

# Horizon DaaS 8.0.0 Tenant Administration

VMware Horizon DaaS

You can find the most up-to-date technical documentation on the VMware website at:

<https://docs.vmware.com/>

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2018 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

- 1 About Horizon DaaS Tenant Administration 6**
  
- 2 Monitoring 7**
  - Dashboard Page 7
  - Activity Page 8
  - Reports Page 8
  - Notifications Page 9
  
- 3 Assignments 10**
  - Types of Assignments 11
  - Capacity and Users Values for Session Desktops Assignments 12
  - Create an Applications Assignment 13
  - Create a Desktop Assignment 14
  - Edit an Assignment 17
  - Edit Assignment Mode 17
  - Update Agents for an Assignment 18
  - Delete an Assignment 20
  - Recover an Assignment 20
  - Manage Servers in an Assignment 20
  - Manage Desktops in an Assignment 21
  - View System or User Activity for an Assignment 23
  - Working with Nested Organizational Units 23
  
- 4 Applications 24**
  - Add Remote Applications 25
  - Add a Custom Application 25
  - Edit an Application 26
  - Delete an Application 27
  - Rename an Application 27
  - Hide an Application 27
  - Unhide an Application 27
  
- 5 Images 29**
  - Managing Images 29
    - Update an Instant Clone Image 31
  - Create an Image 31
  - Update Agent Software for an Image 33
  - Build Your Own Template 34

- Installing and Configuring Agents 35
- Configuring VMware Horizon Smart Policies 39
- Configure Administrator Direct Access to Desktops 40
- Optimizing the Display 41

## 6 Capacity 44

## 7 Imported VMs 45

## 8 Settings 47

- Edit General Settings 47
- Edit Active Directory 49
  - Active Directory Functions 51
  - External and Forest Trusts 52
- Edit Roles and Permissions 52
- Managing File Shares 53
  - Create a File Share 53
  - Add a File Share on the Locations Page 54
  - Edit a File Share 54
  - Remove a File Share 55
  - Import the Contents of a File Share 55
- Managing Utility VMs 55
- 2 Factor Authentication 56
  - Set Up Authentication with RADIUS 56
  - Set Up Authentication with RSA SecurID 57

## 9 Desktop Connections 59

- Desktop Protocols 59
  - Blast Extreme 59
  - Blast with HTML Access 59
  - PCoIP 64
- Troubleshooting Desktop Connections 64
  - Troubleshooting Horizon Client Connections 64
  - Troubleshooting HTML Access (Blast) Connections 65
  - Overriding ADM PCoIP Defaults 65
  - Error Messages 65

## 10 Technical Notes 69

## 11 Helpdesk Console (Beta Feature) 71

- Access the Helpdesk Console 71

- [Launch a Console for a Virtual Machine](#) 72
- [Set Up a Health Scan](#) 72
- [Get Remote Assistance](#) 74
- [View Usage Report](#) 74
- [View History](#) 75

# About Horizon DaaS Tenant Administration

1

The *Horizon DaaS Tenant Administration* guide provides information on how to create, deploy, and administer virtual desktops and applications.

## 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>.

# Monitoring

# 2

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

There are four selections available from the Monitor icon.

Dashboard	Displays details on desktop connections, connection states, and capacity allocation.
Activity	Displays activity details for Administrators and Users.
Reports	Provides mapping details for Users and Desktops.
Notifications	Displays a list of current notifications.

This chapter includes the following topics:

- [Dashboard Page](#)
- [Activity Page](#)
- [Reports Page](#)
- [Notifications Page](#)

## Dashboard Page

The Dashboard shows statistical information about connections and desktop capacity allocation.

The Dashboard page is available from the Monitor icon. You can see statistical information for these categories.

Category	Description
Connections	Number of connected sessions, by assignment type.
Connection States	Number of connected sessions, by status: Active, Idle, Disconnected.
Desktop Capacity Allocation	Desktop capacity in use, and total allocated desktops by type.

The Dashboard refreshes every five minutes with a message indicating the amount of time remaining until the next refresh. You can also refresh the page manually.

## Activity Page

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

The Activity page is available from the Monitor icon. 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.

The Activity page contains tabs for administrator and user events.

## Administrator Events

The Administrator tab displays administrator events with information for each action. Expand an event to view details and subtasks for that event.

Column	Description
Description	Details regarding the event.
Percentage Completion	Current percentage of event completed.
Status	Successful indicates an event was performed in its entirety. Failed indicates an event was either partially performed or not performed at all.
Time	Time that the event was logged.

## User Events

The User tab displays user events with information for each event.

Column	Description
Description	Details regarding the event.
Time	Time that the event was logged.

## Reports Page

Use the Reports page to view mapping data for users and desktops in the system.

Select **Monitor > Reports** to open the Reports page, where you can view details for these User Mapping and Desktop Mapping categories.

Mapping Type	Details
User Mapping	View details and sort by User name, Domain, Desktop Name, Desktop Model, and Mapping Type (User or Group).
Desktop Mapping	View details and sort by Desktop Name, Model, Assignment Name, Type, Active User, Mapped Users, and Mapped User Groups.

You can also manually refresh this page, filter your search, and export data to a Microsoft Excel worksheet.

## 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.

Column	Description
Type	Icon indicates the type of notification. <ul style="list-style-type: none"> <li>■ Blue "i" icon - information</li> <li>■ Yellow "!" icon - warning</li> <li>■ Red "x" icon - critical issue</li> </ul>
Notification	Text of the notification.
Status	Status of the notification. For example, Active or Dismissed,
Date	Date of notification.

**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

# 3

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

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

Action	Description
New	Create a new Applications or Desktops assignment.
Edit	Select an assignment to make changes, or drill down to view summary and sessions information.
Update Agent Software	Update agent(s) for dedicated desktops assignments.
Edit Assignment Mode	Allows you to take assignments off line for maintenance and bring them back online.
Delete	Delete an assignment.
Recover	Recover desktops that encountered an error during a previous image update.

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:

- Desktops - displays for dedicated and floating desktops assignments. See [Manage Desktops in an Assignment](#).
- Servers - displays for Application assignments and session desktops assignments. See [Manage Servers in an Assignment](#).
- System Activity and User Activity - display for all applications and desktops assignments. See [View System or User Activity for an Assignment](#).

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 Session Desktops 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 Session Desktops Assignments
- Create an Applications Assignment
- Create a Desktop Assignment
- Edit an Assignment
- Edit Assignment Mode
- Update Agents for an Assignment
- Delete an Assignment
- Recover an Assignment
- Manage Servers in an Assignment
- Manage Desktops in an Assignment
- View System or User Activity for an Assignment
- 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.

