



Release Notes for VMware Horizon 7 version 7.5.2

Released 7 March 2019

These release notes include the following topics:

- [What's New in This Release](#)
- [Before You Begin](#)
- [Internationalization](#)
- [Compatibility Notes](#)
- [Supported Windows 10 Operating Systems](#)
- [Support for Red Hat Enterprise Linux Workstation](#)
- [Prior Releases of Horizon 7](#)
- [Known Issues](#)
- [Resolved Issues](#)

What's New in This Release

VMware Horizon 7 version 7.5.2 is a maintenance release that contains new user authentication security improvements that resolve CVE-2019-5513 which is documented in [VMSA-2019-0003](#). For information about the issues that are resolved in this release, see [Resolved Issues](#).

Before You Begin

- **Important note about installing VMware View Composer**
If you plan to install or upgrade to View Composer 7.2 or later, you must upgrade the Microsoft .NET framework to version 4.6.1. Otherwise, the installation will fail.
- **Important note about installing VMware Tools**
If you plan to install a version of VMware Tools downloaded from VMware Product Downloads, rather than the default version provided with vSphere, make sure that the VMware Tools version is supported. To determine which VMware Tools versions are supported, go to the [VMware Product Interoperability Matrix](#), select the solution **VMware Horizon View** and the version, then select **VMware Tools (downloadable only)**.
- If you want to install View Composer silently, see the VMware Knowledge Base (KB) article 2148204, [Microsoft Windows Installer Command-Line Options for Horizon Composer](#).
- This Horizon 7 release includes new configuration requirements that differ from some earlier releases. See the *Horizon 7 Upgrades* document for upgrade instructions.
- Horizon 7.5.2 is an Extended Service Branch (ESB) that will receive periodic service pack (SP) updates, which include cumulative, critical bug fixes, and security fixes. See the VMware Knowledge Base (KB) article 52845 [FAQ: Horizon 7, App Volumes, UEM](#)

[Extended Service Branches \(ESB\)](#) for detailed information of ESB. See the *Horizon 7 Upgrades* document for upgrading to SPs.

- You can upgrade Horizon 7.5.2 to version 7.8 and later. See the [VMware Product Interoperability Matrix](#).
- If you intend to upgrade a pre-6.2 installation of Horizon 7, and the Connection Server, security server, or View Composer server uses the self-signed certificate that was installed by default, you must remove the existing self-signed certificate before you perform the upgrade. Connections might not work if the existing self-signed certificates remain in place. During an upgrade, the installer does not replace any existing certificate. Removing the old self-signed certificate ensures that a new certificate is installed. The self-signed certificate in this release has a longer RSA key (2048 bits instead of 1024) and a stronger signature (SHA-256 with RSA instead of SHA-1 with RSA) than in pre-6.2 releases. Note that self-signed certificates are insecure and should be replaced by CA-signed certificates as soon as possible, and that SHA-1 certificates are no longer considered secure and should be replaced by SHA-2 certificates.
Do not remove CA-signed certificates that were installed for production use, as recommended by VMware. CA-signed certificates will continue to work after you upgrade to this release.
- To take advantage of Horizon 7 features such as Virtual SAN 6.1, GRID vGPU, and Virtual Volumes, install vSphere 6.0 and subsequent patch releases.
- When you upgrade to this release, upgrade all Connection Server instances in a pod before you begin upgrading Horizon Agent, as described in the *Horizon 7 Upgrades* document.
- After you have performed a fresh install or upgraded all Connection Server instances to Horizon 7 version 7.2 or later, you cannot downgrade the Connection Server instances to a version earlier than Horizon 7 version 7.2 because the keys used to protect LDAP data have changed. To keep the possibility of downgrading Connection Server instances while planning an upgrade to Horizon 7 version 7.2 or later, you must perform an LDAP backup before starting the upgrade. If you need to downgrade the Connection Server instances, you must downgrade all Connection Server instances and then apply the LDAP backup to the last Connection Server that is downgraded.
- The product build number for Horizon Agent in this release does not appear under the "Version" column in the "Add/Remove Programs" panel. To get the product build number, click "VMware Horizon Agent" and view the comments section in the panel below.
- The download page in this release includes a Horizon HTML Access Direct-Connection file that provides web server static content for supporting HTML Access with View Agent Direct-Connection (VADC). For information about setting up HTML Access for VADC, see [Setting Up HTML Access](#) in the *View Agent Direct-Connection Plug-in Administration* document.
- Selecting the Scanner Redirection setup option with Horizon Agent installation can significantly affect the host consolidation ratio. To ensure the optimal host consolidation, make sure that the Scanner Redirection setup option is only selected for those users who need it. (By default, the Scanner Redirection option is not selected when you install Horizon Agent.) For users who need the Scanner Redirection feature, configure a separate desktop pool and select the setup option only in that pool.
- Horizon 7 uses only TLSv1.1 and TLSv1.2. In FIPS mode, it uses only TLSv1.2. You might not be able to connect to vSphere unless you apply vSphere patches. For information about re-enabling TLSv1.0, see [Enable TLSv1 on vCenter Connections from Connection Server](#) and [Enable TLSv1 on vCenter and ESXi Connections from View Composer](#) in the *Horizon 7 Upgrades* document.
- FIPS mode is not supported on releases earlier than 6.2. If you enable FIPS mode in

Windows and upgrade Horizon Composer or Horizon Agent from a release earlier than Horizon View 6.2 to Horizon 7 version 7.2 or later, the FIPS mode option is not shown. You must do a fresh install instead to install Horizon 7 version 7.2 or later in FIPS mode.

