

# Horizon® Air™ 16.6 Release Notes

This document describes changes to Horizon Air for version 16.6

August 2016

**vmware**

## Revision History

Date	Version	Description
08/29/2016	1.0	Initial release
09/12/2016	1.1	1 <sup>st</sup> revision

© 2016 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

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

## Prerequisites

Prerequisites for upgrading to Horizon Air 16.6 are as follows:

- All appliances and domain controllers must be synchronized to an accurate time source using the NTP protocol. Ideally a common NTP time source should be used.
- All appliances must be able to perform forward and reverse DNS lookups for each domain controller's fully qualified hostname that is contactable from the appliance public network.

If you have any questions about these prerequisites, contact your VMware representative.

## New Features

This release of Horizon® Air™ provides the following new functionality.

### Horizon Air Administration Console Replacing Enterprise Center

The Horizon Air administration console has now replaced the Enterprise Center as the Horizon Air tenant administration user interface. The console provides a streamlined experience and makes your DaaS system faster and easier to use for image management, desktop and application setup, user entitlement, and system status monitoring.

The console is divided into four parts:

- Monitor – View user and system activities.
- Assignments – Configure pools of RDSH applications, dedicated and floating VDI desktops, and RDSH session desktops. Assignments are a bundling of desktop model, pool type, image or applications, and user entitlements.
- Inventory – View desktop model allocation and available capacity, manage images (previously known as gold patterns), and view RDSH application catalog.
- Settings – Update account information such as domain registration, active directory, two-factor authentications, and general settings.

**Note the following differences in functionality:**

- There is no imported desktop pool in the Horizon Air Administration Console, so the option to create gold patterns (now called *images*) from imported desktops is no longer available.
- In a vCloud environment, backing up an image (i.e. gold pattern) in the Horizon Air Administration Console overwrites any previous backup you performed for that image.

### Custom Applications in Horizon Air

Customers who wish to use remote applications invoked via an executable path on an RDSH Server VM can now define and associate these remote application settings with an RDSH image in the Application catalog. This Custom Application definition can be used for invoking centrally managed virtualized applications such as Thinapps, as well as registering remote applications that have been installed on RDSH VMs after pool provisioning. There are now two application types:

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

To facilitate Custom applications, the following items have been added to the Applications page in the Horizon Air Administration Console (**Inventory ► Applications**), shown below.

- Three new buttons in the upper left of the page: New, Edit, and Delete.

**Note: The Edit and Delete functions are only for Custom applications.**

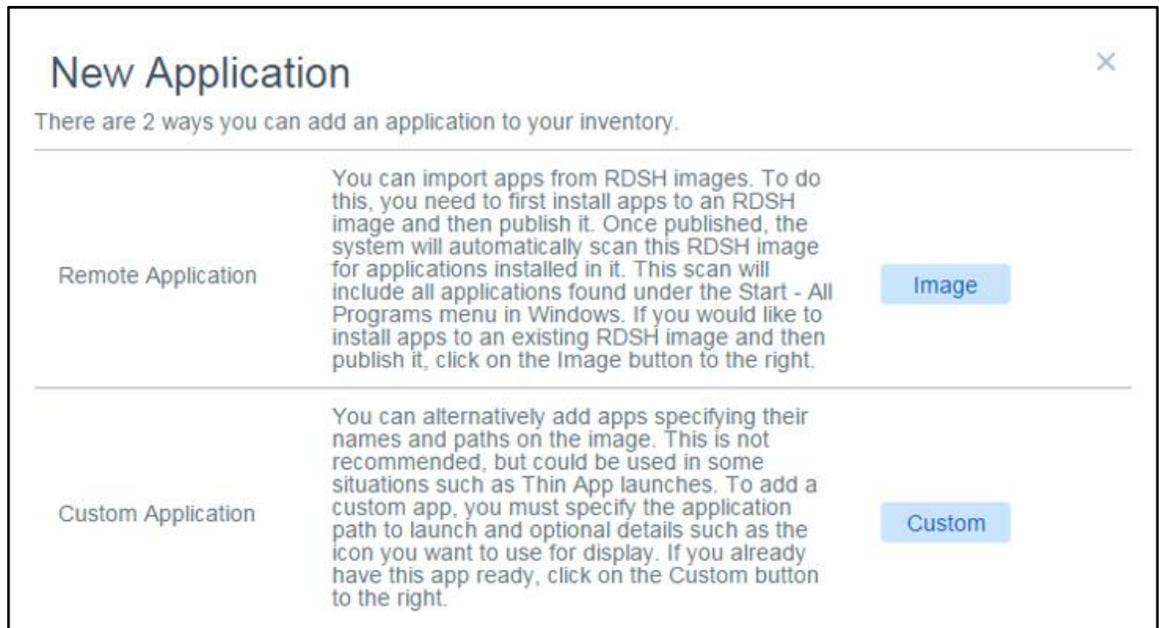
- The Type column in the application list, which identifies the type of each application (Remote or Custom) and allows you to sort by application type.



