



Horizon DaaS Platform 6.1.5 Release Notes

VMware Horizon DaaS Platform | 11 SEP 2015

Check for additions and updates to these release notes.

What's in the Release Notes

The release notes cover the following topics:

- Patch Information
 - Patch Dependencies
 - Affected Horizon DaaS Versions
 - Patch Version
- WARNING: Restore process for HA tenants
- New Features
- Resolved Issues
- Other Updates Included in Patch
- Product Support Notices
- Known Issues
- Installing the Patch
 - Upload the Patch File
 - Install the Patch on All Service Provider Appliances
 - Install the Patch on All Tenant Appliances
- Uninstalling the Patch

Patch Information

Patch Dependencies

Horizon DaaS Platform 6.1.4 (Build 23625)

Affected Horizon DaaS Versions

Horizon DaaS Platform 6.1.0 (Build 22210)

Horizon DaaS Platform 6.1.1 (Build 22355)

Horizon DaaS Platform 6.1.2 (Build 22583)

Horizon DaaS Platform 6.1.3 (Build 22807)

Horizon DaaS Platform 6.1.4 (Build 23625)

Patch Version

WARNING: Restore process for HA tenants

When you restore both appliances in an HA appliance pair, the database is not retained. To avoid data loss, you must restore each appliance separately.

New Features

HTML Access (Blast) Support for RDSH Applications

Launching RDSH applications is supported in HTML Access 3.4.

To enable this functionality:

1. In the Enterprise Center, select **configuration ► general**.
2. Select the check box under HTML Access for RDSH Remote Applications and click **Save**.
3. Click **OK** in the informational dialog box to confirm the action.

Note the following:

- Horizon View Agent 6.1.1 and the View Agent Direct-Connection (VADC) Plug-In 6.1.1 must be installed on the desktops.
Note: When you enable HTML Access for RDSH applications in Enterprise Center as described below, users will no longer be able to reliably connect to VMs running older versions of the View Agent via Blast.
- Access Point 2.0 remote access gateway must be deployed.
- This functionality does not work for iOS or Android.
- There is currently a known issue with this feature. See item DT-8595 under Known Issues below for more information.

Microsoft Windows 10 Support

Microsoft Windows 10 desktops are now supported.

System requirements for Windows 10:

- Horizon View 6.2 is recommended for use with Horizon DaaS 6.1.5. Note the known issue regarding sysprep failure below.
- Horizon View 6.1.1 is supported experimentally. Note the known issues and limitations below.
- The vSphere versions that initially support Windows 10 are vSphere 5.5 U3 and vSphere 6.0 or later.
Note: You can also use Windows 10 in vSphere 5.1 and vSphere 5.5 U1 by creating a desktop Windows 8 image and installing the Windows 10 operating system.

Known issues and limitations for Windows 10:

- Persona Management functionality is not supported with Horizon View 6.1.1.

- Known issue regarding sysprep failure (see DT-9064 below).

vSphere Support

The Horizon DaaS 6.1.5 patch includes support for the following versions of vSphere.

- ESXi 6.0 U1 (build 3029758)
- vCenter Server 6.0 U1 (build 3040890)
- ESXi 6.0 (build 2494585)
- vCenter Server 6.0b (build 2793784)
- ESXi 5.5 U3 (build 3029944)
- vCenter Server 5.5 U3 (build 3000347)

Access Point 2.0.2 Support

Horizon DaaS Platform 6.1.5 supports Access Point 2.0.2.

For more information about setting up Access Point, see the following documents: *Horizon DaaS Platform 6.1 Access Point 2.0 Setup* (available for download with Horizon DaaS 6.1.5 files) and *Deploying and Configuring Access Point* (available online).

Resolved Issues

This patch includes fixes for the following issues:

- DT-6592 – Attempt to register a tenant returned a 404 error if the tenant name had a parentheses or hyphen in it. This has been remedied so that the error no longer occurs.
- DT-6721 – Users who did not have SuperAdmin user status were unable to assign networks to a Desktop Manager in the Service Grid, even though the role assigned to them had the necessary permission. This issue has been fixed so that users with the appropriate permission are able to perform this task.
- DT-8503 – There were cases where log messages for a particular failure or other event was not in the desktop log files even with DEBUG enabled. This has been fixed so that corresponding log message now appear in the logs.
- DT-8504 – If the Desktop Portal login page is left idle for some time, the initial login attempt was returning a 404 error. This issue has been remedied so that the error no longer occurs.
- DT-8567 – When connecting via Access Point to a desktop using HTML Access (Blast), the URL returned contained the IP instead of the FQDN. This caused certificate validation to fail and in some browsers prevented the user from connecting. This issue has been remedied so that the URL is returned as expected.
- DT-8635 – The DaaS Agent was crashing if the configured remote application file path contained the network share path. There is a new version of the DaaS Agent that remedies this problem (see DaaS Agent 6.1.5 Requirement below).
- DT-8695 – SSL certification in Access Point was not functioning on iOS and Android devices. This has been corrected so that SSL certification now works as expected.
- DT-8709 – Dynamic Desktops powered off by end users using the Shutdown function had not reinitializing properly, and so were not available for future users. This has been remedied so that these desktops reinitialize as expected.