Type	Description
Applications	Use applications assignments to assign Windows Applications to groups. See <a href="#">Create an Applications Assignment</a> .
Desktop	<p>Use desktop assignments to assign Dedicated, Floating or RDSH virtual desktop/sessions to users and groups. See <a href="#">Create a Desktop Assignment</a>.</p> <p>Type displayed can be:</p> <ul style="list-style-type: none"> <li>■ Dedicated Desktop - Traditional Clone</li> <li>■ Dedicated Desktop - Instant Clone</li> </ul> <hr/> <p><b>Note</b> 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.</p> <hr/> <ul style="list-style-type: none"> <li>■ Floating Desktop - Traditional Clone</li> <li>■ Floating Desktop - Instant Clone</li> <li>■ Session Desktop - Traditional Clone</li> <li>■ Session Desktop - Instant Clone</li> </ul> <p>Definitions are as follows.</p> <ul style="list-style-type: none"> <li>■ 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.</li> <li>■ 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 sized based on the maximum number of concurrent users.</li> <li>■ Session Desktop - In a session desktop assignment, an RDSH-published desktop experience is shared across multiple users, that is, terminal services.</li> <li>■ 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 <a href="#">Create an Image</a>.</li> </ul> <p>Note the following:</p> <ul style="list-style-type: none"> <li>■ A desktop can have multiple users assigned to it, but it can be used by only one user at a time.</li> <li>■ Desktops in floating desktop assignments do not provide persistence. You can configure persistence as part of an application assignment.</li> <li>■ Where possible, use floating desktop assignments because they cost less than dedicated desktop assignments and do not dedicate VM resources for each user.</li> </ul>

## Capacity and Users Values for Session Desktops Assignments

The Capacity and Users values shown in the respective columns on the Assignments page are calculated as described below.

Value	Description
Capacity	Based on values you entered when creating the session desktop assignment: Capacity = Servers * Users per Server.
Users	Number of users currently mapped to the assignment.  <b>Note</b> This is different from the value you entered for Users per Server when creating a session desktops assignment. Users per Server is the maximum possible number of users that can be mapped to each server in the assignment.

## Create an Applications Assignment

You can create an applications 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, enter the following information.

Fixed Attributes (cannot be changed after assignment is created)

Option	Description
Domain	Select domain from the drop-down list.
Join Domain	Leave default setting (Yes).

Flexible Attributes (can be changed any time)

Option	Description
Assignment Name	Unique name for the assignment.
Default Protocol	Select Blast (HTML Access) or PCoIP.
Servers	Enter the number of servers.
Users per Server	Enter the number of users per server.

- 5 Click **Advanced Properties** to display the Advanced Properties fields, and enter information as described below.

Field	Description
VM Names	Name for all virtual machines, 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.
Computer OU	(Optional) 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 <a href="#">Working with Nested Organizational Units</a> .
Run Once Script	<p>(Optional) Location of scripts that should run after system preparation completes.</p> <p><b>Note</b> The script should end with a reboot step to reboot the VM. A sample reboot line as a Windows command is:</p> <pre>shutdown /r /t 0</pre> <p>The script is run after the Microsoft Windows System Preparation (Sysprep) process. When the system creates a 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 VM. On the next restart, the system logs in to the Windows operating system using the local administrator account and runs the script.</p>
Session Timeout Interval	After this time of inactivity; the user will be logged out. Any unsaved data will be lost.

- 6 Click **Next**.
- 7 On the Applications tab, select the applications to include in the assignment, and click **Next**.
- 8 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.
- 9 (Optional) Repeat the previous step to select additional users or groups.
- 10 Click **Next**.
- 11 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 Desktop Assignment

You can create desktop assignments from the Assignments page.

**Procedure**

- 1 Click the **Assign** icon.

The Assignments page displays.

- 2 Click **New**.

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

The Assign Desktops dialog displays.

- 4 Select the type of assignment to create. For information on types of desktop assignments see [Types of Assignments](#).

---

**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.

Option	Description
Pod	This option only displays if the data center is configured with multiple pods. You can only create assignments from images in the same pod..
Desktop Model	[Dedicated and floating desktop assignments only] Select model from the drop-down list.
Domain	[Traditional Clone images only] Select domain from the drop-down list.
Join Domain	[Traditional Clone images only] Leave default setting (Yes).

- 6 Enter information for the Flexible Attributes displayed.

Option	Description
Image	<p>Select an image from the list.</p> <ul style="list-style-type: none"> <li>■ 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.</li> <li>■ For dedicated desktops 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.</li> <li>■ For dedicated and floating desktops assignments, RDSH role-enabled images will not be listed, since there is no reason that users would want to create dedicated or floating desktops assignments from those images. RDSH role-enabled images appear in the drop-down list only when you are creating a session desktops assignment.</li> </ul>
Assignment Name	A unique name for the new assignment.
Default Protocol	Select Blast (HTML Access) or PCoIP.
Preferred Client Type	Select Browser or Horizon Client.
Capacity	[Dedicated and floating desktop assignments only] Number of desktops required in the assignment.

Option	Description
Servers	[Session desktop assignments only] Enter the number of servers.
Users per Server	[Session desktop assignments only] Enter the number of users per server.

7 Under Flexible Attributes, expand Advanced Properties and enter required information.

Option	Description
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.
Computer OU	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 <a href="#">Working with Nested Organizational Units</a> .
Run Once Script	<p>(Optional) Location of scripts that should run after system preparation completes.</p> <p><b>Note</b> The script should end with a reboot step to reboot the VM. A sample reboot line as a Windows command is:</p> <pre>shutdown /r /t 0</pre> <p>The script is run after the Microsoft Windows System Preparation (Sysprep) process. When the system creates a 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 <code>Windows RunOnce</code> path (<code>System run once</code>) and then restarts the VM. On the next restart, the system logs in to the Windows operating system using the local administrator account and runs the script.</p>
Session Timeout Interval	<p>The timeout value for floating and static desktop session pools. The default is seven days (10,080 minutes). The maximum value is 99,999 minutes, approximately 69 days.</p> <p><b>Note</b> 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 <b>OK</b> in the next 30 seconds. If the logoff occurs, any unsaved documents are lost.</p> <p>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.</p>

8 Click **Next**.

- 9 Select an image from the list.

In the list, the acronym for the cloning type used on the image 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.

- 10 Click **Next**.

- 11 On the Active Directory Search page, start typing the name of a user or group from your Active Directory.

- 12 Select a user or group from the list.

- 13 (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.

- 14 On the Summary page, confirm that the displayed information is correct and click **Submit**.

- 15 Click the **Assign** icon to see your new assignment.

## 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 desktops 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.

## 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 If desired, enter a custom notice in the **Maintenance Notice** text box.

If you do not enter a custom notice, users will see the default notice.

---

**Note** At this time the custom maintenance notice appears only in the legacy Desktop Portal. Users launching through the HTML Access portal or through the Horizon Client directly will always see the default notice.

---

- d 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 Agents for an Assignment

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

---

**Note** You can also update agent software for all other types of assignments by updating the image and pushing changes to the assignment. This process is described in [Update Agent Software for an Image](#).

---

In order for the agent update feature to work, you must have created an Agents file share and added it to the system. 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 agent update files. See [Managing File Shares](#).

The agent update feature allows automated update of all the agents in an assignment in a single operation.

- The system makes regular contact with the VMware CDS software distribution network and downloads agent updates automatically to a file share that you have set up on a local machine. The update files are then automatically imported into the system and made available to assignments.
- The availability of updates is indicated on the Assignments page, where you can apply them to assignments. When you initiate the upgrade task on an assignment, all VMs in the assignment are be updated as part of that task.

