tr>
<tr>
<td>Convert VM to Image</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you cancel this task, and wish to retry it, first confirm that the VM is in a state where it can be converted. If you are not sure, power off and then power on the VM.</td>
<td><strong>Note</strong> If you cancel this task, and wish to retry it, first confirm that the VM is in a state where it can be converted. If you are not sure, power off and then power on the VM.</td>
</tr>
</tbody>
</table>

**User Activity page**

The User Activity page displays activity in the farm due to user actions, such as logging on and logging off sessions provided by the farm.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Power Off         | Shuts down the selected servers.  
|                   | - You can select more than one server at a time.  
|                   | - You can only shut down VMs that do not have active user sessions.  
| Power On          | Starts up the selected powered-off servers.  
| Delete            | Deletes the selected server. To reduce the size of the farm when the server is deleted, select **Yes** under 'Reduce farm size' in the dialog.  
| Reset Agent Pairing | Repairs the agent pairing state when pairing failure has occurred.  
|                   | - You can select multiple servers. The action will only be applied to those selected servers that are currently powered on.  
|                   | - You can view progress on the Monitor > Activity page or on the System Activity tab of the farm's detail page.  
| Launch Console    | Launches a console so that you can log in to the virtual machine.  

Capacity

The Capacity page displays current desktop capacity and usage information.

At the top of the page you can:

- Filter information displayed by Data Center and Pod using the drop-down menus.
- Download a report in .csv format by clicking the **Download Full Service Report** link.

The main area of the page has two sections, described below.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop Model</td>
<td>Shows the total standard capacity, with number of units used for each desktop model and units available. Click on the <strong>Details</strong> link to see VM status broken down by desktop model.</td>
</tr>
<tr>
<td>Storage Types</td>
<td>Shows total storage, with amount used for different storage types and amount free. Click on the <strong>Storage</strong> link to see the storage broken down by individual volumes.</td>
</tr>
</tbody>
</table>
Imported VMs

Imported VMs are unmanaged VMs with supported operating systems imported into Horizon Cloud to be converted into images or migrated to dedicated desktop assignments.

You can perform the following actions using buttons at the top of the page.
<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Import | Import a desktop VM from a file share.  
**Note** In order to import a VM, you must first create a VMs file share and populate it with at least one set of VM files (see Managing File Shares).  
1. Click **Import**.  
The Import Desktop - File Share dialog displays.  
2. Enter information as described below.  
   - **Destination Desktop**  
     - DataCenter - Destination data center for the imported VM.  
     - Pod - Destination pod for the imported VM.  
     - Network - Destination network for the imported VM. To use the least populated network available, select the Load Balance option.  
   - **Desktop to Import**  
     - FileShare - Auto-populates with your VMs file share.  
     - Desktop - Select the VM to import.  
     **Note** The imported VM must meet the following requirements.  
     - Virtual hardware version of 11 or earlier.  
     - Only one network interface controller (NIC).  
   - **Reconfigure Desktop**  
     - Select YES and select a desktop model from the drop-down list to reconfigure the desktop VM to that desktop model when it is imported.  
     - Select NO to import the desktop VM with its current configuration.  
     - Have you optimized Windows image? - Select YES or NO to indicate whether you have run the OS optimization tool on the selected desktop VM.  
   - **Properties**  
     - Desktop Name - Enter a unique name for the imported VM.  
     - Description - Enter a description for the imported VM.  
3. Click the **Import** button at the bottom of the dialog.  
You can view the progress of the import operation on the Activity page (**Monitor > Activity**).  
**Note**  
- If VMware Tools is on the VM, it is upgraded to the latest version of VMware Tools when the VM is imported. If VMware Tools is not on the VM, the tools drive is mounted on the VM and then you need to install VMware Tools manually by launching the VM console from the Imported VMs page.  
- Imported VMs are included in Standard Capacity calculations. |
| Rename | Select a VM and click **Rename**. Enter a new name in the field and click **Save**.  
**Note** For this action to be successful, the selected VM must be paired with the tenant using Agent Pairing and the DaaS Agent must be in Active state. |
### Action Description

**Shutdown**  
Shuts down the VM(s).  
- You can select more than one VM at a time.  
- VM status must be green.  
- You can only shut down VMs that do not have active user sessions.

**Restart**  
Performs a ‘graceful’ restart of the VM(s), allowing you to recover hung VMs without loss of data. If this does not work, it may be necessary to use the Reset menu option, which performs a hard reset of the VM and can result in data loss.  
- You can select more than one VM at a time.  
- VM status must be green.

You can perform the following actions by clicking the **More** button and making a selection from the drop-down menu.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspend</td>
<td>Suspends the selected VM.</td>
</tr>
<tr>
<td>Resume</td>
<td>Resumes operation of the selected VM.</td>
</tr>
<tr>
<td>Power On</td>
<td>Powers on the selected VM.</td>
</tr>
<tr>
<td>Power Off</td>
<td>Powers off the selected VM.</td>
</tr>
<tr>
<td>Reset</td>
<td>Resets the selected VM.</td>
</tr>
<tr>
<td>Convert to Image</td>
<td>Converts the selected VM to an image.</td>
</tr>
<tr>
<td>Delete</td>
<td>Permanently deletes the selected VM.</td>
</tr>
<tr>
<td>Migrate to Utility VMs</td>
<td>Moves the VM to the Utility VMs page. See <a href="#">Managing Utility VMs</a>.</td>
</tr>
</tbody>
</table>
| Migrate to Assignment   | Associates the VM(s) with a dedicated desktop assignment. In the Migrate VM(s) dialog, select an assignment in the Assignment Name field and click [Migrate](#).  
  - VMs can only be migrated to dedicated desktop assignments with the same Desktop Manager ID.  
  - Selected VM must be paired with the tenant using Agent Pairing and DaaS Agent must be in Active state.  
  - Registry entry “Use SVI=0” is required. This is already present with DaaS Agent 17.1.x and View Agent 7.1, but will have to be added manually for older agents. |
| Reset Agent Pairing     | Repairs the agent pairing state when pairing failure has occurred.          
  - You can select multiple VMs. The action will only be applied to those selected VMs that are currently powered on.  
  - You can view progress on the Monitor > Activity page. |
| Launch Console          | Launches a console for the selected desktop. This option is disabled if the VM is powered off or if more than one VM is selected. |
| Generate Logs           | Generates logs for the image VM. If you have configured a VMs file share, the system places log files in that file share. For more information, see [Managing File Shares](#).  
  **Note**  This feature requires Horizon Agent Installer 19.1 or higher. |
| Rectify                 | Deletes and recreates the selected desktop. Use this option for desktop VMs that have become corrupted or otherwise non-operational. |
Settings

Edit a variety of settings for your system.

Select the Settings icon to access these options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Settings</td>
<td>Displays settings for networks, domain, etc. You can edit settings from this page, and upload certificates. See Edit General Settings.</td>
</tr>
<tr>
<td>Active Directory</td>
<td>View and edit Active Directory details. See Edit an Active Directory Domain.</td>
</tr>
<tr>
<td>Roles &amp; Permissions</td>
<td>Edit Roles and Permissions. See Edit Roles and Permissions.</td>
</tr>
<tr>
<td>File Share</td>
<td>Create file shares and perform actions on existing file shares. See Managing File Shares.</td>
</tr>
<tr>
<td>Getting Started</td>
<td>Opens the Getting Started wizard. See Chapter 3 Getting Started Wizard.</td>
</tr>
<tr>
<td>Utility VMs</td>
<td>Opens the Utility VMs page. See Managing Utility VMs.</td>
</tr>
<tr>
<td>2 Factor Auth</td>
<td>Configure 2 Factor authentication for end users. See 2 Factor Authentication.</td>
</tr>
</tbody>
</table>

This chapter includes the following topics:

- Edit General Settings
- Active Directory
- Edit Roles and Permissions
- Managing File Shares
- Managing Utility VMs
- 2 Factor Authentication
- Identity Management Page

Edit General Settings

You can edit general settings and upload certificates from the General Settings page.
Procedure

1. Select **Settings > General Settings.**
2. Click **Edit.**
3. Make changes for these settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Networks</strong></td>
<td>The Networks list shows a list of your currently used network(s). This list is not editable. Contact your service provider to edit or add network(s).</td>
</tr>
<tr>
<td><strong>Default Domain</strong></td>
<td>Default domain that you are editing.</td>
</tr>
</tbody>
</table>
| **Session Timeout**  | - Client Heartbeat Interval - Controls the interval between Horizon Client heartbeats and connected state. These heartbeats report to the broker the amount of idle time that has passed. Idle time occurs when no interaction occurs with the end point device, as opposed to idle time in the desktop session. In large desktop deployments, setting the activity heartbeats at longer intervals might reduce network traffic and increase performance.  
  - Client Idle User - Maximum time that a user can be idle while connected to the tenant. When this maximum is reached, the user is disconnected from all active Horizon Client Desktop sessions. The user must re-authenticate to re-access the Horizon Client.  
    **Note** Set the Client Idle User timeout to be at least double the Client Heartbeat Interval to avoid unexpected disconnects from desktops.  
  - Client Broker Session - Maximum time that a Horizon Client instance can be connected to the tenant before its authentication expires. The timeout count starts each time you authenticate. When this timeout occurs, you can continue to work. If you perform an action that causes communication to the broker, such as changing settings, the system requires you to re-authenticate and log back in to the desktop.  
    **Note** The Client Broker Session timeout must be at least equal to the sum of the Client Heartbeat Interval and the Client Idle User timeout.  
  - User Portal Timeout - How long you can be on the User Portal when you try to broker a connection before you need to log in again.  
  - Admin Portal Timeout - How much idle time can pass in the Administration Console before the session times out. |
| **User Portal Configuration** | This feature is deprecated.                                                                                                           |
| **HTML Access**      | Cleanup credentials when tab is closed - Controls whether to delete credentials of the broker session when a HTML Access portal connection tab is closed. |
| **Notifications**     | Enter email addresses, separated by a comma, for the users you want to receive notifications for system issues such as AD connectivity and authentication failure.  
    **Note** Site24x7 integration must be completed for this feature to be functional. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RDSH Farm</td>
<td>Defines policy parameters for RDSH farms.</td>
</tr>
<tr>
<td></td>
<td>- Session Lifetime Reminder Message - This message reminds users that they will be logged off after a specified grace period.</td>
</tr>
<tr>
<td></td>
<td>Default message is “Dear user, your session has reached the maximum lifetime, you will be logged off in [0] minutes”. The value specified in the Grace Period field replaces [0] in the message seen by the user.</td>
</tr>
<tr>
<td></td>
<td>- Grace Period - Interval of time after which user is logged off following Session Lifetime Reminder Message.</td>
</tr>
<tr>
<td>Pool/Farm Options</td>
<td>Enable Client Retry - This option governs what happens if the end user uses Horizon Client to try to connect to a desktop or remote application when the underlying virtual machine is powered off in the cloud. As a result of an assignment's or RDSH farm's power management settings, there might not be enough powered-on virtual machine capacity to serve the client's request. When the connection is initiated, Horizon Cloud starts powering on the underlying virtual machine needed to fulfill the request. However, while the underlying virtual machine is powering on, the Horizon Cloud agent in the virtual machine has not yet started up and cannot respond to the Horizon Client connection request. Because it can take some time between when the client initiates the connection and the agent is running, you can use this option to have the client automatically retry the connection and inform the end user of the estimated time. For this scenario, when the Enable Client Retry toggle is set to Yes, the client presents a message to the end user that describes the estimated waiting time.</td>
</tr>
<tr>
<td></td>
<td>a. Horizon Cloud starts powering on the underlying virtual machine in the cloud that will serve the end user's client request.</td>
</tr>
<tr>
<td></td>
<td>b. Horizon Cloud notifies Horizon Client to retry the connection when the agent in the virtual machine is up and running.</td>
</tr>
<tr>
<td></td>
<td>c. The client prompts the user with a message that describes the wait time estimated before the client will retry the connection.</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Enable User Session Information - This feature allows user and domain data to be used by the Cloud Monitoring Service (CMS) for reports on the Reports page. If it is disabled, the following are not provided:</td>
</tr>
<tr>
<td></td>
<td>■ The Unique User Summary feature of the Utilization report</td>
</tr>
<tr>
<td></td>
<td>■ The Session History report</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The agents on the virtual machines (RDSH and VDI) need outbound Internet access so they can send the data to Horizon Cloud.</td>
</tr>
<tr>
<td>Domain Security Settings</td>
<td>Use these settings to prevent communication of Active Directory domain names to unauthenticated users using the various Horizon clients. These settings govern whether the Active Directory domain information is sent to the client and, if sent, how it is displayed in the end-user clients' login screens. For details, see Domain Security Settings on General Settings Page.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> The combination of options selected here changes the user experience in the clients. Certain combinations can set requirements on how your end users specify their domain information in the client login screen, especially when using older clients, command-line clients, and when your environment is configured with multiple Active Directory domains. How these settings affect the client user experience depends on the client. You might need to balance your desired end-user experience according to your organization's security policies. For more information, see Domain Security Settings on General Settings Page.</td>
</tr>
</tbody>
</table>
Outbound Proxy Options

Use Proxy - Allows you to configure an outbound proxy to access internet services. To configure a proxy:

a. Click Edit.
b. Select Yes.

Proxy configuration fields display.
c. Enter information as described below.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy</td>
<td>Hostname or IP address for your proxy server.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number that is specified in your proxy server configuration.</td>
</tr>
<tr>
<td>Username</td>
<td>[Optional] Proxy authentication user name. Only required if the proxy requires authentication. Basic authentication is supported.</td>
</tr>
<tr>
<td>Password/Verify</td>
<td>[Optional] Proxy authentication user password. Only required if the proxy requires authentication. Basic authentication is supported.</td>
</tr>
<tr>
<td>Proxy Validation URL</td>
<td>URL to validate if the URL could be reached through the configured proxy. By default, <a href="https://www.vmware.com">https://www.vmware.com</a> is used.</td>
</tr>
</tbody>
</table>

d. Click Test Proxy Status to verify that the validation URL could be reached through the configured proxy setting.

Contact Info

Contact information for administrator and technical support.

4. Click Save.

Domain Security Settings on General Settings Page

You use these settings to prevent communication of Active Directory domain names to unauthenticated users using the various Horizon clients. These settings govern whether the information about the Active Directory domains that are registered with your Horizon Cloud environment is sent to the Horizon end-user clients and, if sent, how it is displayed in end-user clients' login screens.