- Linux desktops use port 22443 for the VMware Blast display protocol.
- Starting with Horizon 7 version 7.2, it is possible that the ordering of cipher suites can be enforced by Connection Server. For more information, see the *Horizon 7 Security* document.
- Starting with Horizon 7 version 7.2, Connection Server must be able to communicate on port 32111 with other Connection Servers in the same pod. If this traffic is blocked during installation or upgrade, installation will not succeed.
- Starting with Horizon 7 version 7.3.2, TLS handshakes on port 443 must complete within 10 seconds, or within 100 seconds if smart card authentication is enabled. In previous releases of Horizon 7, TLS handshakes on port 443 were allowed 100 seconds to complete in all situations. You can adjust the time for TLS handshakes on port 443 by setting the configuration property `handshakeLifetime`. Optionally, the client that is responsible for an over-running TLS handshake can be automatically added to a blacklist. New connections from blacklisted clients are delayed for a configurable period before being processed so that connections from other clients take priority. You can enable this feature by setting the configuration property `secureHandshakeDelay`. For more information about setting configuration properties, see the *Horizon 7 Security* document.

[Top of Page](#)

Internationalization

The Horizon Administrator user interface, Horizon Administrator online help, and Horizon 7 product documentation are available in Japanese, French, German, Spanish, simplified Chinese, traditional Chinese, and Korean. For the documentation, see the [Documentation Center for VMware Horizon 7](#).

[Top of Page](#)

Compatibility Notes

- For the supported guest operating systems for Horizon Agent on single-user machines and RDS hosts, see VMware Knowledge Base (KB) article 2150295, [Supported Windows Versions for Remote Desktop Systems for Horizon Agent](#).
- If you use Horizon 7 servers with a version of View Agent older than 6.2, you will need to enable TLSv1.0 for PCoIP connections. View Agent versions that are older than 6.2 support the security protocol TLSv1.0 only for PCoIP. Horizon 7 servers, including connection servers and security servers, have TLSv1.0 disabled by default. You can enable TLSv1.0 for PCoIP connections on these servers by following the instructions in VMware Knowledge Base (KB) article 2130798, [Configure security protocols for PCoIP for Horizon 6 version 6.2 and later, and Horizon Client 3.5 and later](#).
- For the supported Linux guest operating systems for Horizon Agent, see [System Requirements for Horizon 7 for Linux](#) in the *Setting Up Horizon 7 for Linux Desktops* document.
- For the supported operating systems for Connection Server, security server, and View

Composer, see [System Requirements for Server Components](#) in the *Horizon 7 Installation* document.

- Horizon 7 functionality is enhanced by an updated set of Horizon Clients provided with this release. For example, Horizon Client 4.0 or later is required for VMware Blast Extreme connections. See the [VMware Horizon Clients Documentation](#) page for information about supported Horizon Clients.
- The instant clones feature requires vSphere 6.0 Update 1 or later.
- Windows 7 and Windows 10 are supported for instant clones, but not Windows 8 or Windows 8.1.
- See the [VMware Product Interoperability Matrix](#) for information about the compatibility of Horizon 7 with current and previous versions of vSphere.
- For the supported Active Directory Domain Services (AD DS) domain functional levels, see [Preparing Active Directory](#) in the *Horizon 7 Installation* document.
- For more system requirements, such as the supported browsers for Horizon Administrator, see the *Horizon 7 Installation* document.
- RC4, SSLv3, and TLSv1.0 are disabled by default in Horizon 7 components, in accordance with RFC 7465, "Prohibiting RC4 Cipher Suites," RFC 7568, "Deprecating Secure Sockets Layer Version 3.0," PCI-DSS 3.1, "Payment Card Industry (PCI) Data Security Standard", and SP800-52r1, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations." If you need to re-enable RC4, SSLv3, or TLSv1.0 on a Connection Server, security server, View Composer, or Horizon Agent machine, see [Older Protocols and Ciphers Disabled in View](#) in the *Horizon 7 Security* document.
- If a PCoIP Secure Gateway (PSG) has been deployed for PCoIP connections, zero client firmware must be version 4.0 or later.
- When using Client Drive Redirection (CDR), deploy Horizon Client 3.5 or later and View Agent 6.2 or later to ensure that CDR data is sent over an encrypted virtual channel from an external client device to the PCoIP security server and from the security server to the remote desktop. If you deploy earlier versions of Horizon Client or Horizon Agent, external connections to the PCoIP security server are encrypted, but within the corporate network, the data is sent from the security server to the remote desktop without encryption. You can disable CDR by configuring a Microsoft Remote Desktop Services group policy setting in Active Directory. For details, see [Managing Access to Client Drive Redirection](#) in the *Configuring Remote Desktop Features in Horizon 7* document.
- The USB Redirection setup option in the Horizon Agent installer is deselected by default. You must select this option to install the USB redirection feature. For guidance on using USB redirection securely, see [Deploying USB Devices in a Secure View Environment](#) in the *Horizon 7 Security* document.
- The Global Policy, Multimedia redirection (MMR), defaults to **Deny**. To use MMR, you must open Horizon Administrator, edit Global Policies, and explicitly set this value to **Allow**. To control access to MMR, you can enable or disable the Multimedia redirection (MMR) policy globally or for an individual pool or user. Multimedia Redirection (MMR) data is sent across the network without application-based encryption and might contain sensitive data, depending on the content being redirected. To ensure that this data cannot be monitored on the network, use MMR only on a secure network.
- Before you set the level of Transparent Page Sharing (TPS) in Horizon Administrator, VMware recommends that the security implications be understood. For guidance, see the VMware Knowledge Base (KB) article 2080735, [Security considerations and disallowing inter-Virtual Machine Transparent Page Sharing](#).
- To use View Storage Accelerator in a vSphere 5.5 or later environment, a desktop virtual

machine must be 512GB or smaller. View Storage Accelerator is disabled on virtual machines that are larger than 512GB. Virtual machine size is defined by the total VMDK capacity. For example, one VMDK file might be 512GB or a set of VMDK files might total 512GB. This requirement also applies to virtual machines that were created in an earlier vSphere release and upgraded to vSphere 5.5.