- Your VMware representative can adjust the interval between scans for new agents and the wait time for scans after tenant startup if you request it.

### Procedure

#### 1 Click **Assign**.

The Assignments page displays, with a blue dot appearing next to the name of any assignment that has agent updates available.

- If you hover over a blue dot, a popup displays indicating the agent updates available for that assignment.
  - The system selects the latest versions of each agent by default, but you can open each drop-down to view all available versions.
- 2 Select the check boxes for one or more assignments. By selecting multiple assignments, you can update all of them to a common set of agent versions.

#### 3 Click **Update Agent Software**.

The Agent Update dialog displays.

- 4 On the Software tab, select the agent(s) to update and click **Next**.
- 5 On the Agreements tab, select the **Agree** radio button for each agreement you wish to accept and click **Next**. The system skips the update for any item for which you do not accept the agreement.
- 6 (Optional) On the Command Line tab, add any command line options. For details regarding command line options, see the documentation for the relevant agent.

---

**Note** There are currently no command line options available for the DaaS Agent.

---

#### 7 Click **Finish**.

A message displays at the top of the page indicating that the update has started.

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**. The task description indicate the agent being updated and the assignment on which the update is being performed. If the task is not successful within 24 hours, it fails.

## 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.

### Procedure

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

## Manage Servers in an Assignment

You can manage servers in session desktops assignments and applications assignments.

### 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 **Servers** at the top of the page.  
The Servers tab displays, showing a list of servers 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** Server status must be green to perform these actions.

---

Option	Description
Shutdown	Shuts down the server(s). <ul style="list-style-type: none"> <li>■ You can select more than one server at a time.</li> <li>■ You can only shut down VMs that do not have active user sessions.</li> </ul>
Restart	Performs a 'graceful' restart of the VM(s). You can select more than one server at a time. If this does not work, it may be necessary to use the Reset option (see below).

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

Option	Description
Suspend	Suspends the selected server(s). You can select more than one server at a time.
Resume	Resumes operation of the selected server(s). You can select more than one server at a time.
Power On	Powers on the selected server(s). You can select more than one server at a time.
Power Off	Powers off the selected server(s). You can select more than one server at a time.
Reset	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).
Log Off	Logs off the selected server.
Disconnect	Disconnects the selected server.
Convert to Image	Converts the selected server to an image.  <b>Note</b> You cannot convert a VM to an image if it is currently being used as an appliance.

## Manage Desktops in an Assignment

You can manage desktops in dedicated and floating desktops assignments.

### 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). <ul style="list-style-type: none"> <li>■ You can select more than one desktop at a time.</li> <li>■ You can only shut down VMs that do not have active user sessions.</li> </ul>
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 desktops assignments 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.

Rename	[Dedicated desktops assignments only] Renames the selected desktop. VDI will indicate that a reboot is required.
Unassign	[Dedicated desktops assignments only] Unassigns the selected desktop from user.
Delete	[Dedicated desktops assignments 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 assignments only] Powers on the selected desktop(s). You can select more than one desktop at a time.
Power Off	[Traditional clone assignments only] Powers off the selected desktop(s). You can select more than one desktop at a time.
Reset	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).
Log Off	Logs the currently connected user off the selected desktop.
Disconnect	Disconnects the currently connected user from the selected desktop.
Rebuild	[Floating desktops assignments only] Deletes and recreates the selected desktop. Use this option for desktop VMs that have become corrupted or otherwise non-operational.
Convert to Image	Converts the selected desktop to an image.

## View System or User Activity for an Assignment

You can view system or user activity for desktops and applications assignments.

### 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 **System Activity** or **User Activity** at the top of the page.

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.

## 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 Desktops Assignment page.

Only the OU= part of the string is required. The DC= part is optional.

# Applications

# 4

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 RDSH image that you published after adding applications to the image.
- Custom applications are added by specifying their names and paths on the image, using functionality on the Applications page. This is not recommended, but can be used in some situations such as Thin App launches.

You can take the following actions on the Applications page.

Option	Description
New	Add a Remote or Custom Application.
Edit	Select an application to make changes.
Delete	Delete an application.
Rename	Rename an application.
Hide	Deactivate an application in the list.  <b>Note</b> This does not delete the application from the system, but only deactivates it. The application is moved from the list of visible (activated) to the list of hidden (deactivated) applications. To delete an application, use the Delete function.
Unhide	Re-enables an Application that was previously hidden (deactivated).  <b>Note</b> This button only displays when you have selected Hidden in the Show filter at the top of the Applications list. This filter switches the view between a list of visible (activated) and hidden (deactivated) applications.

This chapter includes the following topics:

- [Add Remote Applications](#)
- [Add a Custom Application](#)
- [Edit an Application](#)

- [Delete an Application](#)
- [Rename an Application](#)
- [Hide an Application](#)
- [Unhide an Application](#)

## Add Remote Applications

You can use the following procedure to add one or more remote applications from an existing RDSH image.

### Prerequisites

You must have an RDSH image with at least one application on it in order to add remote applications.

### Procedure

- 1 Click the **New** button at the top of the Applications page.  
The New Application dialog displays.
- 2 Click the **Image** button.  
The Images page appears.
- 3 Select an RDSH image with at least one application on it and click **Publish**.

### Results

The system scans the RDSH image for applications installed in it. This scan includes all applications found under the Start - All Programs menu in Windows.

## Add a Custom Application

You can use the following procedure to add a custom application and associate it with one or more RDSH images.

---

**Note** Adding custom applications is not recommended. It is recommended that you add remote applications instead. See [Add Remote Applications](#).

---

### Procedure

- 1 Click the **New** button at the top of the Applications page.  
The first New Application dialog displays.
- 2 Click the **Custom** button.  
The second New Application dialog appears

### 3 Enter information as described below.

Field	Description
Name	Unique name for the new application
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 )
RDSH Images to use with	Image(s) with which you want to use the application. Click in box and select from drop-down list. The list includes Windows Server 2008/2012 gold patterns, which are used for applications assignments.
Icon File	PNG file (32 x 32 pixels) to use as application's icon. Click <b>Choose File</b> to browse for file.
Version	(Optional) Version number of application
Publisher	(Optional) Publisher of application

### 4 Click **Save**.

## 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.

Field	Description
Name	Unique name for the application
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 )
RDSH Images to use with	Image(s) with which you want to use the application. Click in box and select from drop-down list. The list includes Windows Server 2008/2012 gold patterns, which are used for applications assignments.
Icon File	.png file (32 x 32 pixels) to use as application's icon. [optional] Click Choose File to browse for file.
Version	Version number of application [optional]
Publisher	Publisher of application [optional]

### 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 (deactivate) an application on the Applications page.

---

**Note** This does not delete the application from the system, but only deactivates it. The application is moved from the list of visible (activated) to the list of hidden (deactivated) 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 deactivated and is moved to the hidden applications list.