Configuring your Horizon Cloud environment includes registering your environment with your Active Directory domains. When your end users use a Horizon client to access their entitled desktops and remote applications, those domains are associated with their entitled access. Prior to this release, the system and clients had default behavior with no options to adjust that default behavior. Starting in this release, the defaults are changed, and you can optionally use the new Domain Security Settings controls to change from the defaults.

Important When changing these settings, it can take up to 5 minutes for the update to take effect.
This topic has the following sections.

- **Domain Security Settings**
- **This Release's Default Behavior Compared with Past Releases**
- **Single Active Directory Domain Scenarios and User Login Requirements**
- **Multiple Active Directory Domain Scenarios and User Login Requirements**
- **When Your Tenant is Configured with Two-Factor Authentication**

**Domain Security Settings**

Combinations of these settings determine whether domain information is sent to the client and whether a domain selection menu is available to the end user in the client.

**Caution** These settings change the user experience in the clients. The behavior for end users using versions of Horizon Client prior to version 5.0 is different than for Horizon Client 5.0 and later. Certain combinations can set requirements on how your end users specify their domain information in the client login screen, especially when using older clients, command-line clients, and when your environment is configured with multiple Active Directory domains. How these settings affect the client user experience depends on the client. You might need to balance your desired end-user experience according to your organization's security policies. See sections **Single Active Directory Domain Scenarios and User Login Requirements** and **Multiple Active Directory Domain Scenarios and User Login Requirements**.

<table>
<thead>
<tr>
<th>Table 12-1. Domain Security Settings on the General Settings Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option</strong></td>
</tr>
<tr>
<td><strong>Show Default Domain Only</strong></td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Hide Domain Field</strong></td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td>The literal text &quot;DefaultDomain&quot;, when <strong>Show Default Domain Only</strong> is Yes. This combination is optimized for user experience in Horizon Clients older than version 5.0, while also providing improved security.</td>
</tr>
<tr>
<td>The list of domain names in a drop-down menu, when <strong>Show Default Domain Only</strong> is No.</td>
</tr>
</tbody>
</table>

**This Release's Default Behavior Compared with Past Releases**

The following table details the previous default behavior, the new default behavior, and the settings you can use to adjust the behavior to meet your organization's needs.
The system sent the names of the registered Active Directory domains to the clients.

The system sends only a literal string value (*DefaultDomain*) to the clients and not the names of the registered Active Directory domains.

**Note** Sending the literal string provides support for older Horizon clients which are implemented to expect a string list of domain names.

<table>
<thead>
<tr>
<th>Previous Release Default Behavior</th>
<th>This Release Default Behavior</th>
<th>Corresponding Domain Security Settings Combination for this Release’s Default Behavior</th>
</tr>
</thead>
</table>
| The clients displayed a drop-down menu in the login screen that presents the list of registered Active Directory domain names for the end user to choose their domain prior to logging in. | The clients display that literal string *DefaultDomain*. | Show Default Domain Only  
Default setting: Yes |
| | | Hide Domain Field  
Default setting: No |

**Single Active Directory Domain Scenarios and User Login Requirements**

The following table describes the behavior for various setting combinations when your environment has a single Active Directory domain, without two-factor authentication, and your end users use the Horizon Clients 5.0 and later versions. These clients are the newest ones starting in this release.
Table 12-2. Behavior For Horizon Clients 5.0 and Later Versions and You Have One Active Directory Domain

<table>
<thead>
<tr>
<th>Show Default Domain Only (enabled sends <em>DefaultDomain</em>)</th>
<th>Hide Domain Field</th>
<th>Horizon Client 5.0 Login Screen Details</th>
<th>How Users Log In</th>
</tr>
</thead>
</table>
| Yes                                                      | Yes               | The client's login screen has the standard user name and password fields. No domain field is displayed. No domain name is sent. The following screenshot is an example for how the resulting login screen looks like for the Windows client. | When there is a single domain, to log in, end users can enter either of the following values in the User name text box. The domain name is not required.  
  - username  
  - domain\username  
  Using the command-line client launch and specifying the domain in the command works. |
| Yes                                                      | No                | The client's login screen has the standard user name and password fields. The domain field displays *DefaultDomain*. No domain name is sent. The following screenshot is an example for how the resulting login screen looks like for the Windows client. | When there is a single domain, to log in, end users can enter either of the following values in the User name text box. The domain name is not required.  
  - username  
  - domain\username  
  Using the command-line client launch and specifying the domain in the command works. |
Table 12.2. Behavior For Horizon Clients 5.0 and Later Versions and You Have One Active Directory Domain (Continued)

<table>
<thead>
<tr>
<th>Show Default Domain Only (enabled sends <em>DefaultDomain</em>)</th>
<th>Hide Domain Field</th>
<th>Horizon Client 5.0 Login Screen Details</th>
<th>How Users Log In</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>The client's login screen has the standard user name and password fields. No domain field is displayed. The system sends the domain name to the client. Note: This combination is atypical. You would not normally use this combination because it hides the domain field even though the system is sending the domain name. The login screen looks the same as the one in the first row of this table, with no domain field displayed.</td>
<td>An end user must include the domain name in the User name text box. $\text{domain}\backslash\text{username}$</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>The client's login screen has the standard user name and password fields and a standard drop-down domain selector displays the one available domain name. The domain name is sent.</td>
<td>The end user can specify their user name in the User name text box and use the single domain that is in the list visible in the client. Using the command-line client launch and specifying the domain in the command works.</td>
</tr>
</tbody>
</table>

This table describes the behavior when your environment has a single Active Directory domain and your end users use previous versions of the Horizon clients (pre-5.0).

**Important** Using the command-line client launch of older (pre-5.0) clients and specifying the domain in the command fails for all of the combinations below. To work around this behavior, either use *DefaultDomain* for the command's domain option or upgrade the client to the 5.0 version. However, when you have more than one Active Directory domain, passing *DefaultDomain* does not work.
### Table 12-3. Behavior For Older Horizon Clients (Before 5.0) and You Have One Active Directory Domain

<table>
<thead>
<tr>
<th>Show Default Domain Only (enabled sends <em>DefaultDomain</em>)</th>
<th>Hide Domain Field</th>
<th>Pre-5.0 Horizon Client Login Screen Details</th>
<th>How Users Log In</th>
</tr>
</thead>
</table>
| Yes                                                     | Yes               | The client's login screen has the standard user name and password fields. No domain field is displayed. No domain name is sent. | An end user must include the domain name in the **User name** text box.  
  ➢ domain\username |
| Yes                                                     | No                | The client's login screen has the standard user name and password fields. The domain field displays *DefaultDomain*. No domain name is sent. | An end user must enter **username** in the **User name** text box. When the domain name is included, an error message displays that states the specified domain name does not exist in the domain list. |
| No                                                      | Yes               | The client's login screen has the standard user name and password fields. No domain field is displayed. The system sends the domain name to the client.  
  **Note**  This combination is atypical. You would not normally use this combination because it hides the domain field even though the system is sending the domain name.  
  The login screen looks the same as the one in the first row of this table, with no domain field displayed. | An end user must include the domain name in the **User name** text box.  
  ➢ domain\username |
| No                                                      | No                | The client's login screen has the standard user name and password fields and a standard drop-down domain selector displays the one available domain name. The domain name is sent. | The end user can specify their user name in the **User name** text box and use the single domain that is in the list visible in the client. |

### Multiple Active Directory Domain Scenarios and User Login Requirements

This table describes the behavior for various setting combinations when your environment has multiple Active Directory domains, without two-factor authentication, and your end users use the Horizon Clients 5.0 and later versions. These clients are the newest ones starting in this release.

Basically, the end user has to include the domain name when they type in their user name, like domain\username, except for the legacy combination where the domain names are sent and are visible in the client.
Table 12.4. Behavior For Horizon Clients 5.0 and Later Versions and You Have Multiple Active Directory Domains

<table>
<thead>
<tr>
<th>Show Default Domain Only (enabled sends <em>DefaultDomain</em>)</th>
<th>Hide Domain Field</th>
<th>Horizon Client 5.0 Login Screen Details</th>
<th>How Users Log In</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>The client's login screen has the standard user name and password fields. No domain field is displayed. No domain names are sent. The following screenshot is an example for how the resulting login screen looks like for the Windows client.</td>
<td>An end user must include the domain name in the <strong>User name</strong> text box. ▪ <code>domain\username</code> Using the command-line client launch and specifying the domain in the command works.</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>The client's login screen has the standard user name and password fields. The domain field displays <em>DefaultDomain</em>. No domain names are sent. The following screenshot is an example for how the resulting login screen looks like for the Windows client.</td>
<td>An end user must include the domain name in the <strong>User name</strong> text box. ▪ <code>domain\username</code> Using the command-line client launch and specifying the domain in the command works.</td>
</tr>
</tbody>
</table>
Table 12-4. Behavior For Horizon Clients 5.0 and Later Versions and You Have Multiple Active Directory Domains (Continued)

<table>
<thead>
<tr>
<th>Show Default Domain Only (enabled sends <em>DefaultDomain</em>)</th>
<th>Hide Domain Field</th>
<th>Horizon Client 5.0 Login Screen Details</th>
<th>How Users Log In</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>The client's login screen has the standard user name and password fields. No domain field is displayed. The system sends the domain names to the client.</td>
<td>An end user must include the domain name in the <strong>User name</strong> text box. <code>domain\username</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> This combination is atypical. You would not normally use this combination because it hides the domain field even though the system is sending the domain names.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The login screen looks the same as the one in the first row of this table, with no domain field displayed.</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>The client's login screen has the standard user name and password fields and a standard drop-down domain selector displays the list of domain names. The domain names are sent.</td>
<td>The end user can specify their user name in the <strong>User name</strong> text box and select their domain from the list visible in the client. Using the command-line client launch and specifying the domain in the command works.</td>
</tr>
</tbody>
</table>

This table describes the behavior when your environment has multiple Active Directory domains and your end users use previous versions of the Horizon clients (pre-5.0).

**Important**

- Setting **Hide Domain Field** to **Yes** allows end users to enter their domain in the **User name** text box in these pre-5.0 Horizon clients. When you have multiple domains and you want to support use of pre-5.0 Horizon clients by your end users, you must set **Hide Domain Field** to **Yes** so that your end users can include the domain name when they type in their user name.

- Using the command-line client launch of older (pre-5.0) clients and specifying the domain in the command fails for all of the combinations below. The only work around when you have multiple Active Directory domains and want to use command-line client launch is to upgrade the client to the 5.0 version.
Table 12-5. Behavior For Older Horizon Clients (Before 5.0) and You Have Multiple Active Directory Domains

<table>
<thead>
<tr>
<th>Show Default Domain Only (enabled sends <em>DefaultDomain</em>)</th>
<th>Hide Domain Field</th>
<th>Pre-5.0 Horizon Client Login Screen Details</th>
<th>How Users Log In</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>The client's login screen has the standard user name and password fields. No domain field is displayed. No domain name is sent.</td>
<td>An end user must include the domain name in the User name text box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>■ domain\username</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>The client's login screen has the standard user name and password fields. The domain field displays <em>DefaultDomain</em>. No domain name is sent.</td>
<td>This combination is unsupported for environments with multiple Active Directory domains.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>■ domain\username</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>The client's login screen has the standard user name and password fields. No domain field is displayed. The system sends the domain name to the client.</td>
<td>An end user must include the domain name in the User name text box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>■ domain\username</td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td>This combination is atypical. You would not normally use this combination because it hides the domain field even though the system is sending the domain names.</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>The client's login screen has the standard user name and password fields and a standard drop-down domain selector displays the one available domain name. The domain name is sent.</td>
<td>The end user can specify their user name in the User name text box and select their domain from the list visible in the client.</td>
</tr>
</tbody>
</table>

When Your Tenant is Configured with Two-Factor Authentication

When your Horizon Cloud tenant is configured with RSA SecureID or RADIUS two-factor authentication, end users attempting to authenticate with their Horizon clients first see a screen asking for their two-factor authentication credentials, followed by a login screen asking for their Active Directory domain credentials. When your tenant is configured with two-factor authentication, the system sends the domain list to the clients only after the end user's credentials successfully pass that initial authentication screen. The system sends the domain list regardless of the Show Default Domain Only setting.
When your tenant with two-factor authentication has multiple Active Directory domains, the optimal end-user experience is to have **Hide Domain Field** set to **No**, and have the domain selector visible on that domain login screen. That configuration allows your end users to select their domain from the drop-down menu in the second login screen, and avoid having to include their domain name when they enter their credentials into the initial authentication screen.

**Important**  When your tenant's two-factor authentication configuration has **Maintain Username** configured as **Yes**, ensure that the **Hide Domain Field** is set to **No**. Otherwise, your end users will not be able to provide the required domain information for the system to associate with their login credentials.

For information on using the Administration Console to see your tenant's two-factor authentication settings, see **2 Factor Authentication**.

The following table describes the resulting behavior from the **Hide Domain Field** setting when your tenant is configured to use two-factor authentication.
Table 12-6. When Your Tenant has Two-Factor Authentication Configured

<table>
<thead>
<tr>
<th>Domain Security Settings</th>
<th>Domain Login Screen Behavior</th>
<th>Description</th>
<th>Horizon Client Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hide Domain Field is No</td>
<td>After the end user authenticates successfully with their two-factor authentication credentials, the domain login screen contains the User name and Password fields and the Domain dropdown menu.</td>
<td>This behavior is the same as the behavior prior to this service release. After the initial two-factor authentication screen, the end user can specify their user name in the User name text box and select their domain from the list visible in the client.</td>
<td>All versions supported for this release.</td>
</tr>
</tbody>
</table>
| Hide Domain Field is Yes | After the end user authenticates successfully with their two-factor authentication credentials, the domain login screen contains the User name and Password fields only. | Avoid using this configuration if your tenant's two-factor authentication configuration has Maintain Username configured as Yes. The end user's steps are:  
- In the initial two-factor authentication screen, the end user must include their domain in the User name text box, domain\username.  
- As appropriate for your tenant's configuration, the end user completes the next two-factor authentication step, such as the domain challenge or passcode.  
- In the domain login screen, the end user provides their user name and password. | All versions supported for this release. |

**Active Directory**

This section describes the procedures for registering and configuring Active Directory domains.