- Horizon 7 does not support vSphere Flash Read Cache (formerly known as vFlash).
- In Horizon (with View) version 6.0 and later releases, the View PowerCLI cmdlets Get-TerminalServer, Add-TerminalServerPool, and Update-TerminalServerPool have been deprecated.
- Screen DMA is disabled by default in virtual machines that are created in vSphere 6.0 and later. View requires screen DMA to be enabled. If screen DMA is disabled, users see a black screen when they connect to the remote desktop. When Horizon 7 provisions a desktop pool, it automatically enables screen DMA for all vCenter Server-managed virtual machines in the pool. However, if Horizon Agent is installed in a virtual machine in unmanaged mode (VDM_VC_MANAGED_AGENT=0), screen DMA is not enabled. For information about manually enabling screen DMA, see VMware Knowledge Base (KB) article 2144475, [Manually enabling screen DMA in a virtual machine](#)
- vGPU enabled instant clone desktop pools are supported for vSphere 2016 and later.
- Microsoft Windows Server requires a dynamic range of ports to be open between all Connection Servers in the Horizon 7 environment. These ports are required by Microsoft Windows for the normal operation of Remote Procedure Call (RPC) and Active Directory replication. For more information about the dynamic range of ports, see the Microsoft Windows Server documentation.
- In Horizon 7 version 7.2 or later, the viewDBChk tool will not have access to vCenter or View Composer credentials and will prompt for this information when needed.
- The forwarding rules for HTTP requests received by Connection Server instances and security servers have changed at this release. If you have defined custom frontMapping entries in locked.properties, you should remove them before upgrading. If you wish to disallow administrator connections to certain Connection Server instances, then instead of defining custom frontMapping entries, add this entry to locked.properties:

```
frontServiceWhitelist = tunnel|ajp:broker|ajp:portal|ajp:misc|moved:*|file:docroot
```

On security servers, this entry is applied automatically and does not need to be set in locked.properties.

- Horizon Persona Management is not compatible with User Writable Volumes created with the UIA + Profile template.
- When you use a subscription license with Horizon Connection Server, the Connection Server switches to Workspace ONE mode, which uses VMware Identity Manager for authentication. For more information, see the VMware Knowledge Base (KB) article 53578 [Feature Limitations for Horizon 7 License Enforcement with Workspace ONE](#)
- In Horizon 7 version 7.0.3 or later, internal validation checks determine if the instant clone and internal template have valid IP addresses and a network connection. If a virtual machine has a NIC that cannot be assigned an IP address during provisioning, instant-clone provisioning fails.

[Top of Page](#)

Supported Windows 10 Operating Systems

For an updated list of supported Windows 10 operating systems, see VMware Knowledge Base (KB) article 2149393, [Supported Versions of Windows 10 on Horizon 7](#).

For more information on upgrade requirements for Windows 10 operating systems, see VMware Knowledge Base (KB) article 2148176, [Upgrade Requirements for Windows 10 Operating Systems](#) here.

[Top of Page](#)

Support for Red Hat Enterprise Linux Workstation

Horizon Agent for Linux supports installation on systems running Red Hat Enterprise Linux Workstation. Red Hat Enterprise Linux Server is not supported.

In the [Setting Up Horizon 7 for Linux Desktops](#) document, all occurrences of "Red Hat Enterprise Linux" and "RHEL" refer to Red Hat Enterprise Linux Workstation only.

For the list of supported versions of Red Hat Enterprise Linux Workstation, see [System Requirements For Horizon 7 for Linux](#).

[Top of Page](#)

Prior Releases of Horizon 7

Features that were introduced in prior releases are described in the release notes for each release, along with existing known issues.

[Top of Page](#)

Resolved Issues

- 2139103: User logon fails because Horizon Client does not connect to Horizon Agent in time and logs the user off from the session.
- 2142357: Horizon Agent installed with the scanner redirection feature on an RDS Host goes into the Agent unreachable state after multiple logons.
- 2142360: The published application hangs because the scanner redirection feature does not work correctly when the user attempts a scan from within the application.
- 2142365: Sessions established with the Blast display protocol fail after many user logons when shared memory optimization is disabled
- 2142393: VMware Blast session starts are blocked because of an internal Blast pipe stall.
- 2181324: The protocol provider loses connection to an internal node manager and doesn't recover.
- 2183184: All users are suddenly disconnected and cannot reconnect to the existing session because of a session protocol failure.

- 2186048: The user's mouse cursor intermittently disappears during an active session.
- 2186220: On reconnect, the published application's full screen size is reduced to 90% of its original size.
- 2189058: When multiple users are logging into the Windows Terminal Services server, the virtual machine crashes with a Blue Screen of Death (BSOD).
- 2189089: When a user logs on to a Windows 10 2016 LTSB desktop, a temporary user profile is used because the ntuser.dat file is corrupted.
- 2189485: Folder redirection does not work while accessing a folder from a Windows 10 virtual machine that uses the Sysprep customization specification with the CopyProfile option.
- 2196256: The desktop manager on an RDS Host that has Horizon Agent installed does not delete session objects when the Windows desktop session ends.
- 2200491: USB redirection failures on zero clients can occur with User Environment Manager.
- 2200526: The USB redirection feature is not available for an RDS Host that has Horizon Agent and View Agent Direct-Connection Plug-In installed.
- 2209512: The Windows Terminal Services server crashes during client drive redirection.
- 2215854: The scanner fails to connect to the RDS Host session when the session starts.
- 2219964: The push image operation for an instant-clone desktop pool fails if the master image has the Content-Based Read Cache (CBRC) feature enabled.
- 220149: Microsoft Windows framework issues related to scale and functionality are fixed.
- 2220233: After an upgrade to Horizon 7 version 7.5, the Horizon Persona Management profile does not get loaded.
- 2224540: VMware Virtual Channel (VVC) issues related to scale and functionality are fixed.
- 2227100: Sometimes it might take more than 10 seconds to launch a desktop from Horizon Client if the user session is stolen.
- 2228863: Consecutive rebalance operations on a desktop pool leaves the .hlog extension file in the folders for the datastore associated with the desktop pool.
- 2232455: Horizon 7 fails to add the enrollment sever configured for TrueSSO to a Connection Server in a pod.
- 2238371: Multiple internal Blast protocol failures occur during 6000 user logons.
- 2247611: VMware Virtual Channel (VVC) API can call a shared channel pointer outside the lock.
- 2223432: Cannot create instant-clone desktop pools in an environment that contains

multiple vLANs.