## Unhide an Application

You can use the following procedure to unhide (reactivate) 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 (activated) to a list of hidden (deactivated) applications.

- 2 Select the application and click **Unhide**.

The application is re-enabled and moved to the visible (activated) applications list.

# Images

# 5

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.

Image Type	Description
Instant Clone	Image type that uses VMware's NGVC technology to create VMs instantly for an assignment.
Traditional Clone	Proprietary image type that does full image cloning when creating assignments

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.

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

Button	Description
New	Begin the image creation process. See <a href="#">Create an Image</a> .
Publish	Publishes the selected image.
Take Offline	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.
Update Agent Software	Updates agent(s) for a selected image. See <a href="#">Update Agent Software for an Image</a> .

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

Option	Description
Backup Now	<p>[Traditional Clone images only] Creates a backup of the selected image.</p> <ul style="list-style-type: none"> <li>■ After you create and name the backup, it appears under Backups on the image detail page.</li> <li>■ 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.</li> </ul> <p><b>Important</b> You must power off the image VM before attempting to roll back to a saved backup. If you attempt this operation with the VM powered on, the task fails with an error.</p>
Duplicate	[Instant Clone images only] Creates a duplicate of the selected image.
Rename	Renames the selected image.
Delete	Permanently deletes the selected image.
Convert to Desktop	Converts the selected image to a desktop.
Assign Image	[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 <b>OK</b> to push the updates.
Push Updates	Pushes updates to floating desktop, session desktop, and remote applications assignments using the selected image. Select the assignment(s) from the list and click <b>OK</b> to push the updates.
Download Bootstrap	<p>Downloads an encrypted bootstrap file for you to deploy to your image(s).</p> <p>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.</p>
Refresh Password	<p>Creates a new default password to be used for bootstrapping images.</p> <p>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.</p>

## 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.

### 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.

## Create an Image

Create a new desktop image from the Images page.

---

**Note** This process takes approximately 40 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 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 5 Images](#).

Option	Description
Instant Clone	Image type that uses VMware's NGVC technology to create VMs instantly for an assignment.  <b>Note</b> 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.

- 6 Enter the required information as described below.

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

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

- 7 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.

---

- 8 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 agent software for an image and push updates to assignments.

The agent update feature allows automated update of all the agents in an image in a single operation.

- The system makes regular contact with the VMware CDS software distribution network and downloads agent updates automatically to a file share that you have set up on a local machine. The update files are then automatically imported into the system and made available for images.
- The availability of updates is indicated on the Images page, where you can apply them to images.
- Your VMware representative can adjust the interval between scans for new agents and the wait time for scans after tenant startup if you request it.

### Prerequisites

In order for the agent update feature to work, you must have created an Agents file share and added it to the system. 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 agent update files. See [Managing File Shares](#).

### Procedure

- 1 Click **Inventory > Images**.

The Images page displays, with a blue dot appearing next to the name of any assignment that has agent updates available.

- If you hover over a blue dot, a popup displays indicating the agent updates available for that image.
- The system selects the latest versions of each agent by default, but you can open each drop-down to view all available versions.

- 2 Select the check box an image. You can only update agents for one image at a time.
- 3 Click **Update Agent Software**.

The Agent Update dialog displays.

- 4 On the Software tab, select the agent(s) to update and click **Next**.

- 5 On the Agreements tab, select the **Agree** radio button for each agreement you wish to accept and click **Next**. The system skips the update for any item for which you do not accept the agreement.
- 6 (Optional) On the Command Line tab, add any command line options. For details regarding command line options, see the documentation for the relevant agent.

---

**Note** There are currently no command line options available for the DaaS Agent.

---

- 7 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**. The task description indicates the agent being updated and the assignment on which the update is being performed. If the task is not successful within 24 hours, it fails.

- 8 Push updates to assignment(s) based on the original image. For more information, see [Managing Images](#).

---

**Note** It is recommended that you push updates to one assignment to begin with and confirm that VDI and other features are working on the assignment VMs.

---

- 9 (Optional) Delete the original image and rename the clone image with the original image name.

## 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:

- Install and configure agents
- Set up direct connection to desktop VMs (optional)
- Optimize the display (optional)

## Installing and Configuring Agents

It is important that you install and configure agents on the template VM in the correct order.

Before you begin installing the agents, perform the tasks described in [Prepare the Template VM for Agent Installation](#).

### 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:

Port(s)	Source	Destination	TCP	UDP
4172 (PCoIP)	Access Point	VM	P	P
443 (View communication)	Tenant Appliance	VM	P	
32111 (PCoIP)	Access Point	VM	P	
22443 (HTML Access)	Access Point	VM	P	
443 (HTML Access)	Access Point	T/VM	P	
8443 (HTML Access)	Access Point	VM	P	
4172 (PCoIP)	Access Point	VM	P	P
80 (redirects to 443)	Access Point	T/VM	P	

#### What to do next

Install the Horizon Agent. See [Installing the Horizon Agent](#)

### Installing the Horizon Agent

After you have completed the preparation steps, you can install the Horizon Agent on the template VM.

There are three possible scenarios when installing the Horizon Agent:

- Install on desktop (Windows 7, Windows 8, Windows 8.1, Windows 10)
- Install on server (Windows Server 2008 R2, Windows Server 2012 R2) as Personal Desktop (Non-RDSH)
- Install on server (Windows Server 2008 R2, Windows Server 2012 R2) as RDSH Role

---

**Note** If you have not installed the most recent version of the Horizon Agent, this can cause problems with creating RDS pools. In this case, 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.

---

### Install the Horizon Agent on a Windows Desktop

You can install the Horizon Agent on a Windows 7, Windows 8, or Windows 8.1 desktop.

#### Procedure

- 1 Download the latest Horizon Agent from the Myvmware download site. Note that there are separate downloads for 32-bit and 64-bit operating systems.
- 2 Double-click the Horizon Agent installation file (file name is: VMware-viewagent-x86\_64-x.y.z-nnnnnnn.exe for the 64-bit installer).
- 3 Perform a custom installation with the following options:
  - Deselect VMware Horizon View Composer Agent.
  - Select VMware Horizon Instant Clone Agent.
- 4 Restart the virtual machine when prompted.

#### What to do next

- For improved security regarding the use of the Horizon Agent, deactivate 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 deactivating weak ciphers in SSL/TLS, such as in the VMware Horizon 7 documentation set.
- [Install the DaaS Agent](#)

### Install the Horizon Agent on Windows Server as Personal Desktop (Non-RDSH)

You can install the Horizon Agent on Windows Server 2008 R2 or 2012 R2 as a personal desktop.

#### Procedure

- 1 Download the latest Horizon Agent from VMware's website (<https://my.vmware.com>). Note that there are separate downloads for 32-bit and 64-bit operating systems.
- 2 Double-click the Horizon Agent installation file (file name is: VMware-viewagent-x86\_64-x.y.z-nnnnnnn.exe for the 64-bit installer).

- 3 Select the option to install the Horizon Agent in desktop mode.
- 4 Perform a custom installation with the following options:
  - ◆ Deselect VMware Horizon View Composer Agent.
- 5 Restart the virtual machine when prompted.