Note the following:

- You must register your first Active Directory domain before you can work with any other services. All services are locked until you complete these tasks.
- When you are defining groups of users or administrators, always select ‘Security’ for the Active Directory group type, as Distribution groups are not supported.
Register Your First Active Directory Domain

You must complete the configuration by registering Active Directory, completing the domain join, and adding the Super Administrator.

**Note**  You must complete the entire Active Directory registration process before you can work with any other services. All services are locked until you complete these tasks.

**Note**  When you have completed the domain registration, do not move any groups from one organizational unit (OU) to another. Doing so will cause login failures for users.

If you click **Cancel** before you complete the registration, you can click **Edit** at any time from the Getting Started page to continue with registration.

**Prerequisites**

- The Active Directory infrastructure must be synchronized to an accurate time source.
- If you have external or forest trusts, root domains must be registered. For more information, see [External and Forest Trusts](#).
- The LDAP bind account is treated by the system as a Super Admin user, so this account should not be shared with any user that does not have Super Admin privileges. For example, if there is another product that also needs an LDAP bind account, a new LDAP account should be created for this purpose so whoever has the new account cannot log in as Super Admin.

**Procedure**

1. On the Getting Started page, select **General Setup** and then click **Configure** next to Active Directory.
2. In the Register Active Directory dialog box, provide the requested registration information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NETBIOS Name</td>
<td>Active Directory domain name</td>
</tr>
<tr>
<td>DNS Domain Name</td>
<td>Fully qualified Active Directory domain name</td>
</tr>
<tr>
<td>Protocol</td>
<td>Not editable; LDAP is the only choice</td>
</tr>
<tr>
<td>Bind Username</td>
<td>Domain administrator</td>
</tr>
<tr>
<td>Bind Password</td>
<td>Domain administrator password</td>
</tr>
</tbody>
</table>

3. Enter information for Auxiliary Account #1.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind Username</td>
<td>Domain administrator</td>
</tr>
<tr>
<td>Bind Password</td>
<td>Domain administrator password</td>
</tr>
</tbody>
</table>

**Note**  Username and password must exist in the Active Directory or the account will not be added successfully.
4 Click Advanced Properties.

5 Enter information the Advanced Properties fields.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| LDAP over TLS       | Enables LDAP communication via TLS, which automates certificate deployment and management. This option is disabled by default.  
Note: This setting is disabled by default and only appears if you have requested that VMware enable it for you. |
| Port                | The default for this field is 389. You should not need to modify this field unless you are using a non-standard port. |
| Domain Controller IP| (Optional) Specify a single preferred domain controller IP address if you want AD traffic to use a specific domain controller. |
| Context             | This option is auto-populated based on the DNS Domain Name information provided earlier.           |

6 Click Domain Bind.

Note: If you see an error stating that the auxiliary account information you entered is invalid, then after completing the Domain Join process below you will need to add a valid auxiliary account by editing the Domain Bind information. See Edit an Active Directory Domain.

7 In the Domain Join dialog, provide the required domain join information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary DNS Server IP</td>
<td>IP address of primary DNS Server</td>
</tr>
<tr>
<td>Secondary DNS Server IP</td>
<td>(Optional) IP of secondary DNS Server</td>
</tr>
<tr>
<td>Default OU</td>
<td>Default organizational unit</td>
</tr>
<tr>
<td>Join Username</td>
<td>Domain administrator</td>
</tr>
<tr>
<td>Join Password</td>
<td>Domain administrator password</td>
</tr>
</tbody>
</table>

8 If desired, create an auxiliary domain join account by entering the information below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auxiliary join Username</td>
<td>Domain administrator for auxiliary account</td>
</tr>
<tr>
<td>Auxiliary join Password</td>
<td>Domain administrator password for auxiliary account</td>
</tr>
</tbody>
</table>

- If you do not choose to add an auxiliary domain join account now, you can do so later.
- You can edit or delete this account later.
- You can add only one auxiliary domain join account for each Active Directory.

9 Click Save.

10 In the Add Super Administrator dialog box, use the Active Directory search function to select the AD administrator group to administer the application.

11 Click Save.
12 If the domain bind or domain join process fail, you must restart the registration process.
   a Restart the browser.
   b Log in first using your My VMware account.
   c Log in to the Active Directory account using the domain service (bind) account login and password.
   d Continue with the domain join process.

What to do next
If desired, you can set up True SSO (single sign-on). See Complete Configuring True SSO for your Horizon Cloud Environment.

Register Additional Active Directory Domains
You can optionally register additional Active Directory domains to assign management roles or provide assignments to users in those domains.

Note When you have completed the domain registration, do not move any groups from one organizational unit (OU) to another. Doing so will cause login failures for users.

If you click Cancel before you complete the registration, you can click Edit at any time from the Getting Started page to continue with registration.

Prerequisites
- The Active Directory infrastructure must be synchronized to an accurate time source.
- If you have external or forest trusts, root domains must be registered. For more information, see External and Forest Trusts.
- The LDAP bind account is treated by the system as a Super Admin user, so this account should not be shared with any user that does not have Super Admin privileges. For example, if there is another product that also needs an LDAP bind account, a new LDAP account should be created for this purpose so whoever has the new account cannot log in as Super Admin.

Procedure
1 In the Administration Console, select Settings > Active Directory.
2 Click Register.
3 In the Register Active Directory dialog box, provide the requested registration information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NETBIOS Name</td>
<td>Active Directory domain name</td>
</tr>
<tr>
<td>DNS Domain Name</td>
<td>Fully qualified Active Directory domain name</td>
</tr>
<tr>
<td>Protocol</td>
<td>Not editable; LDAP is the only choice</td>
</tr>
</tbody>
</table>
4 Enter information for Auxiliary Account #1.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind Username</td>
<td>Domain administrator</td>
</tr>
<tr>
<td>Bind Password</td>
<td>Domain administrator password</td>
</tr>
</tbody>
</table>

**Note** Username and password must exist in the Active Directory or the account will not be added successfully.

5 Click **Advanced Properties**.

6 Enter information the Advanced Properties fields.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP over TLS</td>
<td>Enables LDAP communication via TLS, which automates certificate deployment and management. This option is disabled by default.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This setting is disabled by default and only appears if you have requested that VMware enable it for you.</td>
</tr>
<tr>
<td>Port</td>
<td>The default for this field is 389. You should not need to modify this field unless you are using a non-standard port.</td>
</tr>
<tr>
<td>Domain Controller IP</td>
<td>(Optional) Specify a single preferred domain controller IP address if you want AD traffic to use a specific domain controller.</td>
</tr>
<tr>
<td>Context</td>
<td>This option is auto-populated based on the DNS Domain Name information provided earlier.</td>
</tr>
</tbody>
</table>

7 Click **Domain Bind**.

**Note** If you see an error stating that the auxiliary account information you entered is invalid, then after completing the Domain Join process below you will need to add a valid auxiliary account by editing the Domain Bind information. See **Edit an Active Directory Domain**.

8 In the Domain Join dialog, provide the required domain join information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary DNS Server IP</td>
<td>IP address of primary DNS Server</td>
</tr>
<tr>
<td>Secondary DNS Server IP</td>
<td>(Optional) IP of secondary DNS Server</td>
</tr>
<tr>
<td>Default OU</td>
<td>Default organizational unit</td>
</tr>
<tr>
<td>Join Username</td>
<td>Domain administrator</td>
</tr>
<tr>
<td>Join Password</td>
<td>Domain administrator password</td>
</tr>
</tbody>
</table>
9 If desired, create an auxiliary domain join account by entering the information below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auxiliary join Username</td>
<td>Domain administrator for auxiliary account</td>
</tr>
<tr>
<td>Auxiliary join Password</td>
<td>Domain administrator password for auxiliary account</td>
</tr>
</tbody>
</table>

- If you do not choose to add an auxiliary domain join account now, you can do so later.
- You can edit or delete this account later.
- You can add only one auxiliary domain join account for each Active Directory.

10 Click **Save**.

11 In the Add Super Administrator dialog box, use the Active Directory search function to select the AD administrator group to administer the application.

12 Click **Save**.

13 If the domain bind or domain join process fail, you must restart the registration process.
   a Restart the browser.
   b Log in first using your My VMware account.
   c Log in to the Active Directory account using the domain service (bind) account login and password.
   d Continue with the domain join process.

**What to do next**

If desired, you can set up True SSO (single sign-on). See Complete Configuring True SSO for your Horizon Cloud Environment.

**Edit an Active Directory Domain**

You can edit an Active Directory domain after initial setup.

**Procedure**

1 Select **Settings > Active Directory**.
   The Active Directory page displays.

2 If you have multiple Active Directories configured, select the one you want to edit from the list on the left.

3 Click **Edit** next to Domain Bind to edit domain bind information.
   The Edit Active Directory dialog displays.
Edit information as desired in the fields described below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NETBIOS Name</td>
<td>[Not editable] Active Directory domain name</td>
</tr>
<tr>
<td>DNS Domain Name</td>
<td>Fully qualified Active Directory domain name</td>
</tr>
<tr>
<td>Protocol</td>
<td>[Not editable] LDAP is the only choice</td>
</tr>
<tr>
<td>Bind Username</td>
<td>Domain administrator. Edit only if new username is set up in Active Directory first.</td>
</tr>
<tr>
<td>Bind Password</td>
<td>Domain administrator password. Edit only if new password is set up in Active Directory first.</td>
</tr>
</tbody>
</table>

Make changes to auxiliary bind accounts as described below.

- Change password for an auxiliary bind account:
  1. Confirm that the password for the account has already been changed in the Active Directory.
  2. Click the Change Account Password link for the account (for example, Change Account #1 Password).
  3. Enter the new password.

  **Note** You cannot change the bind username for an auxiliary bind account. Instead, you need to remove the account and add it with the new username.

- Add an auxiliary bind account:
  1. Click the **Add Auxiliary Bind Account** link.
  2. Enter username and password for the account.

  **Note** Username and password must exist in the Active Directory or the account will not be added successfully.

- Remove an auxiliary bind account by clicking the **Remove** link next to the account.

  **Note** You cannot remove an auxiliary bind account if it is the last auxiliary bind account remaining.

Click **Advanced Properties**.

Edit information as desired in the following Advanced Properties fields.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP over TLS</td>
<td>Enables LDAP communication via TLS, which automates certificate deployment and management. This option is disabled by default.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This setting is disabled by default and only appears if you have requested that VMware enable it for you.</td>
</tr>
<tr>
<td>Port</td>
<td>The default for this field is 389. You should not need to modify this field unless you are using a non-standard port.</td>
</tr>
</tbody>
</table>
Option | Description
--- | ---
Domain Controller IP | (Optional) Specify a single preferred domain controller IP address if you want AD traffic to use a specific domain controller.

**Context**
This option is auto-populated based on the DNS Domain Name information provided earlier.

8 Click **Domain Bind** to save changes.

9 Click **Edit** next to Domain Join to edit domain join information.

The Domain Join dialog displays.

10 Edit domain join information as desired.

**Note** To make changes to Primary DNS Server IP or Secondary DNS Server IP, you must file a ticket with VMware support.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default OU</td>
<td>Default organizational unit</td>
</tr>
<tr>
<td>Join Username</td>
<td>Domain administrator. Edit only if new username is set up in Active Directory first.</td>
</tr>
<tr>
<td>Join Password</td>
<td>Domain administrator password. Edit only if new password is set up in Active Directory first.</td>
</tr>
</tbody>
</table>

11 Make changes to the auxiliary join account as described below.

- **Add an auxiliary join account:**
  1. Click the **Add Auxiliary Join Account** link.
  2. Enter username and password for the account.

  **Note** Username and password must exist in the Active Directory or the account will not be added successfully.

- **Change username for the auxiliary join account:**
  1. Confirm that the username for the account has already been changed in the Active Directory.
  2. Enter the new username in the Auxiliary join Username field.

- **Change password for the auxiliary join account:**
  1. Confirm that the password for the account has already been changed in the Active Directory.
  2. Enter the new password in the Auxiliary join Password field.

- **Remove the auxiliary join account** by clicking the **Remove Auxiliary Join Account** link.

12 Click **Save**.

13 In the Add Super Administrator dialog box, make any desired change and click **Save**.

Use the Active Directory search function to select the AD administrator group to administer the system.
What to do next

If desired, you can set up True SSO (single sign-on). See Complete Configuring True SSO for your Horizon Cloud Environment.

Service Accounts That Horizon Cloud Requires For Its Operations

Horizon Cloud requires use of two accounts in your Active Directory (AD) domain to use as service accounts. This topic describes the requirements that those two accounts must meet.

Horizon Cloud requires that you specify two AD accounts to use as these two service accounts.

- A domain bind account that is used to perform lookups in your AD domain.
- A domain join account that is used for joining computer accounts to the domain and performing Sysprep operations.

You use the Administration Console to provide the credentials for these accounts to Horizon Cloud.

You must ensure the Active Directory accounts you specify for these service accounts meet the following requirements that Horizon Cloud requires for its operations.

**Important** You must ensure that your domain bind and domain join accounts continue to have the permissions as described here on all of the OUs and objects that you are using and expect to use with the system. Horizon Cloud cannot pre-populate or predict in advance which Active Directory groups you might want to use in the environment. You must configure Horizon Cloud with the domain bind account and domain join account using the Administration Console.

Domain Bind Account Requirements

- The domain bind account cannot expire, change, or be locked out. You must use this type of account configuration because the system uses the primary domain bind account as a service account to query Active Directory. If the primary domain bind account becomes inaccessible for some reason, the system then uses the auxiliary domain bind account. If both the primary and auxiliary domain bind accounts expire or become inaccessible, then you will not be able to log in to the Administration Console and update the configuration.

  **Important** If both the primary and auxiliary domain bind accounts expire or become inaccessible, then you will not be able to log in to the Administration Console and update the configuration with working domain bind account information. If you choose not to set *Never Expires* on the primary or auxiliary domain bind accounts, you should make them have different expiration times. You will have to keep track as the expiration time approaches and update your Horizon Cloud domain bind account information before the expiration time is reached.

- The domain bind account requires the `sAMAccountName` attribute.
At a minimum, the domain bind account must have read permissions which can look up AD accounts for all of the AD organizational units (OUs) that you anticipate using in the Desktop-as-a-Service operations that Horizon Cloud provides, such as assigning desktop VMs to your end users. The domain bind account needs the ability to enumerate objects from your Active Directory.