- 2238536: The VMware Blast Service crashes because of a URI parsing issue.
- 2284631: Computer-based GPOs do not get applied to instant clones in Horizon 7.
- 2266283: End users who are entitled to a desktop sometimes encounter a “not entitled” error when they start the desktop.
- 2284633: Connection Server cannot accept the HTTPS session because it is waiting on responses from SQL server.
- 2189012: The virtual desktop freezes intermittently because the Blast Protocol process has a CPU spike approximately 10 seconds per minute during network operations.
- 2226182: Following an instant-clone provisioning failure, the instant-clone summary page does not load and errors are generated after a period of time.
- 2289040: Automated desktop pools created on Windows 10 1809 go into the Agent Unreachable state.

Known Issues

The known issues are grouped as follows.

- [Horizon Persona Management](#)
- [View Composer](#)
- [Horizon Connection Server](#)
- [Horizon Agent for Linux](#)
- [Horizon Agent](#)
- [Horizon GPO Bundle](#)
- [Horizon Client](#)
- [Horizon JMP Server and JMP Integrated Workflow](#)

Horizon Persona Management

- Horizon Persona Management might not correctly replicate a user persona to the central repository if the desktop virtual machine is extremely low on disk space.
- With Persona Management, you can use group policy settings to redirect user profile folders to a network share. When a folder is redirected, all data is stored directly on the network share during the user session. Windows folder redirection has a check box called Grant user exclusive rights to folder-name, which gives the specified user exclusive rights to the redirected folder. As a security measure, this check box is selected by default. When this check box is selected, administrators do not have access to the redirected folder. If an administrator attempts to force change the access rights for a user's redirected folder, Persona Management no longer works for that user.

Workaround: See VMware Knowledge Base (KB) article 2058932, [Granting domain administrators access to redirected folders for View Persona Management](#).

- Persona Management is not supported on session-based desktop pools that run on RDS

hosts.

Workaround: Install Persona Management in automated or manual desktop pools that run on single-user machines.

- After every login, Persona Management takes a long time to replicate the first user persona on a guest operating system that uses the "v6" version of the user profile.
- On a Windows 8 desktop, if you enable the View Persona Management setting, Remove local persona at logoff, and a user creates a PDF file, logs off of the desktop, and logs back in again, the user cannot open the offline PDF file. The Windows 8 Reader cannot download the offline PDF content.

Workaround: Manually download the file by right-clicking the file and selecting **Properties** or selecting **Open with... Adobe Reader**.

- When you log in to a Windows 10 LTSB machine using a persona profile and try to access redirected folders from Quick Access, such as Downloads or My Documents, you get this error:

C:\Users\vduser7\Downloads is unavailable. Microsoft doesn't provide the API to add folder or file to Quick Access.

Workaround: None

- When you log into a VM configured with Persona Management for the second time, the Microsoft Edge browser crashes and an error message that states the OneDrive application has never been used appears. Additionally, the files and folders cannot be replicated properly. This happens only with Windows 10 build 1709 November 2017 update.

Workaround: Disable the Persona Management setting **Roam Local Settings Folders**.

When you disable this setting, the Microsoft Edge browser works properly but the OneDrive application is only available when you log in for the first time.

- Offline icons are not displayed for files on a Windows Server 2012 virtual machine with Horizon Persona Management setting enabled.

Workaround: None known.

- After a successful initial login to a virtual machine with Horizon Agent installed on Windows 10 version 1703 CBB system and with Persona Management enabled, the "OneDrive -Bad Image error" message is displayed during subsequent login attempts.

Workaround: Do not use OneDrive on your Windows 10 version 1703 CBB system. In the Group Policy Management Editor, disable the "Roam local settings folders" setting in the **Computer Configuration > Policies > Administrative Templates > VMware View Agent Configuration > Persona Management > Roaming & Synchronization** folder.

- After a recompose, refresh, or rebalance operation with a persistent disk, Windows 10 desktops might fail to start, or become untiled from the Start menu. Windows applications can include applications such as Windows Store, native applications, Edge Browser, and Cortana Search. This issue affects multiple version of Windows 10 intermittently, depending on applications used. This problem affects the following desktop types:
 - Linked-clone dedicated desktops with a persistent disk where the persistent disk is used to store app settings.
 - Linked-clone floating desktops with Persona Management enabled that use a persistent disk as a local disk and the Persona Management setting **Roam Local Settings Folders** enabled.

- This issue is not seen with floating or dedicated linked-clone desktop pools where the user profile is redirected to network share with or without Persona Management enabled. If Persona Management is enabled, the user profile is set to roam with VMware Persona GPO settings.
- This issue is not seen when persistent disk and/or Persona Management are used to persist only My Documents and Exchange 365 .pst/ost files.