#### What to do next

- For improved security regarding the use of the Horizon Agent, deactivate 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 deactivating weak ciphers in SSL/TLS, such as in the VMware Horizon 7 documentation set.
- [Install the DaaS Agent](#)

#### Install the Horizon Agent on Windows Server as an RDSH Role

You can install the Horizon Agent on Windows Server 2008 R2, 2012 R2, or 2016 as an RDSH role.

---

**Note** To install the Horizon Agent in this scenario, you **MUST** run the command line install and cannot use the default “double click” GUI.

---

#### 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 Agent from VMware's website (<https://my.vmware.com>). Note that there are separate downloads for 32-bit and 64-bit operating systems.
  - 3 Run the following on the command line as an administrator user: `VMware-viewagent-x86_64-x.y.z-nnnnnnn.exe /v "VDM_SKIP_BROKER_REGISTRATION=1"`
  - 4 Restart the virtual machine when prompted.

#### What to do next

- For improved security regarding the use of the Horizon Agent, deactivate 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 deactivating weak ciphers in SSL/TLS, such as in the VMware Horizon 7 documentation set.
- [Install the DaaS Agent](#)

## Install the DaaS Agent

After installing the Horizon Agent, install the DaaS Agent.

---

**Note** If you are upgrading the DaaS Agent on an existing setup, you must confirm that the Agent Pairing setting is configured correctly. For more information, see [Edit General Settings](#).

---

### Procedure

- 1 Download the most recent DaaS Agent installer file from the Myvmware.com download site.
- 2 Run the installer on the template virtual machine.

## Configuring VMware Horizon Smart Policies

You can use 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 deactivates 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. 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](#).

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.

- 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`.

## Configure Administrator Direct Access to Desktops

Administrators can now connect to desktops using their domain accounts, instead of being required to have local admin access.

To allow this, a new DaaS Direct Connect Users group will be created during the DaaS Agent installation. This group does not have local administration rights, but is allowed to connect to the desktop through the Helpdesk Console or using a direct RDP connection.

There are two methods for adding a user to the DaaS Direct Connect Users group:

- Update the image.
- using a GPO policy on the tenant appliance.

---

**Note** This procedure is separate from the template VM configuration process and can be performed at any time.

---

To add members by updating the image:

- 1 Join the image VM to the domain and then restart it.

- 2 Add domain user(s) to the DaaS Direct Connect Users group.
- 3 Publish the image and provision desktops. All desktops created using the image will now have the group member details.

To add members using a GPO policy on the tenant appliance:

- 1 Create a new GPO.
- 2 Right-click on the GPO and select **Edit**.
- 3 In the Group Policy Management Editor, navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Restricted Groups**.
- 4 Right-click **Restricted Groups** and select **Add Group**.
- 5 In the Add Group dialog, enter DaaS Direct Connect Users and click **OK**.
- 6 In the properties dialog, enter members in the 'Members of this group' text box, click **Add**, and then click **OK**.
- 7 Close the Group Policy Management Editor and the Group Policy Management Console.
- 8 Link the newly created GPO to the domain.

## 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](https://salesforce.com).

- 9 Click **Open**.
- 10 Close the Add/Remove Templates window.

**Results**

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 yyyyyyy 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.

Option	Description
Windows 2008 or 2012	<ol style="list-style-type: none"> <li>a Select <b>Start &gt; Administrative Tools &gt; Group Policy Management</b>.</li> <li>b Expand your domain, right-click the GPO that you created for the group policy settings, and select <b>Edit</b>.</li> </ol>
Windows 2003	<ol style="list-style-type: none"> <li>a Select <b>Start &gt; All Programs &gt; Administrative Tools &gt; Active Directory Users and Computers</b>.</li> <li>b Right-click the OU that contains your View desktops and select <b>Properties</b>.</li> <li>c On the Group Policy tab, click <b>Open</b> to open the Group Policy Management plug-in.</li> <li>d In the right pane, right-click the GPO that you created for the group policy settings and select <b>Edit</b>.</li> </ol>

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.

---

# Capacity

# 6

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.

Section	Description
Desktop Model	Shows the total standard capacity, with number of units used for each desktop model and units available.
Storage Types	Shows total storage, with amount used for different storage types and amount free. Click on the arrow icon below Storage GB to see the storage broken down by individual volumes.

# Imported VMs

# 7

Imported VMs are unmanaged VMs with supported operating systems that are imported in order 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.

Action	Description
Rename	Select a VM and click <b>Rename</b> . Enter a new name in the field and click <b>Save</b> .  <b>Note</b> 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.
Shutdown	Shuts down the VM(s). <ul style="list-style-type: none"><li>■ You can select more than one VM at a time.</li><li>■ VM status must be green.</li><li>■ You can only shut down VMs that do not have active user sessions.</li></ul>
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. <ul style="list-style-type: none"><li>■ You can select more than one VM at a time.</li><li>■ VM status must be green.</li></ul>

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

Action	Description
Suspend	Suspends the selected VM.
Resume	Resumes operation of the selected VM.
Power On	Powers on the selected VM.
Power Off	Powers off the selected VM.
Reset	Resets the selected VM.
Convert to Image	Converts the selected VM to an image.
Delete	Permanently deletes the selected VM.

Action	Description
Migrate to Utility VMs	Moves the VM to the Utility VMs page. See <a href="#">Managing Utility VMs</a> .
Migrate to Assignment	<p>Associates the VM(s) with a dedicated desktops assignment. In the Migrate VM(s) dialog, select an assignment in the Assignment Name field and click <b>Migrate</b>.</p> <ul style="list-style-type: none"><li>■ VMs can only be migrated to dedicated desktops assignments with the same Desktop Manager ID.</li><li>■ Selected VM(s) must be paired with the tenant using Agent Pairing, and the DaaS Agent must be in Active state.</li><li>■ 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.</li></ul>

# Settings



Edit a variety of settings for your system.

Select the Settings icon to access these options.

Option	Description
General Settings	View and edit settings for networks, domain, etc. See <a href="#">Edit General Settings</a> .
Active Directory	View and edit Active Directory details. See <a href="#">Edit Active Directory</a> .
Roles & Permissions	Edit Roles and Permissions. See <a href="#">Edit Roles and Permissions</a> .
Locations	Create file shares and perform actions on existing file shares. See <a href="#">Managing File Shares</a> .
Getting Started	Opens the Getting Started page. See the Getting Started guide for details.
Utility VMs	Opens the Utility VMs page. See <a href="#">Managing Utility VMs</a> .
2 Factor Auth	Configure 2 Factor authentication for end users. See <a href="#">2 Factor Authentication</a> .