**Important** The typical default settings in Active Directory give a standard domain user account the ability to do that enumeration. However, if you have limited the security permission in your Active Directory, you must ensure that the domain bind account has read permissions for all of the OUs and objects that you anticipate and expect you will use with Horizon Cloud.

### Domain Join Account Requirements

- The domain join account cannot change or be locked out.
- Ensure you meet at least one of the following criteria:
  - In your Active Directory, set the domain join account to **Never Expires**.
  - Alternatively, configure an auxiliary domain join account that has a different expiration time than the first domain join account. If you choose this method, ensure that the auxiliary domain join account meets the same requirements as the main domain join account you configure in the Administration Console.

**Caution** If the domain join account expires and you have no working auxiliary domain join account configured, Horizon Cloud operations for sealing images and provisioning farm server VMs and VDI desktop VMs will fail.

- The domain join account requires the sAMAccountName attribute.
- The domain join account needs the AD permissions in the following list.

**Important** Some of the AD permissions in the list are typically assigned by Active Directory to accounts by default. However, if you have limited the security permission in your Active Directory, you must ensure that the domain join account has these permissions for the OUs and objects that you anticipate and expect to use with Horizon Cloud.

The system performs explicit permission checks on the domain join account within the OU you specify in the Active Directory registration workflow (in the Default OU field in that workflow) and within the OUs you specify in the farms and VDI desktop assignments you create, if those farm and VDI desktop assignment **Computer OU** fields are different from the default OU in the Active Directory registration.

To cover the cases where you might ever use a sub-OU, a best practice is for you to set these permissions to apply for all descendant objects of the Computer OU. The AD permissions required on the domain join account are:

- List Contents [For Descendant Objects of Computer OU]
- Read All Properties [For Descendant Objects of Computer OU]
- Write All Properties [For Descendant Objects of Computer OU]
- Read Permissions [For Descendant Objects of Computer OU]
- Reset Password [For Descendant Computer Objects of Computer OU]
- Create Computer Objects [For Descendant Objects of Computer OU]
- Delete Computer Objects [For Descendant Objects of Computer OU]

**Caution** Notice that the Reset Password permission is slightly different from the others. Reset Password permission is specifically For Descendant Computer Objects.

For the other six permissions, setting Full Control might not work in all cases to satisfy the system's permission checking on the domain join account. Using Full Control and expecting it to satisfy the system's permissions checks might not always work.

**Caution** If you are going to use Instant Clone images, there are additional requirements on the domain join account. In addition to the OU that you specify in the Administration Console when you register the Active Directory domain, the domain join account must also have these permissions listed on any OU or sub-OU in which you want to place a desktop built from an Instant Clone image.

- List Contents
- Read All Properties
- Write All Properties
- Read Permissions
- Reset Password
- Create Computer Objects
- Delete Computer Objects

**Notifications When the Primary Domain-Bind Account is Locked Out**

When Horizon Cloud detects an authentication failure due to a locked primary domain-bind account, a notification is displayed in the Administration Console to alert you to remedy the state of the account. The system uses the primary domain-bind account as a service account to connect to the Active Directory (AD) server and query Active Directory.
Each time an administrator successfully logs in to the Administration Console, the system checks whether the primary domain-bind account is in a failed or inactive state. If the system determines the account is in a failed or inactive state, a notification is created. When the notification is created, it is added to the Notifications page and is reflected in the count on the bell icon located in the upper right corner of the console ( annunciator). You can read the notification details by clicking the bell icon or by navigating to the Notifications page.

**Note** The connection state for the connection between the system and the AD server is cached for 15 minutes. As a result, it might take up to 15 minutes from the time the primary domain-bind account goes into a locked-out state until the notification is reflected in the Administration Console. For example, if you log in to the Administration Console, and then manually locked out your primary domain-bind account in your AD server, it might take up to 15 minutes for the notification to display in the console. Similarly, if you see the lockout notification in the console and then fix the account in your AD server, the console might continue to show the account lockout notification for up to 15 minutes after the fix.

If the primary domain-bind account becomes locked out, the system falls back to use an active configured auxiliary domain-bind account to authenticate the connection to the Active Directory server. When you see a notification that the primary domain-bind account is locked out, you should take action to remedy the state of the primary domain-bind account to ensure successful system connection continues over time.

**Configure True SSO for Use with Your Horizon Cloud Environment**

After you have registered an Active Directory domain with your Horizon Cloud environment, you can configure True SSO for it. True SSO is a feature that integrates with VMware Identity Manager™ to allow users to single sign-on to the virtual Windows desktops and applications served by Horizon Cloud without needing to also enter their Active Directory credentials into the Windows operating system. When True SSO is configured for your environment, the end users authenticate by logging into VMware Identity Manager™. After that authentication, the user is able to launch their entitled desktops or applications without a prompt for Active Directory credentials.

Configuring True SSO for use with your environment is a multi-step process. At a high-level, the steps are:

1. Set up the infrastructure required for True SSO to operate, which involves:
   a. Installing and configuring a Windows Server Certificate Authority (CA) to be an enterprise CA. The procedures in this section are for Windows Server 2012 R2. Very similar steps can be followed on Windows Server 2008 R2.
   b. Setting up a certificate template on the CA.
   c. Downloading the Horizon Cloud pairing bundle from the Administration Console’s Active Directory page. The pairing bundle is used when setting up the Enrollment Server.
   d. Setting up the Enrollment Server.
2. Adding the Enrollment Server information to the Administration Console’s Active Directory page.
When the configuration is complete, the CA will issue certificates on behalf of the users, and those certificates will be used to log the users in to their allocated desktops. Horizon Cloud appliance will ask the ES to issue certificates on behalf of users. The ES will generate the requested certificate on behalf of the requested user via the CA and return it to the Horizon Cloud appliance.

Prerequisites

Before configuring True SSO, you must first have at least one VMware Identity Manager™ configuration on the Identity Management page. See Identity Management Page.

Procedure

1. **Install and Configure a Windows Server 2012 R2 Certificate Authority**
   You can set up a Windows Server 2012 Certificate Authority (CA) using the Service Manager wizard.

2. **Set Up a Certificate Template on the CA**
   You must configure the certificate template on the CA. The certificate template is the basis for the certificates that the CA generates.

3. **Download the Horizon Cloud Pairing Bundle**
   You need this pairing bundle to complete the Enrollment Server setup steps when you are configuring your Horizon Cloud environment for True SSO. You download the pairing bundle from the Administration Console's Active Directory page.

4. **Set up the Enrollment Server**
   The Enrollment Server (ES) is a Horizon Cloud component that you install on a Windows Server machine as the last step in setting up infrastructure for True SSO. By deploying the Enrollment Agent (Computer) certificate onto the server, you are authorizing this ES to act as an Enrollment Agent and generate certificates on behalf of users.

5. **Complete Configuring True SSO for your Horizon Cloud Environment**
   After the Enrollment Server is set up, you enter the information in the Administration Console's Active Directory page.

After completing the steps, your environment is configured with True SSO.

**Install and Configure a Windows Server 2012 R2 Certificate Authority**

You can set up a Windows Server 2012 Certificate Authority (CA) using the Service Manager wizard.

The following are standard steps to set up a Microsoft CA. They are detailed here in a simple form suitable for use in a lab environment, but for a real production system it is recommended that you follow industry best practice for CA configuration.

If you need further guidance about setting up a CA, please check out the standard Microsoft technical references: Active Directory Certificate Services Step-by-Step Guide and Install a Root Certification Authority.

**Note** The procedures in this topic are for Windows Server 2012 R2. Very similar steps can be followed on Windows Server 2008 R2.
Procedure

1. On the Server Manager Dashboard, click **Add Roles and Features** to open the wizard, and then and click **Next**.

2. On the Select Installation Type page, select Role-based or feature-based installation and click **Next**.

3. On the Server Selection page, leave defaults and click **Next**.

4. On the Server Roles page:
   b. In the dialog, select Include management tool (if applicable) and click **Add Features**.
   c. Click **Next**.

5. On the Features page, click **Next**.

6. On the AD CS page, click **Next**.

7. On the Role Services page, select Certification Authority and click **Next**.

8. On the Confirmation page, select Restart the destination server automatically is required and click **Install**.

   Installation Progress displays. When the installation is complete, a URL link displays, allowing you to configure the newly installed CA as “Configure Active Directory Certificate Services” on the destination server.

9. Click on the configuration link to launch the configuration wizard.

10. On the Credentials page, enter user credentials from Enterprise Admin group and click **Next**.

11. On the Role Services page, select CA and click **Next**.

12. On the Setup Type page, select Enterprise CA and click **Next**.

13. On the CA Type page, select Root or Subordinate CA as appropriate (in this example it is a Root CA) and click **Next**.

14. On the Private Key page, select Create a new private key and click **Next**.

15. On the Cryptography page, enter information as follows.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptographic Provider</td>
<td>RSA#Microsoft Software Key Storage Provider</td>
</tr>
<tr>
<td>Key Length</td>
<td>4096 (or another length if you prefer)</td>
</tr>
<tr>
<td>Hash Algorithm</td>
<td>SHA256 (or another SHA algorithm if you prefer)</td>
</tr>
</tbody>
</table>

16. On the CA Name page, configure as preferred or accept defaults and click **Next**.

17. On the Validity Period page, configure as preferred and click **Next**.

18. On the Certificate Database page, click **Next**.

19. On the Confirmation page, review the information and click **Configure**.
Complete the configuration process by performing the following tasks (run all commands from the command prompt).

a Configure CA for non-persistent certificate processing

```
certutil -setreg DBFlags 
+DBFLAGS_ENABLEVOLATILEREQUESTS
```

b Configure CA to ignore offline CRL errors

```
certutil -setreg ca\CRLFlags 
+CRLF_REVCHECK_IGNORE_OFFLINE
```

c Restart the CA service

```
net stop certsvc
net start certsvc
```

Set up a certificate template on the CA by following the steps in Set Up a Certificate Template on the CA.

**Set Up a Certificate Template on the CA**

You must configure the certificate template on the CA. The certificate template is the basis for the certificates that the CA generates.

**Prerequisites**

Complete the steps described in Install and Configure a Windows Server 2012 R2 Certificate Authority.

**Procedure**

1 Create a new Universal Security Group.

Creating this group allows you to have a single Security Group to which you can assign the permissions required for issuing certificates on behalf of users. All the computers where VMware Enrollment Servers are installed can inherit those permissions by becoming a member of this group.

a Click **Start** and type `dsa.msc`.

The Active Directory Users and Computers window displays.

b In the tree, right-click the **Users** folder for the domain controller and select **New > Group**.

The New Object - Group window displays.

c In the **Group Name** field, enter a name for the new group. For example, TrueSSO Enrollment Servers.
d Set the following values.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group scope</td>
<td>Universal</td>
</tr>
<tr>
<td>Group type</td>
<td>Security</td>
</tr>
</tbody>
</table>

e Click **OK**.

The new group appears in the tree in the Active Directory Users and Computers window.

f Right-click the group and select **Properties**.

g On the Member Of tab, add every computer on which you will be installing an Enrollment Server, and then click **OK**.

h Restart every computer on which you will be installing an Enrollment Server.

2 Configure the certificate template.

a Select **Control Panel > Administrative Tools > Certificate Authority**.

b In the tree, expand the local CA name.

c Right-click on the Certificate Templates folder and select **Manage**.

The Certificate Templates Console displays.

d Right-click on the Smartcard Logon template and select **Duplicate Template**.

The Properties of New Template window displays.
Enter information on the tabs of the window as described below.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compatibility</td>
<td>- Select the <strong>Show resulting changes</strong> check box.</td>
</tr>
<tr>
<td></td>
<td>- Certification Authority - Windows Server 2008 R2</td>
</tr>
<tr>
<td></td>
<td>- Certificate recipient - Windows 7 / Server 2008 R2</td>
</tr>
<tr>
<td>General</td>
<td>- Template display name - Name of your choice. For example, True SSO Template.</td>
</tr>
<tr>
<td></td>
<td>- Template name - Name of your choice. For example, True SSO Template.</td>
</tr>
<tr>
<td></td>
<td>- Validity period - 1 hours</td>
</tr>
<tr>
<td></td>
<td>- Renewal period - 0 weeks</td>
</tr>
<tr>
<td>Request Handling</td>
<td>- Purpose - Signature and smartcard logon</td>
</tr>
<tr>
<td></td>
<td>- Select the <strong>For automatic renewal of smart card certificates</strong>... check box</td>
</tr>
<tr>
<td></td>
<td>- Select the <strong>Prompt the user during enrollment</strong> radio button</td>
</tr>
<tr>
<td>Cryptography</td>
<td>- Provider Category - Key Storage Provider</td>
</tr>
<tr>
<td></td>
<td>- Algorithm name - RSA</td>
</tr>
<tr>
<td></td>
<td>- Minimum key size - 2048</td>
</tr>
<tr>
<td></td>
<td>- Select the <strong>Requests can use any provider available</strong>... radio button</td>
</tr>
<tr>
<td></td>
<td>- Request hash - SHA256</td>
</tr>
<tr>
<td>Subject Name</td>
<td>- Select the <strong>Build from this Active Directory Information</strong> radio button</td>
</tr>
<tr>
<td></td>
<td>- Subject name format - Fully distinguished name</td>
</tr>
<tr>
<td></td>
<td>- Select the <strong>User principal name (UPN)</strong> check box.</td>
</tr>
<tr>
<td>Server</td>
<td>- Select the <strong>Do not store certificates and requests in the CA database</strong> check box</td>
</tr>
<tr>
<td>Issuance Requirements</td>
<td>- Require the following for enrollment - Select <strong>This number of authorized signatures</strong> and enter 1.</td>
</tr>
<tr>
<td></td>
<td>- Policy type required in signature - Application policy</td>
</tr>
<tr>
<td></td>
<td>- Application policy - Certificate Request Agent</td>
</tr>
<tr>
<td></td>
<td>- Require the following for enrollment - Valid existing certificate</td>
</tr>
<tr>
<td>Security</td>
<td>- In the upper part of the tab, select the new group you created. Then in the lower part of the tab, select <strong>Allow</strong> for Read and Enroll permissions.</td>
</tr>
</tbody>
</table>

Click **OK**.

Issue the template for True SSO.

a. Right-click again on the Certificate Templates folder and select **New > Certificate Template to Issue**.

The Enable Certificate Templates window displays.

b. Select TrueSsoTemplate and click **OK**.
4 Issue the Enrollment Agent template.
   a Right-click again on the Certificate Templates folder and select **New > Certificate Template to Issue**.
      The Enable Certificate Templates window displays.
   b Select the Enrollment Agent computer and click **OK**.
      