View Composer

- When Horizon Administrator provisions a linked-clone pool with thousands of desktops, a few machines (one or two per thousand) might fail with a "Customization timed out" error. If automatic recovery is enabled (the recommended setting for production environments), machines in error are automatically recreated and provisioned. No workaround is required.
Workaround: If automatic recovery is disabled, manually delete the machines in error in Horizon Administrator. Horizon Administrator will provision new machines as part of normal pool management.
- When deleting a large desktop pool, a number of folders containing a.hlog file and an empty sub folder named.sdd.sf might remain undeleted.
Workaround: Manually delete the folders that are left behind after a deletion operation. For instructions, see the Solution in VMware Knowledge Base (KB) article 2108928, [Rebalance operation leaves VM folders in previous data stores](#).
- If you upgrade a virtual machine with an IDE controller from Windows XP to Windows 7, take a snapshot of the virtual machine, and create a linked-clone pool, the linked clone cannot be customized, and pool creation fails.
Workaround: Add a SCSI controller and a disk to the virtual machine. Next, launch VMware Tools and install a VMware SCSI controller driver on the virtual machine. Next, take a snapshot and create the linked-clone pool.
- When you provision linked-clone desktops that are customized by Sysprep, some desktops might fail to customize.
Workaround: Refresh the desktops. If a small number of desktops still fail to customize, refresh them again.
- Do not change the log on account for the VMware View Composer Guest Agent Server service in a parent virtual machine. By default, this is the Local System account. If you change this account, the linked clones created from the parent do not start.
- Desktop pool provisioning fails with the error messagePolling progress failure: Unable to connect to View Composer server<https://machine-name:18443>.java.net.ConnectException: Connection refused: connect.
Workaround: Restart the VMware vCenter Server service and then reprovision the desktop pool.
- When you run View Composer installer on Windows Server 2016 with the latest Windows update from command line, you get a Microsoft .NET 4.6 framework error. This issue occurs because the CLI installer is not able to recognize latest version of Microsoft .NET 4.7.
Workaround: Use the View Composer installer user interface to run the installer.
- If a linked-clone pool consists of vSphere 5.5 virtual machines, a View Composer rebalance operation can fail with a FileAlreadyExists error. This problem occurs only when the desktop pool uses different data stores for the OS disk and the user data disk and the data store selection for the user data disk changes before the View Composer rebalance operation takes place.

Workaround: Detach the persistent disk from the linked clone desktop that has the FileAlreadyExists error. Later, you can attach the archived disk to a new virtual machine and recreate the linked-clone desktop or attach it to an existing linked-clone desktop as a secondary disk. You can prevent this problem from occurring by either keeping the OS disk and user data disk on the same data store or by not changing the data store selections before a View Composer rebalance operation.

- Provisioning View Composer linked clones fails on some Virtual Volumes storage arrays. The following message is displayed: "Error creating disk Error creating VVol Object. This may be due to insufficient available space on the datastore or the datastore's inability to support the selected provisioning type." View Composer creates a small internal disk in thick-provisioned format, although all other linked clone disks use thin provisioning. This issue occurs if the 3rd-party Virtual Volumes storage array does not support thick-provisioned disks by default.

Workaround: Enable thick provisioning on the storage array to allow Virtual Volumes to create thick-provisioned disks.

- When you attach or recreate a View Composer persistent disk stored on a Virtual SAN data store, the virtual disk's storage policy in vCenter Server is shown as "Out of date." The original storage profile is not preserved.

Workaround: In vSphere Web Client, reapply the storage policy to the virtual disks.

- When a space reclamation operation is run for Windows 8.x linked clone virtual machines, the size of the system disposable disk and user persistent disk might increase to its maximum capacity. This space increase only happens the first time space reclamation is done. For the OS disk, space reclamation works as expected and reclaims the unused space. This issue does not affect View Composer desktops that do not use system disposable disks or user persistent disks.

Workaround: When you configure View Composer desktops on Windows 8 or 8.1 virtual machines and enable space reclamation, do not configure system disposable disks or user persistent disks.

- Creating or recomposing desktop pools fails after you upgrade the parent virtual machine from build 1511 to build 1607 of the Windows 10 operating system. Build 1607 is the Windows 10 Anniversary Update operating system.

Workaround:

- Option 1. Perform a fresh installation of Windows 10 Build 1607 on the parent virtual machine.
 - Option 2. Do not select "Redirect disposable files" in the desktop pool creation wizard.
- Virtual SAN data stores are only accessible from hosts that belong to the Virtual SAN cluster, and not from hosts that belong to a different cluster. Therefore, rebalance of pools from one Virtual SAN data store to another Virtual SAN data store in a different cluster is not supported.
- In an environment where a large virtual desktop pool (for example, 2,000 desktops) is created on Virtual Volumes data stores that reside on a NetApp storage system running ON TAP 8.2.x or earlier, a recompose operation may fail for a small number of desktops with the error message "The VVol target encountered a vendor specific error."

Workaround: Upgrade the NetApp storage system to ONTAP 8.3 or later.

- When recomposing Windows 8.1 desktops, the Sysprep customization can fail with a Customization operation timed out error message. This problem is caused by a Windows 8.1 scheduled maintenance task that recovers disk space by removing unused features.

Workaround: Use the following command to disable the maintenance task immediately after completing Setup: `Schtasks.exe/change /disable /tn"Microsoft\Windows\AppxDeploymentClient\Pre-`

staged appcleanup"

- The rebalance operation from a vSAN datastore to a non-vSAN datastore with VMFS6 file system fails in the vSAN cluster.

Workaround: None.

- Connection to View Composer fails when you run the following command: `viewdbchk.cmd -findMachine`

Workaround: Import the self-signed certificate for View Composer into Connection Server's keystore or use a custom CA certificate.

- Due to recent changes to the Guest Customization utility on vSphere 6.7, during an Horizon 7 upgrade to version 7.5 you cannot use View Composer 7.5 with an earlier version of Horizon Agent for provisioning and recomposing linked-clone pools using the Sysprep customization method. The linked-clone desktops and farms get stuck indefinitely in the customization state during provisioning or recomposing operations.