This chapter includes the following topics:

- [Edit General Settings](#)
- [Edit Active Directory](#)
- [Edit Roles and Permissions](#)
- [Managing File Shares](#)
- [Managing Utility VMs](#)
- [2 Factor Authentication](#)

## 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.

---

**Note** 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).

---

Option	Description
Default Domain	Default domain that you are editing.
Session Timeout	<ul style="list-style-type: none"> <li>■ 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.</li> <li>■ 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.</li> </ul> <hr/> <p><b>Note</b> Set the Client Idle User timeout to be at least double the Client Heartbeat Interval to avoid unexpected disconnects from desktops.</p> <ul style="list-style-type: none"> <li>■ 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.</li> </ul> <hr/> <p><b>Note</b> The Client Broker Session timeout must be at least equal to the sum of the Client Heartbeat Interval and the Client Idle User timeout.</p> <ul style="list-style-type: none"> <li>■ 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.</li> <li>■ Admin Portal Timeout - How long you can be on the Administration Console before you need to log in again.</li> </ul>
User Portal Configuration	Enter the helpdesk email address, the trouble ticket system URL, and the external style sheet URL to allow for end-user portal configuration.

Option	Description
IDM	<p>Settings for VMware Identity Manager. If more than one IDM is configured, a set of fields displays for each.</p> <ul style="list-style-type: none"> <li>To add an IDM, click the <b>Add IDM</b> button and enter information for the new IDM: <ul style="list-style-type: none"> <li>IDM URL - URL of the IDM. Format is <pre>https://VMwareIdentityManagerFQDN/SAAS/API/1.0/GET/metadata/idp.xml</pre> <p>where VMwareIdentityManagerFQDN is the domain name for the IDM.</p> </li> <li>Timeout SSO Token - Timeout value in minutes.</li> <li>Data Center - Name of data center. Select from drop-down list.</li> <li>Tenant Address - Address of the tenant appliance.</li> </ul> </li> <li>For an existing IDM, you can edit the following fields: <ul style="list-style-type: none"> <li>Identity Provider (IdP) metadata URL. The format for the URL is: <pre>https://VMwareIdentityManagerFQDN/SAAS/API/1.0/GET/metadata/idp.xml</pre> <p>where VMwareIdentityManagerFQDN is the domain name for the IDM.</p> </li> <li>Timeout SSO Token - Timeout value in minutes.</li> <li>Data Center - Name of data center. Select from drop-down list.</li> <li>Tenant Address - Address of the tenant appliance.</li> <li>Force Remote Users to vIDM - Enable to block remote user access except through IDM. Option only displays if IDM status is green.</li> <li>Force Internal Users to vIDM - Enable to block internal user access except through IDM. Option only displays if IDM status is green.</li> </ul> </li> <li>To delete an IDM, click the "x" to the top right of the IDM to delete.</li> </ul>
HTML Access	Controls whether to delete credentials of the broker session when a HTML Access portal connection tab is closed.
Contact Info	Administrator and Technical Contact information.

#### 4 Click **Save**.

## Edit Active Directory

You can edit the Active Directory after initial setup.

The Active Directory is normally registered during the setup process. Follow the directions here to edit your Active Directory setup after it has been configured.

Note the following:

- In the case of 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 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.

- 4 Edit information as desired in the fields described below.

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

- 5 Click **Advanced Properties**.

- 6 Edit information as desired in the following Advanced Properties fields.

Option	Description
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.

- 7 Make changes to auxiliary bind accounts as described below.

- 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.

---

- 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.

---

- 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 active service account remaining.

---

- 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.

Option	Description
Join Username	Domain administrator. Edit only if new username is set up in Active Directory first.
Join Password	Domain administrator password. Edit only if new password is set up in Active Directory first.
Primary DNS Server IP	IP address of primary DNS Server
Secondary DNS Server IP	(Optional) IP of secondary DNS Server
Default OU	Default organizational unit

- 11 Click **Save**.
- 12 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.

## Active Directory Functions

This topic provides details regarding the system's Active Directory.

- Distribution groups not supported

When you are defining groups of users or administrators, always select 'Security' for the Active Directory group type, as Distribution groups are not supported.

## 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

You can edit roles that were previously configured.

### Procedure

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

The Roles & Permissions page displays.

There are two default roles, shown below.

Role	Description
Super-Administrator	Users with this role have access to all functionality and can save changes.
Demo-Administrator	Users with this role have access to all functionality but cannot save any changes.

- 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**.

## 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 Locations 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.

#### Procedure

- 1 Create a Windows folder following the usual procedure.

You must name the folder 'agentFiles'. Later the system will create several subfolders, only two of which you use. These subfolders are described below.

Subfolder Name	Description
cdsClient	This folder will contain agent files downloaded automatically from the upgrade server that your VMware representative has configured for you.
hotpatch	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.

- 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 Locations Page](#).

## Add a File Share on the Locations Page

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

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

#### Prerequisites

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

#### Procedure

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

Option	Description
<b>Name</b>	Name of the file share.
<b>Domain</b>	Domain of the file share. Select from the drop-down list.
<b>Username</b>	Admin user for the file share.
<b>Password</b>	Admin password for the file share.
<b>Type</b>	Select Agents.
<b>Source Path</b>	Network path to file share.

- 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 > Locations**.
- 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 Locations page.

### Procedure

- 1 On the Locations 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 Locations page.

### Procedure

- 1 Select **Settings > Locations**.
- 2 On the Locations 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 Assignments page of the user interface (see [Update Agents for an Assignment](#)).
  - 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.

Action	Description
Rename	Select a VM and click <b>Rename</b> . Enter a new name in the field and click <b>Save</b> .  <b>Note</b> 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.
Shutdown	Shuts down the VM(s). <ul style="list-style-type: none"> <li>■ You can select more than one VM at a time.</li> <li>■ VM status must be green.</li> <li>■ You can only shut down VMs that do not have active user sessions.</li> </ul>
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. <ul style="list-style-type: none"> <li>■ You can select more than one VM at a time.</li> <li>■ VM status must be green.</li> </ul>

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

Action	Description
Suspend	Suspends the selected VM.
Resume	Resumes operation of the selected VM.
Power On	Powers on the selected VM.
Power Off	Powers off the selected VM.
Reset	Resets the selected VM.
Migrate To Imported VMs	Moves the VM to the Imported VMs page. See <a href="#">Chapter 7 Imported VMs</a> .

## 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 the appropriate topic below.

### 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.

Option	Description
<b>2nd factor Auth Method</b>	Select <b>Radius</b> .
<b>Maintain Username</b>	Select <b>Yes</b> 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 <b>No</b> , the username field is not locked and the user can enter a different name.
<b>External Connections Only</b>	Select <b>NO</b> to configure 2 Factor Authentication for internal users from within the system. Use Access Point to configure external users.
<b>Provider Name</b>	(Required) Name that distinguishes the type of RADIUS authentication being used.
<b>Host Name / IP Address</b>	(Required) DNS name or IP address of the authentication server.

Option	Description
Shared Secret	(Required) Secret for communicating with the server. The value must be identical to the server configured value.
Authentication Port	UDP port configured to send or receive authentication traffic. Default is 1812.
Accounting Port	UDP port configured to send or receive accounting traffic. Default is 1813.
Mechanism	Select the RADIUS authentication protocol: PAP or CHAP.
Server Timeout	Number of seconds to wait for a response from the RADIUS server. Default is five seconds.
Max number of retries	Maximum number of times to retry failed requests. Default is three tries.
Realm Prefix	Name and delimiter of realm to be prepended to the username during authentication.
Realm Suffix	Name and delimiter of realm to be appended to the username during authentication.
Auxiliary Server	Default is <b>NO</b> . If set to <b>YES</b> , specify a secondary RADIUS server to be used when the primary server is not responding.