### Add a New Custom Application

1. Click the **New** button at the top of the Applications page.

The first New Application dialog appears.



2. Click **Custom**.

**Note: The other option is click Image to open the Images page, where you can install applications on an existing RDSH image and then publish it.**

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, \\fileservers.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: <div data-bbox="745 1291 1313 1507" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> </div> <p>The list includes Windows Server 2008/2012 gold patterns, which are used for applications assignments.</p>
Icon File	.png file (32 x 32 pixels) to use as application's icon. <b>[optional]</b> Click <b>Choose File</b> to browse for file: <div data-bbox="750 1682 1180 1745" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> </div>
Version	Version number of application <b>[optional]</b>
Publisher	Publisher of application <b>[optional]</b>

4. Click **Save**.

## Edit an Existing Custom Application

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.

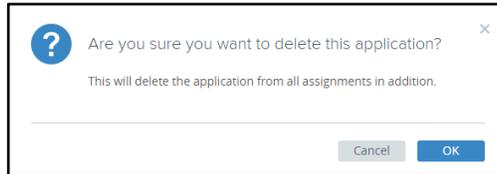
Field	Description
Name	Unique name for the new application
Application Path	Location of the application executable on the VM (for example, Z:\Customapps\app.exe) or UNC-specified path (for example, \\fileserver.accounting.com\vol1\software\app.exe)
RDSH Images to use with	Image(s) with which you want to use the application. Click in box and select from drop-down list: <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> </div> <p>The list includes Windows Server 2008/2012 gold patterns, which are used for applications assignments.</p>
Icon File	.png file (32 x 32 pixels) to use as application's icon. <b>[optional]</b> Click <b>Choose File</b> to browse for file: <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> </div>
Version	Version number of application <b>[optional]</b>
Publisher	Publisher of application <b>[optional]</b>

3. Click **Save**.

## Delete a Custom Application

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.

## View Agent Direct Connect No Longer Needed

Beginning in this release, Horizon Air no longer requires use of the View Agent Direct Connect (VADC) component.

## Updated Search Procedure in Horizon Air Administration Console

When performing AD searches in the old Enterprise Center tenant administration interface, you were required to enter the beginning of the DN. For example, searching "CN=Admin" would find the Built-in Administrators group. In the Horizon Air Administration Console, you must search by entering the name only. In this example, entering "Admin" instead of "CN=Admin".

## Note Regarding the Horizon Air User Documentation

The Horizon Air 16.6 Documentation Center, which is launched when user click the help icon in the user interface, is located here: <https://pubs.vmware.com/horizon-air-166/index.jsp> (link is not active until after GA release).

If users will be using Horizon Air behind a firewall, you must make sure that they are able to access the URL above in order to view the documentation.

## Product Support Notices

### Access Point 2.7.2 Required

Access Point 2.7.2 is now required. For more information on this version of Access Point, see [VMware Access Point Documentation](#).

### DaaS Agent 16.6 Required

Once the tenant appliances are upgraded, the DaaS Agent 16.6 is required in order to make use of all Horizon Air 16.6 functionality.

### DaaS Agent 16.6 Upgrade Recommendations

To take full advantage of Horizon Air's Agent Pairing feature, it is recommended that you follow the guidelines below.

- For floating desktop assignments, upgrade the agent on the image, bootstrap it, and then re-publish the image. You can then Push Updates for the image so that all desktops have updated agents that are bootstrapped.

- For dedicated desktop assignments, set the registry setting "pairWithLegacyCredentials" (under HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc.\VMware DaaS Agent) to 1 for all dedicated desktop VMs on which you are upgrading the DaaS agent. Then proceed with the agent upgrade as usual.

You can use the Agent Pairing setting to control the agents that communicate with DaaS desktop manager. For more information, see Edit General Settings in the [Horizon Air Administration](#) documentation.

## Horizon 7 Agent Required

- It is required that you install VMware Horizon 7 Agent on all virtual machines.
- When installing the Horizon Agent, you must now de-select the option to install the View Composer component.
- There is a performance limitation with Horizon 7.0.1 Agent. There is an observed 20% reduction in Blast consolidation. The expectation is that this issue will be fixed in Horizon 7.0.2.

For more information, see Install Horizon Agent in the HTML Access (Blast) Setup section of the *Horizon Air 16.6 Service Provider Manual*, and also the Horizon Agent [standard](#) and [silent](#) installation procedures online.

## View Agent Direct Connect No Longer Required

As mentioned above, Horizon Air no longer requires use of the View Agent Direct Connect (VADC) component.

## Firmware Requirement for Tera2 Client

Firmware 5.1.1 or higher is required to connect to Horizon Air using a Tera2 client.