Workaround: Upgrade to the latest version of VMware Tools and upgrade Horizon Agent to version 7.5 on the parent virtual machine and take a snapshot of the upgraded parent virtual machine. Then, provision or recompose linked-clone desktop pools using the Sysprep customization method on vSphere 6.7.

Horizon Connection Server

- If you upgrade to vSphere 5.5 or a later release, verify that the domain administrator account that you use as the vCenter Server user was explicitly assigned permissions to log in to vCenter Server by a vCenter Server local user.
- During provisioning of an instant-clone desktop pool, if there is not enough space available on the data stores, the error message that is displayed in Horizon Administrator is "Cloning of VM <VM name> has failed -VC_FAULT_FATAL: Failed to extend swap file from 0 KB to 2097152 KB." This message does not clearly indicate the root cause of the problem.

Workaround: Not required.

- In Horizon Administrator, if you go to **Catalog > Desktop Pools**, double-click an instant-clone desktop pool, go to the **Inventory** tab and click **Machines (Instant Clone Details)**, the window displays details of the instant clones. However, the OS Disk data store column displays no information.

Workaround: None

- In a large scale environment, some of the desktops in an instant-clone desktop pool might go into the Invalid IP state.

Workaround: In Horizon Administrator, go to **Pool Inventory**, select the desktops in the **Invalid IP** state and click **Recover**.

- When you restart or reset a virtual machine for which an end user session exists in a desktop pool from vCenter Server or from the Windows Operating System menu, the virtual machine restarts but the status of the virtual machine might appear in the "Already Used" state in Horizon Administrator.

This problem can occur for the following pool types:

- Instant-clone desktop pools.
- Linked-clone floating desktop pools with "Delete on log Off" enabled.
- Linked-clone floating desktop pools with "Refresh on log Off" enabled.
- Full-clone floating desktop pools with "Delete on log Off" enabled.

Workaround: Use Horizon Administrator or Horizon Client to restart or reset the virtual

machine in the instant-clone desktop pool. If the virtual machine is already in the “Already Used” state, remove the virtual machine. This action automatically creates a new virtual machine based on the pool provisioning settings.

- Instant-clone desktop pool creation fails when the OU or sub-OU name contains the special character "ß".

Workaround: Remove "ß" in the OU or sub-OU name when you create instant clones.

- If you provision instant clones on local datastores, the corresponding hosts cannot be put into maintenance mode. This occurs because the internal VMs and the instant clones are stored on local datastores so they cannot be migrated.

Workaround: Delete the instant-clone desktop pool. This will delete the related VMs and enable the corresponding hosts to enter maintenance mode.

- ESXi host remediation that uses VUM fails if the instant-clone Parent VM is present on the host in a powered-on state

Workaround: For more information, see the VMware Knowledge Base (KB) article 2144808, [Entering and exiting maintenance mode for an ESXi host that has Horizon instant clones](#).

- For this release, Windows Universal apps are not supported as hosted remote applications. For example, Universal apps do not appear in the list of apps provided by a Windows Server 2016 RDS farm. Universal apps, such as the Edge browser or the Calculator included with Windows 10 or a Windows Server 2016 RDS host, are built on the Universal Windows Platform (UWP). Universal apps require Windows Explorer to be run. In addition, manually launching Universal apps through the Command Prompt will show an error message.
- If you deploy an automated farm from a Windows Server 2012 parent virtual machine that has the RDS role enabled, Sysprep customization will fail on the deployed linked-clone virtual machines. This 3rd-party issue does not occur on other Windows Server versions that have the RDS role enabled.

Workaround: On the Windows Server 2012 parent virtual machine, apply the Microsoft hotfix available at <https://support.microsoft.com/en-us/kb/3020396>.

- For True SSO, the connectivity status between the Connection Server instance and the enrollment server is displayed only on the System Health Status dashboard for the connection server that you are using to access Horizon Administrator. For example, if you are using <https://server1.example.com/admin> for Horizon Administrator, the connectivity status to the enrollment server is collected only for the server1.example.com connection server. You might see one or both of the following messages:

- The primary enrollment server cannot be contacted to manage sessions on this connection server.
- The secondary enrollment server cannot be contacted to manage sessions on this connection server.

It is mandatory to configure one enrollment server as primary. Configuring a secondary enrollment server is optional. If you have only one enrollment server, you will see only the first message (on error). If you have both a primary and a secondary enrollment server and both have connectivity issues, you will see both messages.

- When you set up True SSO in an environment with CAs and SubCAs with different templates setup on each of them, you are allowed to configure True SSO with a combination of template from a CA or SubCA with another CA or SubCA. As a result, the dashboard might display the status of True SSO as green. However, it fails when you try to use True SSO.