      **Note** This template must have the same security settings as the template issued in the previous step.

The CA is now set up and configured with a certificate template suitable for use with True SSO.

5 Download the Horizon Cloud pairing bundle by following the steps in **Download the Horizon Cloud Pairing Bundle**.

**Download the Horizon Cloud Pairing Bundle**

You need this pairing bundle to complete the Enrollment Server setup steps when you are configuring your Horizon Cloud environment for True SSO. You download the pairing bundle from the Administration Console’s Active Directory page.

The pairing bundle contains the Horizon Cloud tenant appliances’ certificate files in CRT format that you upload to the Enrollment Server.

**Procedure**

1 In the Administration Console, navigate to **Settings > Active Directory**.

2 In the True SSO Configuration area, obtain the `pairing_bundle.7z` file by clicking **Download Pairing Token**.

3 Save the file to a location where you can extract its contents.

4 Extract the CRT files from the pairing bundle to a location where you can retrieve them when you are setting up the Enrollment Server.

5 Set up the Enrollment Server by following the steps in **Set up the Enrollment Server**.

**Set up the Enrollment Server**

The Enrollment Server (ES) is a Horizon Cloud component that you install on a Windows Server machine as the last step in setting up infrastructure for True SSO. By deploying the Enrollment Agent (Computer) certificate onto the server, you are authorizing this ES to act as an Enrollment Agent and generate certificates on behalf of users.

**Prerequisites**

Verify that you have completed the steps in **Install and Configure a Windows Server 2012 R2 Certificate Authority**, **Set Up a Certificate Template on the CA**, and **Download the Horizon Cloud Pairing Bundle**.
Procedure

1 Install the Enrollment Server.
   a Download the Enrollment Server.exe file from the My VMware site. The file name should be similar to VMware-HorizonCloud-TruessoEnrollmentServer-x86_64-7.3.0-xxxxx.exe.
   b Confirm that the system is running Windows Server 2008 R2, 2012 R2, or 2016, and that it has a minimum of 4GB memory.
   c Run the installer and follow the wizard.

2 Deploy the Enrollment Agent (Computer) Certificate.
   a Open the Microsoft Management Console (MMC).
   b On the File menu, click Add/Remove Snap-in.
   c Under Available snap-ins, double-click Certificates.
   d Select Computer account and click Next.
   e Select Local computer and click Finish.
   f On the Add or Remove Snap-ins dialog, click OK.
   g In the MMC, right-click the Personal folder under Certificates and select All Tasks > Request New Certificates.
   h In the Certificate Enrollment dialog, select the check box for the Enrollment Agent (Computer) and click Enroll.

3 Import the certificate CRT files extracted from the pairing_bundle.7z file.
   a In the MMC, right-click the Certificates sub-folder under the VMware Horizon Cloud Enrollments Server Trusted Roots folder and select All Tasks > Import.
   b Click Next.
   c Navigate to the location where you unzipped the certificate files from the pairing_bundle.7z bundle.
   d Import the two certificate files one at a time.
   e Click Next, then click Finish.

4 Complete the remaining configuration steps described in Complete Configuring True SSO for your Horizon Cloud Environment.

Complete Configuring True SSO for your Horizon Cloud Environment

After the Enrollment Server is set up, you enter the information in the Administration Console’s Active Directory page.

Prerequisites

Complete the previous step Set up the Enrollment Server.
Procedure

1. In the Administration Console, navigate to Settings > Active Directory.

2. Click Add next to True SSO Configuration. The True SSO Config dialog displays. 
   
   **Note** Because you already configured the Enrollment Server you can ignore the Download Pairing Token link in this dialog.

3. Enter the fully-qualified domain name (FQDN) of your enrollment server in the Primary Enrollment Server field and click the Test Pairing button next to the field. The other required fields are auto-populated.

4. Click Save

5. To configure a Secondary Enrollment Server for high-availability, do the following.

   a. Repeat the process described in Set up the Enrollment Server on a second machine.

   b. Edit the True SSO configuration and add the second ES address in the Secondary Enrollment Server field, and then test the pairing.

   c. Save the configuration again.

   The configuration information now appears on the Active Directory page under True SSO Configuration.

External and Forest Trusts

The system supports traversing external (or forest) trusts between domains in different forests. This includes:

- Assignment/entitlement of users/groups in one forest to resources in a different forest.
- Support for one-way trusts.

For this functionality to work, you must do the following.

- Register all domains from all forests that contain accounts and desktops you wish to use.

- Register forest root domains from both sides of a forest trust. This is required to allow the tenant to connect to the forest roots and decode the relevant TDO. This requirement holds even if there are no DaaS desktops or users in the forest root domains.

- Enable global catalog for at least one of the registered domains in each forest. For optimal performance all registered domains should have global catalog enabled.

- To entitle groups from different forests to a desktop, register at least one universal group from each forest. Entitlement/assignment using domain local groups is not supported. As a result, the system filters out FSPs from ‘member’ attribute DNs and tokenGroups.

- Follow a hierarchical structure with regard to DNS name and root naming context for forest domains. For example, if the parent domain is called example.edu, a child domain could be called vpc.example.edu but not vpc.com.
Avoid having a domain from an externally trusted forest with a clashing NETBIOS name, as such domains will be excluded. The registered NETBIOS name will always take precedence over a clashing NETBIOS name found during enumeration of a trusted forest's domains.

## Edit Roles and Permissions

Use the Administration Console's role-based access control to determine which administrative privileges are granted to which of your Active Directory user accounts.

These roles and their associated rights determine which management actions a user can perform using the Administration Console. The visibility of the Administration Console's features and elements is controlled by the role assigned to the person's Active Directory account. For example, a person in an Active Directory group that is assigned the **Help Desk Read Only Administrator** role can navigate to the user cards for end users and view the information, but not perform operations on the desktops. A person in an Active Directory group that is assigned the **Help Desk Administrator** role can navigate to the user cards and perform troubleshooting operations as well as view the information. You must assign a role to your organization's appropriate Active Directory groups before the users in that group can log in to the Administration Console's second login screen and access management actions.

### Prerequisites

**Caution**  Prior to assigning roles to your existing Active Directory groups, review the user account membership in the Active Directory groups to ensure a user account receives only one of these Horizon Cloud roles. Create specific Active Directory groups if needed. Because these roles are assigned at the level of the Active Directory group, some unexpected results can occur if a user's Active Directory account belongs to two Active Directory groups and each group is assigned a different role. The Administration Console features are visible according to this precedence order:

1. **Super Administrator**
2. **Help Desk Administrator**
3. **Demo Administrator**
4. **Help Desk Read Only Administrator**

As a result of this precedence order, if a user's Active Directory account belongs to both Active Directory groups ADGroup1 and ADGroup2, and you assign the **Super Administrator** role to ADGroup1 and assign the **Help Desk Read Only Administrator** role to ADGroup2, the Administration Console will display all of the features according to the **Super Administrator** role, instead of the subset of features for the other role, because the **Super Administrator** role takes precedence.

### Procedure

1. Select **Settings > Roles & Permissions**.

   The Roles & Permissions page displays.

   There are four default roles, shown below.
<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super Administrator</td>
<td>A mandatory role that you must assign to at least one group in your Active Directory domain and optionally to others. This role grants all the permissions to perform management actions in the Administration Console. <strong>Important</strong> Ensure that the domain-join account that you specified when registering the Active Directory domain with the first node is in one of the groups given the Super Administrator role. For the end-to-end success of operations involving images and domain join operations, that domain-join account must be granted this Super Administrator role.</td>
</tr>
</tbody>
</table>
| Help Desk Administrator   | A role that you can optionally assign to one or more groups. The purpose of this role is to provide access to the Administration Console so that your Active Directory groups with this role can work with the user card features to:  
  - See the status of end user sessions.  
  - Perform troubleshooting operations on the sessions.                                                                                                                                                                                                                                                                                                                                                           |
| Help Desk Read Only       | A role that you can optionally assign to one or more groups. The purpose of this role is to provide access to the Administration Console so that your Active Directory groups with this role can work with the user card features to see the status of end user sessions.                                                                                                                                                                                                                                                                     |
| Demo Administrator        | A read-only role that you can optionally assign to one or more groups. Demo administrators can view the settings and select options to see additional choices in the console, but the selections do not change the configuration settings.                                                                                                                                                                                                                                                                                          |

2. Select a role from the Roles list and click **Edit**.

3. In the edit dialog, use the Active Directory search function to select a group for the role and click **Save**. **Important** These roles can be assigned to groups only. The Administration Console does not provide a way to choose individual Active Directory user accounts for each role.

This point is critical for the domain-join account. If the domain-join account that you registered for your initial node is not already in one of your Active Directory groups, create an Active Directory group for that account so that you can ensure the Super Administrator role can be assigned to that domain-join account. That domain-join account must be given the Super Administrator role.

**Note** Do not add the same group to both the Super-Administrator role and the Demo-Administrator role. Doing so can cause users in that group not to have full access to all expected functions.

## Managing File Shares

You can set up file shares to import data into the user interface.

- You create a file share on a separately-managed machine outside of the user interface and then add it on the File Share page.
- After the file share has been added to the system, the contents are imported either automatically or manually, depending on the functionality involved.
Create a File Share

You can create a file share outside of the user interface.

There are two types of file shares, depending on what the file share contains.

- **Agents file shares** are used only to import agent software updates.
- **VMs file shares** are used to import VMs and to store downloaded VM logs.

**Note**

- If you want to use the agent update feature and have multiple tenants, you must create an Agents file share on each of the tenants.
- If you want to import VMs and have multiple tenants, you must create a VMs file share on each of the tenants.
- You can only have one of each type of file share (that is, one Agents file share and one VMs file share) on a tenant at any given time.

**Procedure**

1. Create a Windows folder following the usual procedure.
   - If this is an Agent file share (that is, a file share for use with Agent Software Update), you must name the folder ‘agentFiles’. Later the system will create several subfolders, only two of which you use. These subfolders are described below.

<table>
<thead>
<tr>
<th>Subfolder Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdsClient</td>
<td>This folder will contain agent files downloaded automatically from the upgrade server that your VMware representative has configured for you.</td>
</tr>
<tr>
<td>hotpatch</td>
<td>This folder will contain any agent files that you manually put into it. You will not have any need to do this unless specifically asked to do so by your VMware representative.</td>
</tr>
</tbody>
</table>

   - If this is VMs file share, the name can be anything you choose.

2. Make the following settings for the file share folder:
   - Confirm that the file share is joined to the tenant domain.
   - Enable sharing.
   - Add a domain user to the permissions.

3. Note the following information, which you will need when adding the file server in the user interface:
   - Username and password of the domain user used you added in the previous step.
   - Source path of the file share folder.

**What to do next**

Add the file share in the user interface. See *Add a File Share on the File Share Page*. 
Add a File Share on the File Share Page

After you create a file share outside of the user interface, you can add it on the File Share page.

There are two types of file shares, as described below. You can only have one of each type of file share in your environment at any given time.

Prerequisites

In order to add a file share on the File Share page, you must first create it outside of the user interface. See Create a File Share.

**Note** When you add a file share, the contents of the file share (agent files or VMs) are imported into the system. If you put new content into the file share later, you can import that content using the Import function.

Procedure

1. Select **Settings > File Share**.
2. Click **New**.
3. Provide the required information in the New File Share dialog box.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the file share.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain of the file share. Select from the drop-down list.</td>
</tr>
<tr>
<td>Username</td>
<td>Admin user for the file share.</td>
</tr>
<tr>
<td>Password</td>
<td>Admin password for the file share.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of file share. Select Agents or VMs, depending on what the file share contains.</td>
</tr>
<tr>
<td></td>
<td>Agents file shares are used only to import agent software updates.</td>
</tr>
<tr>
<td></td>
<td>VMs file shares are used to import VMs and to store downloaded VM logs.</td>
</tr>
</tbody>
</table>

**Note**

- If you want to use the agent update feature and have multiple tenants, you must create an Agents file share on each of the tenants.
- If you want to import VMs and have multiple tenants, you must create a VMs file share on each of the tenants.
- You can only have one of each type of file share (that is, one Agents file share and one VMs file share) on a tenant at any given time.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Path</td>
<td>Network path to file share.</td>
</tr>
<tr>
<td>Destination Pod</td>
<td>[VMs Type only] This field only displays if you have multiple pods on the tenant. Select the pod from the drop-down list.</td>
</tr>
</tbody>
</table>

4. Click **Save**.
Edit a File Share
You can edit the name, source path, and destination pod of a file share.

Procedure
1. Select Settings > File Share.
2. Select the check box next to the file share to edit.
3. Click Edit and make your changes.
4. Click Save.

Remove a File Share
You can remove a file share on the File Share page.

Procedure
1. On the File Share page, select the file share to remove.
2. Click Remove and confirm you want to remove the file share.
   The file share no longer appears in the list.

Import the Contents of a File Share
You can import the contents of a file share on the File Share page.

Procedure
1. Select Settings > File Share.
2. On the File Share page, select the file share.
3. Click the "..." button and select Import.
   - In most cases, all files will be imported automatically, and will be available on the appropriate page of the user interface.

<table>
<thead>
<tr>
<th>File Type</th>
<th>User Interface Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>Assignments page (see Update Agent Software for an Assignment).</td>
</tr>
<tr>
<td>VM</td>
<td>Imported VMs page (see Chapter 11 Imported VMs).</td>
</tr>
</tbody>
</table>

- If there is an agent file being delivered as a hotpatch, you will be prompted to enter the hash value that you received from your VMware representative. You have no need to use this functionality unless specifically asked to by your VMware representative.
Managing Utility VMs

Utility VMs are discovered VMs with unsupported operating systems used for infrastructure services such as DHCP.