- DT-8728 – Users had been able to bypass the RSA two-factor login page in Enterprise Center. This issue has been fixed so it is no longer possible to bypass two-factor login.
- DT-8936 – When attempting to delete a tenant, users were receiving the message ‘An unexpected error occurred’. This issue has been remedied so that the error no longer occurs.
- DT-9040 – When log level was set to debug, the first attempt to access desktop via PCoIP or HTML Access (Blast) was resulting in an error. This has been remedied so that the error no longer occurs.
- DT-9256 – When connecting via Horizon Client for iOS or Horizon Client for Android, users had been able to connect to desktops to which they were not entitled. This has been fixed so that unauthorized desktops no longer appear as available in the Horizon Client.

Other Updates Included in Patch

- The Oracle (Sun) JDK package is updated to 1.6.0_95. The update addresses multiple security issues that exist in the earlier releases of Oracle (Sun) JDK. Oracle has documented the CVE identifiers that are addressed in JDK 1.6.0_95 in the Oracle Java SE Critical Patch Update Advisory for April 2015.

Product Support Notices

- DaaS Agent 6.1.5 Requirement
The new DaaS Agent 6.1.5 is required in order to avoid the issue described in DT-8635 above.

Known Issues

- DT-8275 – In German language implementations, the DaaS Agent does not recognize the Remote Desktop Users group. In the German version of Windows this group is called "Remotedesktopbenutzer", so the agent does not correctly add the domain groups to the local groups.
- DT-8937 – Tenant name does not display properly when it contains one or more letters with a German umlaut (such as ä, ö, ü).
- DT-8467 – Timeout occurs after 10 hours, even if broker timeout is set higher than 600 minutes. The workaround for this issue is described in <http://kb.vmware.com/kb/2131762>.
- DT-8593 – When users log off from the HTML Access (Blast) client, they are also logged out of the Desktop Portal.
- DT-8595 – Attempts to launch applications via HTML Access (Blast) fail with an error when the older version of the HTML Access client is still selected. To prevent this error, verify that the HTML Access for RDSH Remote Applications option is enabled and that the prerequisites have been met as described above under HTML Access (Blast) Support for RDSH Applications.
- DT-9064 – Convert to Gold Pattern process may fail with timeout error for Windows operating systems. See VMware KB article for more information: <http://kb.vmware.com/kb/2126179>.
- 1688411 - When a user is connected to an RDS-published application over PCoIP, the session times out at the value configured for Idle Session Timeout, even though the

application is still in use. Workaround: Upgrading to Horizon DaaS 7.0.0 will resolve this issue. In the case of a staggered environment, you do not need to upgrade, but can resolve the issue by uninstalling View Agent Direct Connect (VADC).

Installing the Patch

Note: Confirm that all appliances have patch 6.1.4 installed before performing the 6.1.5 patch installation.

Pushing out software patches to all appliances in one or more Data Centers is a multi-step process:

- Upload the patch. When you upload the patch file, it is automatically replicated to all appliances.
- Install the patch file on all Service Provider appliances.
- Install the patch file on all Tenant appliances.

These steps are described below.

Upload the Patch File

Note: The upload will fail if the Pre-Patch Cleanup Script has not been run first.

1. In the Service Center, select **appliances ► software updates**. The Software Updates screen displays.
2. Click **Browse** to browse for the patch file.
3. Click **Upload**.

The Service Center checks whether the file is the correct file type. The patch file is automatically replicated to all Service Provider appliances in each Data Center. The Replications column in the lower portion of the screen indicates the progress. For example, 2/2 means that the patch file has been replicated to both the primary and secondary Service Provider appliances in a single Data Center and 4/4 means that the patch file has been replicated to the primary and secondary Service Provider appliances in two Data Centers. It can take up to one minute for each appliance. You must wait until the patch file has been replicated to an appliance before installing the patch on that appliance.

Note: If you receive an error message indicating that the file is invalid, clear the /tmp folder on your SP1 appliance and try the upload again.

Install the Patch on All Service Provider Appliances

Note: If you start the installation before the patch file has been replicated to all Service Provider appliances, you are warned that replication is not complete on specific appliances. However, you can begin installation on those appliances where replication is complete.

1. In the Service Center, select **appliances ► software updates**. The Software Updates screen lists the available patches. Each patch name is a link.
2. Click on the name of a patch. The Software Updates screen redisplay to show those organizations that have appliances that have not been patched.
3. Mark the checkbox for organization 1000.
4. To install the patch in a single Data Center, select a Data Center from the drop-down. To install the patch on all appliances in all Data Centers, accept the default value "All".
5. Click **Install**.

Install the Patch on All Tenant Appliances

1. In the Service Center, select **appliances ► software updates**. The Software Updates screen lists the available patches. Each patch name is a link.
2. Click on the name of a patch. The Software Updates screen redisplay to show those organizations that have appliances that have not been patched.
3. For each Tenant:
 - a. Mark the checkbox for the organizations you need to patch.
 - b. The Data Center drop-down default value is All, which installs the patch on all appliances in all Data Centers. To install in a single Data Center, select that Data Center from the drop-down.
4. Click **Install**.

Uninstalling the Patch

To revert to the previous version, uninstall the patch by executing these commands on all appliances as the root user:

```
sudo apt-get remove dt-platform-6-1-0-patch-5  
sudo service dtService restart
```

Copyright © 2021 VMware, Inc. All rights reserved.