- When using Horizon Administrator from a Firefox browser, if you enter Korean characters in a text field using the Korean Input Method Editor (IME), the Korean characters are not displayed correctly. This issue occurs only with Firefox. This is a 3rd-party issue.
Workaround: Use a different browser. If you still want to use Firefox, input Korean characters one by one.
- If you change the Blast Secure Gateway (absg.log) log level on a Connection Server instance from Info to Debug, the log level remains Info. (You change the log level by opening the **Set View Connection Server Log Levels** on a Connection Server instance, changing the absg log level, and restarting the VMware View Blast Secure Gateway service.) Changing the log level from Debug to Info works properly.
Workaround: None.
- On rare occasions, the system health status of Event Database maybe displayed as red on the Horizon Administrator dashboard, with the error message "Cannot drop the view 'VE_user_events', because it does not exist or you do not have permission." This condition does not indicate a real error and will resolve itself after a short period.
Workaround: None.
- In Horizon Help Desk Tool, the pod name does not appear if the session is a local session or a session running in the local pod.
Workaround: Set up the Cloud Pod Architecture environment to view pod names in Horizon Help Desk Tool.
- The Workspace ONE mode setting does not get reflected in the replica server from Workspace ONE.
Workaround: Configure the Workspace ONE mode in Connection Server.
- If NVIDIA drivers are installed on a virtual machine that you use as a parent or template to deploy a desktop pool, and the machines are deployed on non-NVIDIA GRID hardware on the ESXi hosts, users might not be able to start desktop sessions correctly. This issue might occur if the virtual machine was used previously in an NVIDIA GRID vGPU deployment.
Workaround: Remove the NVIDIA drivers from the virtual machine before you take a snapshot or make a template and deploy the desktop pool.
- When you create full-clone desktop pools, sometimes wrong templates are displayed and valid templates are hidden due to a cache issue.
Workaround: Restart Connection Server.
- When you use the vdmutil command to create a URL content redirection setting, you must name the setting url-filtering. If the setting name is not url-filtering, there will be no redirection. For example:


```
vdmutil --createUrlSetting --urlSettingName url-filtering --urlScheme http --entitledApplication iexplore2012 --agentURLPattern "http://google.*" --urlRedirectionScopeLOCAL --authAs johndoe --authDomain mydomain --authPasswordsecret
```
- VMware does not recommend creating more than one URL content redirection setting in this release.
- For virtual machines that have hardware version 8, the maximum allowed video RAM is 128MB. For virtual machines that have hardware version 9 and later, the maximum allowed video RAM is 512MB. If you configure a value from Horizon Administrator that exceeds the video RAM limit for a virtual machine's hardware version, errors appear in the vSphere Client Recent Tasks pane and the configuration operation keeps repeating. This problem

occurs only if you configure the video memory value through Horizon Administrator (Pool Settings page) and not through vSphere Client.

Workaround: Either upgrade the hardware version of the virtual machines in vSphere Client, or use Horizon Administrator to set the proper value for video memory based on the current virtual machine hardware version.

- When you try to add a SAML authenticator in Horizon Administrator, the **Add** button is disabled on the Manage SAML Authenticators page.

Workaround: Log in to Horizon Administrator as a user who has the Administrators or Local Administrators role.

- The ViewDbChk utility can display an "Archiving persistent disks..." message while removing machines from an automated linked-clone pool with floating assignment or an automated farm.

Workaround: None.

- Cloud Pod Architecture configuration changes made by another Horizon administrator while you are logged in to Horizon Administrator are not visible in your current Horizon Administrator session.

Workaround: Log out of Horizon Administrator and log in again to see the changes.

- In a Cloud Pod Architecture environment, pre-launched application sessions from global application entitlements are not shown in **Inventory > Search Sessions** in Horizon Administrator.

Workaround: Log in to the Horizon Administrator user interface for a Connection Server instance in the hosting pod and select **Monitoring > Events** to view pre-launched session information.

- Users that are assigned to 20 to 50 Cloud Pod Architecture global application entitlements have a 20 to 30 second delay while being authenticated to Horizon 7 when connecting through any version of Horizon Client.

Note: In Horizon 7 version 7.2, this connection time is slightly improved.

Workaround: None.

- When using Internet Explorer 10 or 11 on a Windows 8 or later computer, if you set the browser locale to Traditional Chinese, and you log in to Horizon Administrator, the navigation panel might be displayed in Simplified Chinese.

Workaround: Use an alternate browser to log in to Horizon Administrator.

- When provisioning 64- or 32-bit Windows 8 desktops in a vSphere 5.1 environment, the Sysprep customization can fail. The desktops end up in an ERROR state with a Customization timed out error message. This issue occurs when anti-virus software is installed in the parent virtual machine or template. The issue applies to full clone and linked clone desktops. It does not apply to linked clone desktops customized with QuickPrep.

Workaround: Uninstall the anti-virus software on the parent virtual machine or template and recreate the pool.

- For Intel vDGA, only the Haswell and Broadwell series of Intel integrated GPUs are supported. Broadwell integrated GPUs are supported only on vSphere 6 Update 1b and later. Haswell integrated GPUs are supported on vSphere 5.5 and later. The GPU must be enabled in the BIOS before it can be recognized by ESXi. For more information, see the documentation for your specific ESXi host. Intel recommends leaving the graphics memory settings in the BIOS set to their default values. If you choose to change the settings, keep the aperture setting at its default (256M).
- View Storage Accelerator might take tens of minutes to generate or regenerate the digest

files for large virtual disks (for example, a 100 GB virtual disk). As a result, the desktop might be inaccessible for longer than expected.

Workaround: Use the blackout period to control when digest regeneration operations are allowed. Also, use the digest regeneration interval to reduce the frequency of these operations. Alternatively, disable View Storage Accelerator in desktop pools that contain very large virtual machines.

- After you upgrade to vSphere 5.5, a heap size error can occur if you use space-efficient virtual disks and you have more than 200 linked-clone virtual machines per ESXi host. For example: Error:Heap seSparse could not be grown by 12288 bytes for allocation of 12288 bytes

Workaround: Reduce the number of linked-clone virtual machines that use space-efficient virtual disks to less than 200 per ESXi host.

- In a hybrid vSAN environment, about three percent of the virtual machines might not use View Storage Accelerator. These machines will take few seconds longer to start up.

Workaround: Delete and recreate the virtual machines that failed to use View Storage Accelerator.

- In this release, View Storage Accelerator is not supported on Virtual Volume datastores.

Workaround: None

- Provisioning of virtual machines based on View Composer desktop pools configured to use NVIDIA GRID vGPU fails with the following error: The amount of graphics resource available in the parent resource pool is insufficient for the operation.

Workaround: Use a single vGPU profile for all virtual desktops configured for 3D rendering in a cluster.

- For vCenter Server 6.0 U3 or later, including vCenter Server 6.5, internal parent VMs migrate to another host during failure. This migration causes an issue because unnecessary parent VMs reside on the destination host.