You can perform the following actions using buttons at the top of the page.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rename</td>
<td>Select a VM and click <strong>Rename</strong>. Enter a new name in the field and click <strong>Save</strong>.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>For this action to be successful, the selected VM must be paired with the tenant using Agent Pairing, and the DaaS Agent must be in Active state.</td>
</tr>
<tr>
<td>Shutdown</td>
<td>Shuts down the VM(s).</td>
</tr>
<tr>
<td></td>
<td>- You can select more than one VM at a time.</td>
</tr>
<tr>
<td></td>
<td>- VM status must be green.</td>
</tr>
<tr>
<td></td>
<td>- You can only shut down VMs that do not have active user sessions.</td>
</tr>
<tr>
<td>Restart</td>
<td>Performs a 'graceful' restart of the VM(s), allowing you to recover hung VMs without loss of data. If this does not work, it may be necessary to use the Reset menu option, which performs a hard reset of the VM and can result in data loss.</td>
</tr>
<tr>
<td></td>
<td>- You can select more than one VM at a time.</td>
</tr>
<tr>
<td></td>
<td>- VM status must be green.</td>
</tr>
</tbody>
</table>

You can perform the following actions by clicking the "..." button and making a selection from the drop-down menu.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspend</td>
<td>Suspends the selected VM.</td>
</tr>
<tr>
<td>Resume</td>
<td>Resumes operation of the selected VM.</td>
</tr>
<tr>
<td>Power On</td>
<td>Powers on the selected VM.</td>
</tr>
<tr>
<td>Power Off</td>
<td>Powers off the selected VM.</td>
</tr>
<tr>
<td>Reset</td>
<td>Resets the selected VM.</td>
</tr>
<tr>
<td>Reset Agent Pairing</td>
<td>Repairs the agent pairing state when pairing failure has occurred.</td>
</tr>
<tr>
<td></td>
<td>- You can select multiple VMs. The action will only be applied to those selected VMs that are currently powered on.</td>
</tr>
<tr>
<td></td>
<td>- You can view progress on the Monitor &gt; Activity page.</td>
</tr>
<tr>
<td>Launch Console</td>
<td>Launches a console for the selected desktop. This option is disabled if the VM is powered off or if more than one VM is selected.</td>
</tr>
<tr>
<td>Migrate To Imported VMs</td>
<td>Moves the VM to the Imported VMs page. See Chapter 11 Imported VMs.</td>
</tr>
</tbody>
</table>

2 Factor Authentication

The system supports RSA SecurID and Radius authentication for internal users.

To enable 2 Factor Authentication for users on your internal network, see Set Up Authentication with RADIUS and Set Up Authentication with RSA SecurID.
Set Up Authentication with RADIUS

You can use RADIUS to enable 2 Factor Authentication for end users.

**Note**  Make sure that primary and secondary tenant appliance IP addresses are registered as clients in the RADIUS server. Obtain the tenant appliance IP addresses from your VMware representative.

**Procedure**

1. Select **Settings > 2 Factor Auth**.
2. Configure the authentication.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2nd factor Auth Method</td>
<td>Select Radius.</td>
</tr>
<tr>
<td>Maintain Username</td>
<td>Select Yes to maintain the username during authentication. The user who is attempting to authenticate must have the same username credentials for RSA and Domain Challenge. If you select No, the username field is not locked and the user can enter a different name.</td>
</tr>
<tr>
<td>External Connections Only</td>
<td>Select NO to configure 2 Factor Authentication for internal users from within the system. Use Access Point to configure external users.</td>
</tr>
<tr>
<td>Provider Name</td>
<td>(Required) Name that distinguishes the type of RADIUS authentication being used.</td>
</tr>
<tr>
<td>Host Name / IP Address</td>
<td>(Required) DNS name or IP address of the authentication server.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>(Required) Secret for communicating with the server. The value must be identical to the server configured value.</td>
</tr>
<tr>
<td>Authentication Port</td>
<td>UDP port configured to send or receive authentication traffic. Default is 1812.</td>
</tr>
<tr>
<td>Accounting Port</td>
<td>UDP port configured to send or receive accounting traffic. Default is 1813.</td>
</tr>
<tr>
<td>Mechanism</td>
<td>Select the RADIUS authentication protocol: PAP, CHAP, MS-CHAPv1, or MS-CHAPv2.</td>
</tr>
<tr>
<td>Server Timeout</td>
<td>Number of seconds to wait for a response from the RADIUS server. Default is five seconds.</td>
</tr>
<tr>
<td>Max number of retries</td>
<td>Maximum number of times to retry failed requests. Default is three tries.</td>
</tr>
<tr>
<td>Realm Prefix</td>
<td>Name and delimiter of realm to be prepended to the username during authentication.</td>
</tr>
<tr>
<td>Realm Suffix</td>
<td>Name and delimiter of realm to be appended to the username during authentication.</td>
</tr>
<tr>
<td>Auxiliary Server</td>
<td>Default is NO. If set to YES, specify a secondary RADIUS server to be used when the primary server is not responding.</td>
</tr>
</tbody>
</table>

3. Click **Save**
4. Enter your username and passcode in the Test Authentication dialog box, then click **Test**.

If authentication is successful, users attempting to authenticate with the tenant portals will see a dialog box asking them to log in with their RADIUS credentials, followed by their domain credentials.
If the Test Authentication credentials fail, the settings are not saved. Correct the username or passcode and try again.

## Set Up Authentication with RSA SecurID

You can use RSA SecurID to enable 2 Factor Authentication for end users.

### Procedure

1. Select **Settings > 2 Factor Auth.**
2. Configure the authentication.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2nd factor Auth Method</td>
<td>Select <strong>RSA SecurID</strong></td>
</tr>
<tr>
<td>Maintain Username</td>
<td>Select <strong>Yes</strong> to maintain the Username during authentication. The user attempting to authenticate must have the same username credentials for RSA and Domain Challenge. If you select <strong>No</strong>, the username is not locked and the user can enter a different name.</td>
</tr>
<tr>
<td>External Connections Only</td>
<td>If YES, users inside the network do not need to enter RSA credentials. The distinction between internal and external is configured by the service provider. If NO, all users, both inside and outside of the network, must enter RSA credentials.</td>
</tr>
<tr>
<td>Upload Configuration File</td>
<td>Click <strong>Select</strong> and navigate to the file named <code>sdconf.rec</code>. Click <strong>Open</strong>.</td>
</tr>
</tbody>
</table>

3. Click **Save**.

### Identity Management Page

On the Identity Management page, you can add, edit, and configure those identity management providers you want to use with your Horizon Cloud environment.

The Identity Management page displays the currently configured providers, including the following information for each:

- **Status** - Current status of the listed configuration. Hover on the icon to see the current status.
- **Identity Manager URL** - URL of the provider.
- **Timeout SSO Token** - Timeout value in minutes.
- **Workspace ONE Redirection** - Indicates whether automatic redirection to Workspace ONE is configured for the listed configuration. You can only enable redirection for one identity provider per tenant. This feature is primarily used with the feature to force end-user access to their desktops and applications through VMware Identity Manager. See **Configure the Option to Force End-User Access to Use VMware Identity Manager**.
- **Data Center** - Name of your data center.
- **Tenant Address** - Address of the tenant appliance.
Create an Identity Management Provider Configuration

To configure a new entry on this page:

1. Click **New**.

2. Enter information as described below.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Identity Manager URL</td>
<td>The SAML identity provider (IdP) metadata URL from your VMware Identity Manager environment. You usually can obtain the environment's SAML IdP metadata URL using the VMware Identity Manager administration console and navigating to <strong>Catalog</strong> &gt; <strong>Settings</strong> &gt; <strong>SAML Metadata</strong>. When you click the Identity Provider (IdP) metadata link on that page, your browser's address bar displays the URL, typically in the form <code>https://&lt;VMwareIdentityManagerFQDN&gt;/SAAS/API/1.0/GET/metadata/idp.xml</code>, where <code>&lt;VMwareIdentityManagerFQDN&gt;</code> is the fully qualified domain name (FQDN) of your VMware Identity Manager environment. For more details, see the VMware Identity Manager product documentation.</td>
</tr>
<tr>
<td>Timeout SSO Token</td>
<td>Timeout value in minutes.</td>
</tr>
<tr>
<td>Data Center</td>
<td>Name of your data center. Select from the drop-down list.</td>
</tr>
<tr>
<td>Tenant Address</td>
<td>FQDN of the tenant appliance, such as <code>https://&lt;HorizonDaaSTenantApplianceFQDN&gt;/admin/SAML/metadata</code>, where <code>&lt;HorizonDaaSTenantApplianceFQDN&gt;</code> is the FQDN of your data center's tenant floating host appliance. This value must correspond to the settings that you configured in the corresponding federation artifact in the VMware Identity Manager environment.</td>
</tr>
<tr>
<td>Workspace ONE Redirection</td>
<td>When you also have the configuration to force end-user access to go through VMware Identity Manager, you can set this toggle to <strong>YES</strong> to have the end users' clients automatically redirect to their Workspace ONE environment. Read about the options to force end-user access to go through VMware Identity Manager in Configure the Option to Force End-User Access to Use VMware Identity Manager. With the automatic redirection configured to <strong>YES</strong>, in the end-user clients, when the client attempts to connect to Horizon Cloud and is forcing access through VMware Identity Manager, the client is automatically redirected to the Workspace ONE environment that is configured in VMware Identity Manager. When the toggle is set to <strong>NO</strong>, automatic redirection is not enabled, and the clients display an informational message to the user instead.</td>
</tr>
</tbody>
</table>

**Note** You can have Workspace ONE redirection enabled for only one of the identity management URLs per tenant address. If you try to enable this feature for multiple VMware Identity Manager URLs and the same tenant, an error message is displayed.

3. Click **Save**.

Edit Settings for a Configuration

To edit the information for a configuration on this page:

1. Select the listed configuration.

2. Click **Edit**.
3 Edit the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout SSO Token</td>
<td>Timeout value in minutes.</td>
</tr>
<tr>
<td>Tenant Address</td>
<td>Address of the tenant appliance. Enter here the FQDN of the tenant appliance, such as <a href="https://HorizonDaaSTenantApplianceFQDN/admin/SAML/metadata">https://HorizonDaaSTenantApplianceFQDN/admin/SAML/metadata</a>, where HorizonDaaSTenantApplianceFQDN is the FQDN of your data center's tenant floating host appliance. This value must correspond to the settings that you configured in the corresponding federation artifact in the VMware Identity Manager environment.</td>
</tr>
<tr>
<td>Workspace ONE Redirection</td>
<td>When editing the configuration, you can change the current setting of this toggle. When you also have the configuration to force end-user access to go through VMware Identity Manager, you can set this toggle to YES to have the end users' clients automatically redirect to their Workspace ONE environment. Read about the options to force end-user access to go through VMware Identity Manager in Configure the Option to Force End-User Access to Use VMware Identity Manager. With the automatic redirection configured to YES, in the end-user clients, when the client attempts to connect to Horizon Cloud and is forcing access through VMware Identity Manager, the client is automatically redirected to the Workspace ONE environment that is configured in VMware Identity Manager. When the toggle is set to NO, automatic redirection is not enabled, and the clients display an informational message to the user instead. Note You can have Workspace ONE redirection enabled for only one of the identity management URLs per tenant address. If you try to enable this feature for multiple VMware Identity Manager URLs and the same tenant, an error message is displayed.</td>
</tr>
</tbody>
</table>

4 Click **Save**.

**Configure the Option to Force End-User Access to Use VMware Identity Manager**

For each listed provider, you can use the following steps to configure whether end users can access their assigned desktops and remote applications directly from Horizon Cloud or must access only using the Workspace ONE portal that is configured in their VMware Identity Manager environment.

*Note* When you change these settings, it can take up to 15 minutes for the update to take effect.

1 Click **Configure**.

2 Edit settings as described below.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force Remote Users to Identity Manager</td>
<td>Select YES to block remote user access except through the identity management provider. Option only displays if that provider status is green.</td>
</tr>
<tr>
<td>Force Internal Users to Identity Manager</td>
<td>Select YES to block internal user access except through the identity management provider. Option only displays if that provider status is green.</td>
</tr>
</tbody>
</table>

3 Click **Save**.
When you force end-user access through VMware Identity Manager, you typically also edit the corresponding identity provider configuration to specify that the end-user clients automatically redirect to the Workspace ONE environment. See Edit Settings for a Configuration.

The feature to force end-user access to VMware Identity Manager works with the Workspace ONE redirection feature in the following ways.

<table>
<thead>
<tr>
<th>Force end-user access through VMware Identity Manager setting</th>
<th>Workspace ONE redirection setting</th>
<th>What happens when the end user's client connects to Horizon Cloud to access their desktops and applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled (yes)</td>
<td>Enabled (yes)</td>
<td>Client is automatically redirected to their Workspace ONE environment.</td>
</tr>
<tr>
<td>Enabled (yes)</td>
<td>Disabled (no)</td>
<td>Client displays a message that tells the user that they must access Horizon Cloud using Workspace ONE. Automatic redirection does not occur.</td>
</tr>
<tr>
<td>Disabled (no)</td>
<td>Enabled (yes)</td>
<td>Client displays the Horizon Cloud login screen for the end user to log in. Automatic redirection does not occur because forced access to VMware Identity Manager is not enabled.</td>
</tr>
<tr>
<td>Disabled (no)</td>
<td>Disabled (no)</td>
<td>Client displays the Horizon Cloud login screen for the end user to log in. In this scenario, both forced access and the automatic redirection features are disabled.</td>
</tr>
</tbody>
</table>

Remove a Configuration

To remove one of the configurations:

1. Select the configuration in the list.
2. Click Remove.
3. Click Delete to confirm.
Desktop Connections

This section provides information on setting up and maintaining connections to desktop virtual machines.

This chapter includes the following topics:

- Desktop Protocols
- Using the VMware Horizon Client

Desktop Protocols

There are a variety of connection protocols for establishing connections to desktop virtual machines.

The VMware Horizon Agent has a very small footprint (90Kb) and supports the full Horizon Client capabilities: Blast Extreme, Blast with HTML Access, PCoIP, RDP, HTTPS, SSL, SSO, USB Redirection, printer support, and session management.

The Horizon Agent supports two desktop connection styles: Native Application (Blast Extreme and PCOIP protocols) and HTML Access (Blast with HTML Access protocol).

Blast Extreme

Blast Extreme is a high performance display protocol. The protocol contains both WAN optimization and support for 3D graphics, resulting in a far superior end user experience when compared to RDP.

To use the Blast Extreme protocol:

- Each virtual desktop must have the latest versions of the Horizon Agent and DaaS Agent installed.
- End users must have the VMware Horizon Client installed on their end point device.
- Blast Extreme is the default protocol for Native Clients in the pool settings.

Blast with HTML Access

Blast with HTML Access enables access to a desktop via any HTML5 compliant web browser.