## Fixed Defects

The following defects have been fixed in this version:

- When a user that is not part of a registered user group was added to an assignment in the Horizon Air administration console, the following limitations applied:
  - Such users could not make an RDP connection unless they had been explicitly added to the Remote Desktop Users group on the target desktop(s).
  - Mappings screen searches in Enterprise Center did not find users who were not part of any registered groups, whether or not they were assigned to any assignments or desktops.

This has been remedied so that these limitations no longer apply.

- The following issues had occurred in the process of adding users to assignments:
  - After a user was removed from a pool, the user sometimes still had a desktop assigned and be able to log into the pool. The assigned desktop had to be removed manually by the administrator.
  - After a desktop was unassigned from the user, the user sometimes still was shown in the assignment in the user interface. However, the user was not able to log into the assignment anymore. The administrator had to either manually assign the user a new desktop or remove the user from the assignment.
  - The following associations could not be found using the search function:
    - When a user was manually assigned to a desktop, the relationship between the user and the assignment could not be discovered in a search.
    - If a user was added to an assignment then logged into the assignment, the relationship between the user and the assignment could not be found in a search.

This has been remedied so that these issues no longer occur.

- Authentication failed if a user's password included any of the following special characters: < > ( )  
This has now been remedied so that these passwords will work as expected.

## Known Issues and Workarounds

The following are known issues in this release.

- Adding an application with ampersand (&) in the shortcut name to an assignment makes all applications in that assignment unusable. The workaround for this is to replace the "&" with "and".
- When an individual user (i.e. not in a group) is added to an assignment, the user does not have access to the assignment as expected. The workaround is to add the user to a group and then add the group to the assignment. Alternatively, you can configure a GPO policy to add a user in RDP local group.
- Login fails when username contains non-ASCII character on Desktop Portal login page when using Microsoft Edge browser.
- Users have been unsuccessful connecting to Horizon DaaS using a Tera2 client. To resolve this issue, upgrade to Firmware 5.1.1 or higher.
- If the Tenant database password includes an ampersand (&) character, installation will fail even though Tenant creation was successful.
- If you have users that are entitled to multiple pools and app stacks, it is recommended that you as the administrator consistently set whether a user writable volume is enabled for a particular user and/or group.
- On the Applications page, the Hide button is only enabled when the application selected in the list is a remote application (only one application can be selected at a time). On the **Application > Hidden** app page, the **Hide** button is also used to unhide remote application which are hidden.
- On the Locations page, a file share may still show a status of Green (connected) even after the file share has been unmounted.
- During image creation, if you restore the VM to a snapshot which was taken prior to bootstrapping of agent, then the agent may not be able communicate if it has been already boot-strapped before restoration of the VM's snapshot. To avoid this issue, do not restore a VM to a snapshot taken prior to the bootstrapping process, in case the agent has been already boot-strapped.
- When you export a .csv file on the Desktop Mapping page, the content of the exported file may not match the language of the user interface.
- When you export a .csv file on the Activities page, the exported file shows the user's protocol incorrectly as RDP instead of Blast.
- Desktop VMs in a dedicated desktop assignment continue to launch even if the Agent Pairing mode is updated from 16.6 Upgrade Mode to 16.6 Mode. To avoid this issue, before setting agent pairing to 16.6 Mode, request that your Service Provider set element allocator.staticVM.agentState.check to true, request all dedicated desktop assignment users to log off, and then update agent pairing mode to 16.6.
- When you create a new assignment and set Blast as the default protocol, this is not reflected in the Horizon Client when you connect to the tenant.
- For an App Assignment that has user groups assigned, only the number of groups (as opposed to the total number of users in the groups) appears in the Users column on the Assignment page.
- 1716010 – In larger environments, the ARP cache overflows during certain operations (e.g. mass/sequential logoffs initiated from the admin console). This causes unexpected network interruptions. The workaround is to raise the garbage collection thresholds by editing the /etc/sysctl.conf file. This can be done at any time after the tenant/DM appliance has been successfully created, as reported by the Service Center (although if you do this after pools have been created, end users will be affected by the reboot).
  - a. Create a working copy of the file.

```
cp /etc/sysctl.conf /tmp/sysctl.conf
```

- b. Edit the file as superuser with an available text editor, for example:

```
vi /tmp/sysctl.conf
```

- c. Add the following lines to the file.

```
net.ipv4.neigh.default.gc_thresh1 = 4096  
net.ipv4.neigh.default.gc_thresh2 = 4096  
net.ipv4.neigh.default.gc_thresh3 = 4096
```

- d. Verify that your edit was successful, as in the example below.

```
diff /etc/sysctl.conf /tmp/sysctl.conf  
66a67,69  
> net.ipv4.neigh.default.gc_thresh1 = 4096  
> net.ipv4.neigh.default.gc_thresh2 = 4096  
> net.ipv4.neigh.default.gc_thresh3 = 4096
```

- e. Copy the edited version back in place of the original.

```
cp /tmp/sysctl.conf /etc/sysctl.conf
```

- f. Reboot the appliance.