### 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.

### 5 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.

Option	Description
2nd factor Auth Method	Select <b>RSA SecurID</b>
Maintain Username	Select <b>Yes</b> 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 <b>No</b> , the username is not locked and the user can enter a different name.

Option	Description
<b>External Connections Only</b>	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.
<b>Upload Configuration File</b>	Click <b>Select</b> and navigate to the file named <code>sdconf.rec</code> . Click <b>Open</b> .

3 Click **Save**.

# Desktop Connections

# 9

This section provides information on setting up and maintaining connections to desktop virtual machines.

For information on using the Horizon Client, see the [VMware Horizon Client Documentation](#) site.

This chapter includes the following topics:

- [Desktop Protocols](#)
- [Troubleshooting Desktop Connections](#)

## 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 or higher
- Internet Explorer 10 or higher
- Safari 7 or higher (Mobile Safari is not supported for this release.)
- Firefox 36 or higher

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**.

- h Click **Next** and click **Finish**.

The new certificate appears in the Certificates (Local Computer) > Personal > Certificates folder.

- i 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.

- If your root certificate is in this folder, and there are no intermediate certificates in your certificate chain, skip this procedure.
  - 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:

```
31 2a 32 50 1a 0b 34 b1 65 46 13 a8 0a 5e f7 43 6e a9 2c 3e
```

---

**Note** When you copy the thumbprint, do not to include the leading space. If you inadvertently paste the leading space with the thumbprint into the registry key (in Step 7), the certificate might not be configured successfully. This problem can occur even though the leading space is not displayed in the registry value text box.

---

### 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).

<http://technet.microsoft.com/en-us/library/dd744268%28v=ws.10%29.aspx>

For example:

- Copy the SSL certificate file under C: drive. For this example, the "C:\desktopone\_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:\desktopone_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:\desktopone_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 end point device.

**Troubleshooting Desktop Connections**

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.

**Troubleshooting Horizon Client Connections**

There are several configuration/setup problems that can result in an inability to use the Horizon Client successfully

Problem	Solution
Login Problems	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.
Desktop Does Not Launch	If the Desktop does not launch, verify that no other software in the environment is using port 443.
Unable to Connect to Desktop	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.

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 <a href="#">#unique_78</a> .

## 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.

Problem	Solution
Browser is not HTML5 compliant	Check that the browser version is one cited in the requirements.
Pop-up blocker enabled	The browser's pop-up blocker could prevent opening the new window for a HTML Access connection. Make sure that the user deactivates the pop-up blocker for the Desktop Portal.
Windows firewall deactivated	Make sure that the Windows Firewall is installed and running on the user's desktop. A deactivated Windows Firewall will result in errors reported in the HTML Access logs.

## 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 sections 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 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.

View Agent Login Failed. Error Details: <Message from Agent>	The View Agent failed the login request sent.
Session has Expired, Please Restart Horizon Client to Connect	Desktop Portal session timeout has occurred. The Desktop Portal 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.
Unable to allocate a desktop - pool refresh is in progress.	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.
Error communicating with desktop. Please contact your Administrator. Error Details: Desktop Agent Communication Error	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.
Could not parse XML	Data Horizon Client or Agent returned XML which could not be read by the DaaS platform.
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.	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).
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.	OS state is not running. Wait until it is running or reboot from Desktop Portal or administration console.
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.	Domain rejoin maintenance is occurring for a dynamic desktop. This can also occur during dynamic pool refresh.
Unable to Connect to Desktop. Please contact your Administrator. Error Details: View Agent is not running	The DaaS Agent has reported that the View Agent service is not running or listening on the require ports. Make sure that the View Agent is installed and that the firewall ports are open (4172, 32111, 443). Reboot machine or check service "View Agent Connect" through RDP (User Portal) if possible.
Unable to Connect to Desktop. Please contact your Administrator. Error Details: VMware Tools is not running	VMware Tools are offline. See troubleshooting/solution on VMware tools.

Unable to Connect to Desktop. Please contact your Administrator. Error Details: VMware Tools is not installed	VMware Tools are not installed. See troubleshooting/solution on VMware tools.
Unable to Connect to Desktop. Please wait a few minutes and try again. If problem persists, please contact your Administrator	Desktop Unavailable. This is a generic message from the Allocator Service. Try checking the state of the machine and the tenant system to see if there are other issues.
Unable to Connect to Desktop. Desktop has been allocated to a different user. Please Contact your Administrator. Error Details: Desktop Already in Allocated State.	Another user has been allocated this desktop. A session exists with a GUID different from the current user.
Login Failure. Please contact your Administrator. Error Details: Unable to lookup user GUID using credentials	An exception was raised by the Horizon DaaS software during a GUID lookup. Possible reasons include: Domain controller is offline; the Fabric node had failures; general tenant problems.
Unable to Connect to Desktop. Please wait a few minutes and try again. If problem persists, please contact your Administrator. Error Details: Unknown IP Address	IP Address is null or invalid. The IP address can be null if the DaaS Agent is in the middle of logging in or the VM is starting up.
Unable to Connect to Desktop. Please contact your Administrator. Error Details: Invalid IP Address <IP_address>	The IP address is listed only if it is known.
Unable to Connect to Desktop. Please contact your Administrator. Error Details: Unable to retrieve Tenant Domain information	There is no Domain information logged in the database. The DaaS platform cannot associate the tenant with any Domain.
Login Failure: Unknown user name or bad password. Please try again.	User name or password are invalid for the given domain.
Unable to Allocate Desktop, No Desktops Available. All desktops in pool are currently in use.	Dynamic pool has no desktops that are available to the user.
Unable to Connect to Desktop (current connected protocol incompatible). Please log off previous session and try again.	The Allocator Service is indicating the current session is using a non-compatible protocol.
Unable to complete log off. If problem persists, please contact your Administrator. Error Details: Invalid session id	This error occurs if the DaaS platform cannot parse the XML, the session-id key returned in the XML is null, or if the key is malformed.
Unable to complete log off. If problem persists, please contact your Administrator. Error Details: Unable to Associate Session Id with Active Sessions	There are no active sessions for the current user.

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.

Please Enter the Old Password and the New Password.	Some or all of the password fields are blank.
Provided Old Password is invalid, please try again.	If the password you logged in with is different from the "Old Password".
Provided New Passwords do not match, please try again.	The user mistyped the password.
Please Enter a New Password that is different from the Old Password .	The new password the user entered is the same as their old password
Unable to Change Password. Please restart Horizon Client and try again. Error Detail <message from View Agent>	After the user selected desktop, completing password change screen, and clicked connect, the View Agent was unable to change the Domain password.  <b>Note</b> 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:

<

>

<!—

&amp;

- For example, none of the following passwords are supported:

Desktone

< Desktone>

Desktone <!—

Desktone&amp;

The following are technical notes regarding various system features.