To use Blast with HTML Access:

- Each virtual desktop must have the latest versions of the Horizon Agent and DaaS Agent installed.
- For internal access not via Access Point, SSL certificate install automation must be configured. See Automating SSL Certificate Install for VMware Blast.
There are additional requirements for launching remote applications, as described below.

**System Requirements for Using HTML Access (Blast)**

**Browser on client system:**
- Chrome 41, 42, and 43
- Internet Explorer 10 and 11
- Safari 7 and 8 (Mobile Safari is not supported for this release.)
- Firefox 36, 37, and 38

**Client operating systems:**
- Windows 7 SP1 (32- or 64-bit)
- Windows 8.x Desktop (32- or 64-bit)
- Windows 10 desktop (32- or 64-bit)
- Mac OS X Mavericks (10.9)
- Mac OS X Yosemite (10.10)
- Chrome OS 28.x or later

**HTML Access (Blast) Support for RDSH Applications**

Launching RDSH applications is supported in HTML Access.

Note the following:
- Access Point 2.0 remote access gateway must be deployed (confirm with your Service Provider).
- This functionality does not work for iOS or Android.

**Automating SSL Certificate Install for VMware Blast**

The process described in this appendix is needed to facilitate internal access that is not via Access Point. If you do not have users requiring this type of access, you do not need to perform this procedure.

Note the following:
- You must follow this process on the image before converting the VM to an image or republishing.
- You must repeat this process each time you open and republish an image.

You can install the certificate using post sysprep script execution in order to avoid sysprep issues and duplicate certificate problems. You can also use your own standard practice as well (for example, Active Directory GPO and scripts). See the Horizon View feature pack documentation for SSL certificate requirements.

Follow the steps below to configure post sysprep commands/scripts in the Horizon DaaS environment.
- Import certificate on test machine and note certificate thumbprint.
- Create post sysprep script/batch file on template VM and copy certificate.
Convert template VM to image or republish.

**Import Certificate and Record Certificate Thumbprint**

The first step in automating SSL certificate install is importing the certificate and recording the thumbprint.

**Procedure**

1. Add the certificate snap-in to MMC by performing the steps below.

   In order to add certificates to the Windows certificate store, you must first add the certificate snap-in to the Microsoft Management Console (MMC). Before you begin, verify that the MMC and certificate snap-in are available on the Windows guest operating system.

   a. On the desktop, click **Start** and type `mmc.exe`
   
   b. In the MMC window, select **File > Add/Remove Snap-in**.
   
   c. In the Add or Remove Snap-ins window, select **Certificates** and click **Add**.
   
   d. In the Certificates snap-in window, select Computer account, click **Next**, select local computer, and click **Finish**.
   
   e. In the Add or Remove snap-in window, click **OK**.

2. Import a certificate for the HTML Access Agent into the Windows Certificate Store by performing the steps below.

   To replace a default HTML Access Agent certificate with a CA-signed certificate, you must import the CA-signed certificate into the Windows local computer certificate store. Before you begin, verify that the HTML Access Agent is installed, the CA-signed certificate was copied to the desktop, and the certificate snap-in was added to MMC (see Step 1 above).

   a. In the MMC window, expand the Certificates (Local Computer) node and select the Personal folder.
   
   b. In the Actions pane, select **More Actions > All Tasks > Import**.
   
   c. In the Certificate Import wizard, click **Next** and browse to the location where the certificate is stored.
   
   d. Select the certificate file and click **Open**.

   To display your certificate file type, you can select its file format from the File name drop-down menu.

   e. Type the password for the private key that is included in the certificate file.
   
   f. Select **Mark this key as exportable**.
   
   g. Select **Include all extendable properties**.
1. Click **Next** and click **Finish**.

The new certificate appears in the **Certificates (Local Computer) > Personal > Certificates** folder.

2. Verify that the new certificate contains a private key.

   1. In the **Certificates (Local Computer) > Personal > Certificates** folder, double-click the new certificate.

   2. In the **General** tab of the Certificate Information dialog box, verify that the following statement appears: 'You have a private key that corresponds to this certificate'.

3. Import root and intermediate certificates for the HTML Access Agent.

   If the root certificate and intermediate certificates in the certificate chain are not imported with the SSL certificate that you imported for the HTML Access Agent, you must import these certificates into the Windows local computer certificate store.

   a. In the MMC console, expand the **Certificates (Local Computer)** node and go to the **Trusted Root Certification Authorities > Certificates** folder.

      i. If your root certificate is in this folder, and there are no intermediate certificates in your certificate chain, skip this procedure.

      ii. If your root certificate is not in this folder, proceed to step b.

   b. Right-click the **Trusted Root Certification Authorities > Certificates** folder and click **All Tasks > Import**.

   c. In the Certificate Import wizard, click **Next** and browse to the location where the root CA certificate is stored.

   d. Select the root CA certificate file and click **Open**.

   e. Click **Next**, click **Next**, and click **Finish**.

   f. If your server certificate was signed by an intermediate CA, import all intermediate certificates in the certificate chain into the Windows local computer certificate store.

      1. Go to the **Certificates (Local Computer) > Intermediate Certification Authorities > Certificates** folder.

      2. Repeat steps c through f for each intermediate certificate that must be imported.

4. In the certificate MMC window, navigate to the **Certificates (Local Computer) > Personal > Certificates** folder.

5. Double-click the CA-signed certificate that you imported into the Windows certificate store.

6. In the Certificates dialog box, click the **Details** tab, scroll down, and select the Thumbprint icon.

7. Copy the selected thumbprint to a text file.

   For example:
Create Post Sysprep Script/Batch File and Copy Certificate

The second step in automating SSL certificate install is creating the post sysprep script/batch file and copying the certificate.

Use post build configuration script "SetupComplete.cmd "to import the SSL certificate and configure the VMware HTML Access registry (applies to Windows 7 and later).


For example:

- Copy the SSL certificate file under C: drive. For this example, the "C:\desktone_ca_cert" file.
- Create a file SetupComplete.cmd under "%WINDIR%\Setup\Scripts\" folder. Create "Scripts" folder if it does not exist.
- Add following commands in SetupComplete.cmd file. The thumbprint value is what you copied above.
- Note that if you have root certificate and intermediate certificates in the certificate chain, then you need to add appropriate CertUtil commands in batch file.

```
CertUtil  -importPFX -f  -p "<password>" "C:\desktone_ca_cert.pfx"
reg add "HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config" /f /v "SslHash" /t REG_SZ /d "31 2a 32 50 1a 0b 34 b1 65 46 13 a8 0a 5e f7 43 6e a9 2c 3e"
del /F /Q "C:\desktone_ca_cert.pfx"
del /F /Q "%systemroot%\setup\scripts\SetupComplete.cmd"
```

- Save the SetupComplete.cmd file. You can test the SetupComplete.cmd file on test machine.

Convert Template VM to Image or Republish

The third step in automating SSL certificate install is converting the template VM to an image or republishing

Procedure

1. Convert the template VM to an image or republish, and create an assignment.
2. Verify the HTML Access connection for the certificate, or check certificates and HTML Access registry on desktops.

Note  If the HTML Access (Blast) service generates the self-signed certificate even after you set the valid CA certificate as described above, then you can troubleshoot this issue by looking at the logs located here: %ProgramData%\VMWare\Vmware Blast\Blast-worker.txt
PCoIP

PCoIP is a legacy high performance display protocol.

The PCoIP protocol contains both WAN optimization and support for 3D graphics, resulting in a far superior end user experience when compared to RDP.

To use the PCoIP protocol:

- Each virtual desktop must have the latest versions of the Horizon Agent and DaaS Agent installed.
- End users must have the VMware Horizon Client installed on their endpoint device.

Using the VMware Horizon Client

This section describes some of the Horizon Client features you should understand and any environment characteristics unique to the DaaS integration. For complete information on using the Horizon Client, refer to the Horizon Client documentation on VMware.com.

Accessing Desktops and Applications

Note the following when launching desktops and remote applications.

- If you log into the Horizon Client and have an active application session, you may be prompted to reconnect depending on the Horizon Client settings. The Horizon Client will only prompt to reconnect to an application session once. It will not prompt again until you logout and log back in. If the session fails to connect, users should attempt to launch applications normally.
- You cannot have an active RDS desktop and active remote application session at the same time.
- Idle timeouts are based on the activity on the endpoint device, not on the desktop or application.
- RDP is not a compatible protocol if you are logged in via PCoIP on another device. You must log out of the PCoIP session before attempting to connect via RDP.
- The Horizon Client displays RDS desktops and remote applications as launchable items. If you do not see an option to connect to your RDS pool as a desktop, confirm that the RDSH service is enabled for full desktop access and that you have Horizon Client 3.0 or higher.
- The remote application name displayed is the name assigned in the pool, so it is important to make the names meaningful in order to distinguish between the applications when multiple pools are mapped to them.
- The Reset Application function will log you off of all application sessions regardless of the session host you are using.
- USB re-direction is not supported for RDS-based servers.
- Launching RDSH applications is supported in HTML Access. See Blast with HTML Access.
Accessing Local Files with Remote Applications Using File Redirection

The file redirection feature allows users to open local files in entitled remote applications that support a given file type.

The feature is enabled in the Horizon Client when the Open local files in hosted applications option is selected.

This functionality allows users to do the following:

- Open a local file in a remote application by double-clicking the file in the client machine or by right-clicking, selecting Open with, and choosing the remote application in the menu.
- In the remote application, browse the complete folder where the file resides.
- Save changes made using the remote application to the local client disk.
- Register an entitled application as a file handler for the file types that those applications can open, or chose to open with the remote application a single time.

When an application is set as the default handler:

- The file's preview icon matches the entitled application's icon in the application launcher page.
- The file type description is overridden by the remote application, if any.
- Double-clicking a file of that type launches the Horizon Client.

Session Timeout

The session begins when the user authenticates. This timeout can be changed in the administration console.

- User Activity Heartbeat interval

  This value controls the interval between Horizon Client heartbeats. These heartbeats report to the Tenant the amount of idle time that has passed. Idle time occurs when there is no interaction with the end point device, as opposed to idle time in the desktop session. In large desktop deployments, it may reduce network traffic and increase performance to have the activity heartbeats at longer intervals.

- User Idle timeout

  This value controls the maximum time that a user can be idle while connected to the Tenant. When this time is reached, the user is disconnected from all active Horizon Client Desktop sessions. Additionally, when the user returns, they will be required to re-authenticate in order to access the Horizon Client.

  **Note** The User Idle timeout should always be greater than the User Activity Heartbeat interval, and is recommended to be at least double the User Activity Heartbeat Interval to avoid unexpected disconnects from desktops.
Broker Session timeout

This value controls the maximum time that a Horizon Client can be connected to the Tenant before its authentication expires (timeout count starts each time you authenticate). When this timeout occurs, you will not be automatically disconnected from the desktop and are able to keep working, but if you then perform an action that causes communication to the broker (for example, changing settings), the system requires you to re-authenticate and also to log back into the desktop.

**Note** The Broker Session timeout should always be greater than the User Idle timeout, and is recommended to be at least equal to the sum of the User Activity Heartbeat interval and the User Idle timeout.

**Note** Horizon Clients running on the Android OS have been known to override this policy setting, resulting in a session timeout of approximately ten minutes.

Resetting the User Password

When logging in to the Horizon Client, a user might be prompted to change their password.

- After entering the new password, the Horizon Client displays a message indicating that the password reset was successful. However, the password is not actually updated until the connection to the Horizon Agent has occurred. So if the session times out before the connection occurs or the user never launches a desktop session, the password will not be updated.

- If the new password does not conform to AD rules, the log in will be unsuccessful. The user then needs to exit the Horizon Client and attempt to reset the password again. Note that the following character combinations cannot be used in Horizon Client passwords:

  `<
  `>
  `<!—
  `&

Desktop Options

After logging into a desktop, a user can click Options to open the Options menu.

The following table describes the functionality available from the Options menu.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch Desktop</td>
<td>Allows the User to access the Desktop Selection Screen or Switch between open desktop sections. See the Desktop Selection Screen Section for controls and info. This will not work if your session has timed out.</td>
</tr>
</tbody>
</table>
| Autoconnect to this Desktop | For PC and thin clients, makes the specified desktop the user's default desktop when the desktop is part of a dynamic pool. On the next login, the desktop will immediately be displayed as long as:  
  - The user has only one desktop mapped to them.  
  - There is not a problem with the login credentials or desktop state.  
  If a user selects Autoconnect and then logs in with multiple desktops, the Autoconnect to this Desktop setting is set to off/true. If the session times out, the Autoconnect setting is not saved and the user cannot autoconnect at the next log in. |
| Reset Desktop           | Triggers a reboot on the desktop. This will not work if the session has timed out.                                                            |
| Disconnect              | Disconnects the current user from their active session.                                                                                       |
| Disconnect and Logoff   | Disconnects and logs off the user from their active session.                                                                                   |

**Triggering a Desktop Logoff**

Logging off initiates a call to the DaaS Agent, which can take up to 30 seconds to complete.

As a result, if a user attempts to log back in before the 30 seconds elapses, the log off dialog might still be present.

**VRAM Settings During Assignment Provisioning**

To prevent black screen, the platform provisions assignments of these desktops with the video RAM (VRAM) size set to 128. This setting can be changed by your service provider.
Troubleshooting

This section describes the most common problems you might need to troubleshoot.

For information on other problems that might occur when using VMware software, refer to the VMware Knowledge Base.

This chapter includes the following topics:

- Troubleshooting Horizon Client Connections
- Troubleshooting HTML Access (Blast) Connections
- Black Screen
- Overriding ADM PCoIP Defaults
- Error Messages
- Emergency Direct Desktop Connection Without Tenant
- Give Feedback Menu Choice Does Not Work

Troubleshooting Horizon Client Connections

There are several configuration/setup problems that can result in an inability to use the Horizon Client successfully

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Problems</td>
<td>If you cannot log in to the Horizon Client, verify that the version of the VMware Horizon Client you are using is compatible with VMware View 5.1 or higher.</td>
</tr>
<tr>
<td>Desktop Does Not Launch</td>
<td>If the Desktop does not launch, verify that no other software in the environment is using port 443.</td>
</tr>
<tr>
<td>Unable to Connect to Desktop</td>
<td>If you receive the error message “Unable to Connect to Desktop,” it means that the View Agent is not running. In the Windows Control Panel programs, verify that Horizon Agent and View Agent Direct Connect appear in the list of installed programs. If they do not, the installation did not complete properly and you will need to reinstall. If the View Agent software is installed, verify that the View Agent Service is running.</td>
</tr>
</tbody>
</table>
Problem | Solution
---|---
Desktop Disconnects | If a Horizon Client session ends too quickly when idle, this means that Horizon Client Session Timeout settings are configured to allow only a very short idle period. You can configure the Horizon Client Session Timeout settings in the administration console.

Black Screen | See Black Screen.

### Troubleshooting HTML Access (Blast) Connections

There are several configuration/setup problems that can result in an inability to launch a HTML Access (Blast) connection successfully.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser is not HTML5 compliant</td>
<td>Check that the browser version is one cited in the requirements.</td>
</tr>
<tr>
<td>Pop-up blocker enabled</td>
<td>The browser’s pop-up blocker could prevent opening the new window for a HTML Access connection. Make sure that the user disables the pop-up blocker.</td>
</tr>
<tr>
<td>Windows firewall disabled</td>
<td>Make sure that the Windows Firewall is installed and running on the user's desktop. A disabled Windows Firewall will result in errors reported in the HTML Access logs.</td>
</tr>
</tbody>
</table>

### Black Screen

Users can see a black screen for a variety of reasons.

- When you update VMware Tools, the update can in some cases install the wrong video driver, resulting in black screen. The workaround is to log into the session using RDP and install the correct driver.

- If the System Administrator moves a desktop from a non-PCoIP pool to a PCoIP pool and users experience a black screen when trying to connect to the desktop, solutions can be found in the VMware Knowledge Base.
  
  - Refer to the steps outlined in the VMware Knowledge Base article Black screen when logging into a VMware View virtual desktop using PCoIP.
  
  - Verify that the Video RAM (VRAM) settings in the Virtual Machine settings (.vmx) file are set properly for multi-monitor access when using the PCoIP protocol. Refer to the VMware Knowledge Base article Determining display and screen resolution settings for PCoIP.
  
  - Verify that the Video driver is correct for the VMware View Agent and operating system. Refer to the VMware Knowledge Base article "The PCoIP server log reports the error: Error attaching to SVGADevTap, error 4000: EscapeFailed."

### Overriding ADM PCoIP Defaults

ADM can be configured on the Domain Controller or the master desktop image being used to create a gold pattern.
On the master desktop image, the System Administrator can override ADM defaults by running gpedit.msc on the desktop and navigating to the Administrative Template > Classic Administrative Templates (ADM) > PCoIP folder.

## Error Messages

This section describes error messages that users can encounter during desktop connections.

- **Error 500**

  If a user receives Error 500 in the Horizon Client, look in the tenant log and make a note of the exception before contacting support. The exception to look for will mention the ViewClientServlet.

- **Common Error Messages**

  The following table lists the most common error messages users can receive and the causes when using the Horizon Client to connect to their desktop. The Error Details portion of the message provides information needed by customer support to troubleshoot the connection problem.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Agent Login Failed. Error Details: &lt;Message from Agent&gt;</td>
<td>The View Agent failed the login request sent.</td>
</tr>
<tr>
<td>Session has Expired, Please Restart Horizon Client to Connect</td>
<td>Session timeout has occurred. The timeout is based on a policy (userportal.session.timeout) set at the service provider, but may be overridden by a setting in the administration console.</td>
</tr>
<tr>
<td>Unable to allocate a desktop - pool refresh is in progress.</td>
<td>Wait a few minutes and try again. Dynamic pool refresh is underway. This means that desktops are being destroyed and recreated based on a new or altered Gold Pattern. Once the refresh completes, users will be able to log into their desktop.</td>
</tr>
<tr>
<td>Error communicating with desktop. Please contact your Administrator. Error Details: Desktop Agent Communication Error</td>
<td>Unable to parse error from Authentication Error Response due to interrupted communication between the Horizon Client, Tenant and View Agent Connect. There might be a warning or error in the desktop.log file related to ViewClientServlet.</td>
</tr>
<tr>
<td>Could not parse XML</td>
<td>Data Horizon Client or Agent returned XML which could not be read by the DaaS platform.</td>
</tr>
<tr>
<td>Desktop is not ready for connection (DaaS Agent may be starting up). Please wait a few minutes or try again. If problem persists, please contact your Administrator.</td>
<td>DaaS Agent is reported as offline. Reboot the desktop if the problem persists and console access is too long. The DaaS Agent should come up when the desktop comes up (within a few minutes).</td>
</tr>
<tr>
<td>Desktop is not ready for connection (may be shutting down or rebooting). Please wait a few minutes or try again. If problem persists, please contact your Administrator.</td>
<td>OS state is not running. Wait until it is running or reboot from administration console.</td>
</tr>
<tr>
<td>Desktop is not ready for connection (currently in maintenance mode). Please wait a few minutes or try again. If problem persists, please contact your Administrator.</td>
<td>Domain rejoin maintenance is occurring for a dynamic desktop. This can also occur during dynamic pool refresh.</td>
</tr>
<tr>
<td>Error Description</td>
<td>Details</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Unable to Connect to Desktop. Please contact your Administrator. Error Details:</td>
<td>The DaaS Agent has reported that the View Agent service is not running or listening on the</td>
</tr>
<tr>
<td>View Agent is not running</td>
<td>require ports. Make sure that the View Agent is installed and that the firewall ports are</td>
</tr>
<tr>
<td></td>
<td>open (4172, 32111, 443). Reboot machine or check service &quot;View Agent Connect&quot;</td>
</tr>
<tr>
<td></td>
<td>through RDP (User Portal) if possible.</td>
</tr>
<tr>
<td>Unable to Connect to Desktop. Please contact your Administrator. Error Details:</td>
<td>VMware Tools are not running. See troubleshooting/solution on VMware tools.</td>
</tr>
<tr>
<td>VMware Tools is not running</td>
<td></td>
</tr>
<tr>
<td>Unable to Connect to Desktop. Please contact your Administrator. Error Details:</td>
<td>VMware Tools are not installed. See troubleshooting/solution on VMware tools.</td>
</tr>
<tr>
<td>VMware Tools Tools is not installed</td>
<td></td>
</tr>
<tr>
<td>Unable to Connect to Desktop. Please wait a few minutes and try again. If problem</td>
<td>Desktop Unavailable. This is a generic message from the Allocator Service. Try checking</td>
</tr>
<tr>
<td>persists, please contact your Administrator</td>
<td>the state of the machine and the tenant system to see if there are other issues.</td>
</tr>
<tr>
<td>Unable to Connect to Desktop. Desktop has been allocated to a different user.</td>
<td>Another user has been allocated this desktop. A session exists with a GUID different from</td>
</tr>
<tr>
<td>Please Contact your Administrator. Error Details: Desktop Already in Allocated</td>
<td>the current user.</td>
</tr>
<tr>
<td>State.</td>
<td></td>
</tr>
<tr>
<td>Login Failure. Please contact your Administrator. Error Details: Unable to lookup</td>
<td>An exception was raised by the Horizon DaaS software during a GUID lookup. Possible reasons</td>
</tr>
<tr>
<td>user GUID using credentials</td>
<td>include: Domain controller is offline; the Fabric node had failures; general tenant</td>
</tr>
<tr>
<td></td>
<td>problems.</td>
</tr>
<tr>
<td>Unable to Connect to Desktop. Please wait a few minutes and try again. If problem</td>
<td>IP Address is null or invalid. The IP address can be null if the DaaS Agent is in the</td>
</tr>
<tr>
<td>persists, please contact your Administrator</td>
<td>middle of logging in or the VM is starting up.</td>
</tr>
<tr>
<td>Unable to Connect to Desktop. Please contact your Administrator. Error Details:</td>
<td>The IP address is listed only if it is known.</td>
</tr>
<tr>
<td>Unknown IP Address</td>
<td></td>
</tr>
<tr>
<td>Unable to Connect to Desktop. Please contact your Administrator. Error Details:</td>
<td>There is no Domain information logged in the database. The DaaS platform cannot</td>
</tr>
<tr>
<td>Unable to retrieve Tenant Domain information</td>
<td>associate the tenant with any Domain.</td>
</tr>
<tr>
<td>Login Failure: Unknown user name or bad password. Please try again.</td>
<td></td>
</tr>
<tr>
<td>Unable to Allocate Desktop, No Desktops Available. All desktops in pool are</td>
<td>Dynamic pool has no desktops that are available to the user.</td>
</tr>
<tr>
<td>currently in use.</td>
<td></td>
</tr>
<tr>
<td>Unable to Connect to Desktop (current connected protocol incompatible). Please log</td>
<td>The Allocator Service is indicating the current session is using a non-compatible protocol.</td>
</tr>
<tr>
<td>off previous session and try again.</td>
<td></td>
</tr>
<tr>
<td>Unable to complete log off. If problem persists, please contact your Administrator.</td>
<td>This error occurs if the DaaS platform cannot parse the XML, the session-id key returned</td>
</tr>
<tr>
<td>Error Details: Invalid session id</td>
<td>in the XML is null, or if the key is malformed.</td>
</tr>
<tr>
<td>Unable to complete log off. If problem persists, please contact your Administrator.</td>
<td>There are no active sessions for the current user.</td>
</tr>
<tr>
<td>Error Details: Unable to Associate Session Id with Active Sessions</td>
<td></td>
</tr>
</tbody>
</table>
Unable to complete log off. If problem persists, please contact your Administrator. Error Details: Error communicating with Desktop Manager

This error occurs if when the DaaS platform throws an exception.

The desktop <x>,<n> is not in the list of entitled desktops

In this message, <x> is the application name you are attempting to launch and <n> is a number.
This message indicates that you may be using an incompatible Horizon Client and should reference the client's release notes to confirm it supports Remote Application functionality.

Error Messages Associated with Password Changes

The following table lists the error messages a user can receive and the causes when attempting to change their password in the Horizon Client.

<table>
<thead>
<tr>
<th>Error Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please Enter the Old Password and the New Password.</td>
</tr>
<tr>
<td>Some or all of the password fields are blank.</td>
</tr>
<tr>
<td>Provided Old Password is invalid, please try again.</td>
</tr>
<tr>
<td>If the password you logged in with is different from the &quot;Old Password&quot;.</td>
</tr>
<tr>
<td>Provided New Passwords do not match, please try again.</td>
</tr>
<tr>
<td>The user mistyped the password.</td>
</tr>
<tr>
<td>Please Enter a New Password that is different from the Old Password .</td>
</tr>
<tr>
<td>The new password the user entered is the same as their old password</td>
</tr>
<tr>
<td>Unable to Change Password. Please restart Horizon Client and try again. Error Detail &lt;message from View Agent&gt;</td>
</tr>
<tr>
<td>After the user selected desktop, completing password change screen, and clicked connect, the View Agent was unable to change the Domain password.</td>
</tr>
</tbody>
</table>

Note: A user confirmation dialog after the password change screen incorrectly indicates "You successfully changed your password and should use it in the future."

Note that the following character combinations cannot be used in Horizon Client passwords:

- `<`
- `>`
- `<!—`
- `&` &

For example, none of the following passwords are supported:

Desktone

- `< Desktone>`
- `Desktone <!— Desktone&`
Emergency Direct Desktop Connection Without Tenant

In an emergency situation where a tenant is down or unreachable but the network is still working, you can globally instruct the agent software on all of the desktops to allow temporary RDP native access so end users can connect without the broker being functional.

To enable this temporary functionality, add the registry keys described below to the desktop VMs, either directly or via GPO policy. Add the keys in one of the following locations, depending on whether the agent software is installed on a 32-bit or 64-bit Windows system:

- `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware DaaS Agent` (for 32-bit)
- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc.\VMware DaaS Agent` (for 64-bit)

<table>
<thead>
<tr>
<th>Key</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AllowDirectConnections</td>
<td>DWORD</td>
<td>0 = do not allow direct connections</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = allow direct connections.</td>
</tr>
<tr>
<td>DirectConnectionExpiryInUTC</td>
<td>REG_SZ</td>
<td>Date and time until which direct connections access is allowed if direct connections access is enabled (AllowDirectConnections = 1). Date and Time Format: YYYY-MM-DD HH:MM:SS</td>
</tr>
</tbody>
</table>

This functionality requires the following:

- The agent software is version 17.2 or later.
- RDP access by the end users is not being blocked by Horizon View GPOs or any other GPOs.
- The end users are in a group associated with a desktop assignment. When this functionality is enabled, the agent software configures the desktop assignment's specified users and groups for RDP access in the desktop's local RDP group.

**Note**  
The default Group Policy refresh interval is 90 minutes. You have to perform additional steps to force a refresh sooner than that. See the relevant Microsoft documentation for more information.

Give Feedback Menu Choice Does Not Work

When you click the Give Feedback menu choice in the Administration Console, nothing happens or a browser error message appears.

**Problem**

The Administration Console's Help menu (.randn) has a Give Feedback choice. Depending on your settings for your local system's browser or mail application, when you click it, you might see one of the following:

- Nothing happens.
- A browser error message appears.
Cause

The design for this menu choice is to run the new mail action of your local system's default mail application, using mailto:feedback.horizonair@vmware.com. This error occurs when the browser cannot perform the mailto action, such as under these conditions:

- Your browser is set up to block pop-up windows.
- Your browser's applications list is not configured with a default action for the mailto content type or the mailto content type is configured with the action Always ask.
- Your local system does not have a default local mail application configured

Solution

1. If your browser blocks pop-up windows, add the Administration Console's URL to the exception list.
2. Configure your browser's mailto content type's action with a mail application, so that the Give Feedback choice can successfully open a new email form.
3. If you do not want to change your browser settings, you can submit feedback by manually sending an email to feedback.horizonair@vmware.com.
The following are technical notes regarding various system features.

- **Enabling Post-Sysprep Commands**
  - To enable post-sysprep commands, perform these steps on a desktop before converting it to an image.
    1. Create a folder named sysprep under C:\driver.
    2. Create a batch file named postprep-extra.bat in the sysprep folder.
    3. Add required commands in batch file and save it.
    4. Convert the desktop to an image. File path: c:\sysprep\postprep-extra.bat. Sysprep launches this batch file during specialize pass execution (before agent comes and joins the domain).

- To set the post sysprep batch file in the template before converting to a gold pattern (executed before domain join), perform the following steps.
  1. Create a batch: c:\sysprep\postprep-extra.bat
  2. Create the C:\Sysprep\... folder structure (for Windows 7): C:\Sysprep\ postprep-extra.bat
  3. Save it with your commands. Sysprep executes this batch file in post execution.