- Custom Branding

If you have a custom branding scheme for the Desktop Portal, you will need to check whether everything appears as expected after upgrading a tenant. There are a few areas to which you should pay particular attention due to VMware branding changes.

- Login page:

CSS selector: `#productNameInner`

You may need to adjust the `margin-left` property and/or decrease the font-size, for example :

`font-size: 14px;`

- Other pages:

You will likely need to make the same changes as for the login page. Additionally, you may need to adjust the `background-position` of the `#banner` selector:

`background-position: 0px 0px;`

- 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.

# Helpdesk Console (Beta Feature)

# 11

The Helpdesk Console is a user interface that you can use to access VMs, perform health scans, get remote assistance, and perform other tasks.

## Notice Regarding Beta Features and Support

HELPDESK CONSOLE IS PROVIDED "AS IS", WITHOUT SLA OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

If you encounter questions or issues using Helpdesk Console, you can send them to [deployment@vmware.com](mailto:deployment@vmware.com). VMware is not committed to productization of any features or resolution of any issues of the Helpdesk Console.

---

**Note** Not all of the tabs described in this section are displayed by default. Your service provider is able to enable additional tabs if you request it.

---

This chapter includes the following topics:

- [Access the Helpdesk Console](#)
- [Launch a Console for a Virtual Machine](#)
- [Set Up a Health Scan](#)
- [Get Remote Assistance](#)
- [View Usage Report](#)
- [View History](#)

## Access the Helpdesk Console

You can access the Helpdesk Console from your web browser.

Note the following:

- Use HTTPS, not HTTP. Using HTTP will not launch the console.

- Chrome is the only supported browser for Console access. The following browsers are not yet supported: Microsoft Internet Explorer, Firefox, Safari, and Opera.
- If console access is failing to launch, you may need to open the following URL and accept the certificate: `https://<tenant_appliance_tenant_network_ip>:18001/`
- In a vCloud Director based environment, you need to make sure your browser accepts the vCloud Director server certificate.
- Access to the Helpdesk Console is restricted to:
  - Tenant Administrators (Users with Admin access to the Administration Console)
  - Members of the Horizon\_Air\_Helpdesk AD group. This group can be used to provide access to support personnel that are not tenant administrators.

#### Procedure

- 1 In a Chrome web browser, navigate to `https://<TenantApplianceNodeAddress>/haca` where `<TenantApplianceNodeAddress>` is the IP address of the tenant.

The login page displays.

- 2 Enter your admin username and password, confirm that the correct domain is selected, and click **Login**.

The Virtual Machines tab displays, containing a list of all VMs in all pools.

## Launch a Console for a Virtual Machine

You can launch a console for a virtual machine in the Helpdesk Console.

To launch a console for a virtual machine in the Helpdesk Console, click the VM name in the Virtual Machines list.

A console opens showing the login screen for the VM. Ctrl-Alt-Del and power operations are supported by buttons in the top right of the console window.

## Set Up a Health Scan

The Health Scan tool allows you to monitor application of VM changes that may compromise the port access, performance, or overall access by end users to the desktop.

---

**Note** This tab is not displayed by default. Your service provider can enable it if you request it.

---

#### Procedure

- 1 Install the Horizon DaaS Health Agent on all VMs that will be monitored. Click the **Install Horizon DaaS Health Agent** link at the top right of the VM Health Scan tab for more information.

---

**Note** By default, the Health Agent listens on TCP port 10762.

---

- 2 Filter the list as desired using the Scan Filter field and/or Select Pool drop-down list.
- 3 Initiate the scan by doing one of the following:
  - Click **One Time Scan** to perform a single scan immediately.
  - Enter a number of minutes and click **Schedule Scan** to schedule recurring scans at a selected time interval.

Information for the scanned VMs appears in columns as described below.

Column	Description
VM	Name of the virtual machine.
Pool	Pool (assignment) to which the VM belongs.
IP	IP address of the VM.
Result	Overall result of the scan. Result can be: <ul style="list-style-type: none"> <li>■ Power off – VM is powered off.</li> <li>■ Agent failure – Health Agent is not installed or reachable on the VM</li> <li>■ VM issue(s) - Indicated by an "X" icon with number next to it. VM has one/more issues, which are detailed in other columns.</li> </ul>
Ports	Verifies that necessary ports are open.
Firewall	Indicates whether the VM's firewall is enabled.
Sleep Policy	Indicates whether there is a policy set on the VM to put it in a sleep state.
Services	Verifies that the following services are running: <ul style="list-style-type: none"> <li>■ Desktop Windows Manager Session Manager</li> <li>■ VMware HTML Access (Blast)</li> <li>■ VMware Horizon Agent</li> <li>■ VMware DaaS Agent</li> <li>■ VMware Tools</li> </ul>
RDP Enabled	Verifies that RDP is enabled and set to allow connections from computers running any version of RDP.
BAD IP	Verifies that the desktop does not have a 169.x.x.x IP address, and so is more likely to get DHCP.
DHCP	Verifies that the desktop is set for DHCP, not STATIC.
Domain Trust Relationship	Confirms domain trust relationship between desktop and Domain Controller.
Remote Assistance	Verifies Remote Assistance is enabled on the desktop.

- 4 When the scan is complete, you can perform the following actions:
  - Mouse over the errors in the scan results table to see additional information.

- Click the **Report** button on the top left of the list (button is labelled **Report: <day date time>**) to view history of recent scans performed. In this table, double-clicking anywhere in a row opens the results for that scan.
- Select the **Show Only VMs** with Error check box to hide VMs that have no errors.
- Type a name or partial name in the Search field and press **Enter** to search for VMs by name.
- Select a value in the Show drop-down menu to adjust number of VMs shown per page.
- Click **Export** and select one of the following options:
  - **Copy** – Copy information to clipboard.
  - **CSV** – Export results in CSV format.
  - **PDF** – Export results in PDF format.
  - **Print** – Generate a printable web version of the results.

## Get Remote Assistance

The Remote Assistance tool provides a way for a helpdesk operator or administrator to shadow an active user session.

---

**Note** This tab is not displayed by default. Your service provider can enable it if you request it.

---

For more information on using this feature, click the **Guide for Remote Assistance** link on the Remote Assistance tab.

## View Usage Report

The Usage Report tab displays usage trends and allows you to view user activity session reports.

The Usage Report can be filtered by date, pool, and data type. Data displayed in the Usage Report include:

- Usage Trends – Max Concurrent Users, Max Concurrent Sessions, Daily Unique Users, Total Capacity
- User information – Client Access Demographics, Internal vs. External Users Access
- Session information – Protocol, Service Type, Session Duration

Pool-based usage information such as max concurrent users and unique users accessing a specific pool can be helpful for determining overall utilization and licensing requirements of your applications on RDSH pools.

- Select **User Activity** from the Usage Report drop-down menu to view the User Activity Summary.
- Click on a user name in the User Activity Summary list to view User Activity Details.

## View History

The History tab provides the access log for auditing purposes.

You can search or filter data by pool (assignment) using the controls at the top of the page.