Workaround: Manually remove these parent VMs. For more information, see the *Setting Up Virtual Desktops in Horizon 7* document.

- To reduce the possibility of memory exhaustion, vGPU profiles with 512 MB or less of frame buffer support only one virtual display head on a Windows 10 guest operating system.

The following vGPU profiles have 512 Mbytes or less of frame buffer:

- Tesla M6-0B, M6-0Q
- Tesla M10-0B, M10-0Q
- Tesla M60-0B, M60-0Q
- GRID K100, K120Q
- GRID K200, K220Q

Workaround: Use a profile that supports more than one virtual display head and has at least one GB of frame buffer.

- Published desktops and application pools fail to launch if they have the client restriction feature enabled and are entitled to a domain that is configured with a one-way AD trust.

Workaround: None

- After an upgrade, the option to add a farm is grayed out if you have a role with the "Manage Farms and Desktops and Application Pools" (object-specific privilege).

Workaround: Edit the role or create the role again with the "Manage Farms and Desktops and Application Pools" privilege, which also adds the "Manage Global Configuration and

Policies” privilege.

- After an upgrade, the bookmarks do not appear in Workspace ONE.

Workaround: Add the bookmarks from the catalog in Workspace ONE again.

- After you disconnect and reconnect the network cable and click "Disconnect and Log Off" on the client machine, the remote desktop does not disconnect and log off.

Workaround: Manually close the window of the remote desktop and disconnect from the remote session.

- When you create linked clones and full clones with the Sysprep customization method, customization and domain joining sometimes fails on Windows 10 guest operating systems.

Workaround: This occurs because of a Microsoft Windows issue. To resolve this issue, follow the steps in the Microsoft Knowledge Base (KB) article: <https://support.microsoft.com/en-us/help/2769827>.

- Log in to Horizon Console fails from the Microsoft Edge browser and log in to Horizon Console from the Internet Explorer browser displays only keywords instead of icons. This issue occurs when you connect to a Connection Server or security server using an IP address instead of a DNS name.

Workaround: Use a DNS name instead of an IP address when connecting. For more information, see the VMware Knowledge Base (KB) article <https://kb.vmware.com/s/article/2150307>.

- When you use Safari version 10.1.1 as the Web browser to log in to Horizon Console with a Fully Qualified Domain Name, user interface issues such as the bottom panels appearing blank can occur.

Workaround: Safari version 10.1.1 is not a supported Web browser version for Horizon Console. Use a Safari version earlier than version 10.1.1 or version 11.0.2 and later to log in to Horizon Console.

- The following user interface issues occur in Horizon Help Desk Tool for global Linux sessions in a Cloud Pod Architecture deployment:

- An internal error occurred message appears, the Skype for Business status is not displayed, and the operating system version displays as “-” when you click the session details on the Details tab.
- A “failed to get Remote Assistance ticket” message appears when you click Remote Assistance.
- An internal error occurred message appears when you click the Applications tab.

Workaround: None. Horizon Help Desk does not support the following user interface features for Linux desktops: Skype for Business status, Remote Assistance, Applications tab, and the session idle status.

- Horizon Administrator does not update the space reclamation information for a vCenter Server on vSphere version 6.7 that uses the VMFS6 with the automatic UNMAP feature.

Workaround: None.

- The recompose operation for linked clones that use vSphere 6.7 fails in the Virtual Volumes (VVols) data store.

Workaround: Use vSphere 6.5 if you use VVols.

- After an upgrade to Horizon 7 version 7.5, only the first Connection Server that was installed can connect to the enrollment server.

Workaround: Stop the Horizon Connection Server service, remove certificates with the friendly name “vdm.ec” from the VMware Horizon View Certificates store, and restart the Horizon Connection Server service.

- Single Sign-On does not work if you access Horizon Administrator in a timed out tab of Horizon Console and then click the Horizon Console link from Horizon Administrator.

Workaround: Clear the website data in the browser and restart the browser.

- In Horizon Console, filtering for non-vGPU and vGPU templates does not work when you select a desktop pool of full virtual machines and click Edit > vCenter Settings > Browse Template.

Workaround: Use Horizon Administrator to see the correct filtering for non-vGPU and vGPU enabled templates.

- Login to Horizon Console fails if you use the IP address to login to Horizon Console on a Google Chrome, Microsoft Edge, or Safari Web browser.

Workaround: Use the Fully Qualified Domain Name (FQDN) to login to Horizon Console. For more information on using FQDN to log in to Web applications, see the *Horizon 7 Security* document.

- Horizon Administrator displays null/null in the user name column in the Users and Groups page for the following users: Account Operators, Incoming Forest Trust Builders, Terminal Server License Servers, Windows Authorization Access Group, Server Operators, and Pre-Windows 2000 Compatible Access.

Workaround: None.

- After an upgrade to vSphere 6.7, you cannot use the custom specification created with a vSphere version earlier than 6.7.

Workaround: After an upgrade to vSphere 6.7, create a new custom specification and use this specification for pool provisioning.

- Horizon Help Desk Tool displays the logon time for both the brokering pod and the hosting pod but does not display the logon time for a pod that is neither the brokering pod nor the hosting pod. Horizon Help Desk Tool displays the logon time after a few minutes for the hosting pod if the brokering pod is a remote pod.

Workaround: If Horizon Help Desk Tool does not display the logon time for the hosting pod, close the page that displays session details, wait 7-8 mins and navigate to the Details tab to view the session details again.

- VMware Identity Manager sometimes fails to launch desktops. When you save SAML configuration details for the first time in VMware Identity Manager with SAML enabled on Connection Server, desktops do not start.

Workaround: Save the profile again and perform a sync operation on the new profile. The sync operation can occur every hour or day, as set by the administrator.

- Horizon Administrator on Chrome in incognito mode displays an error when you try to export a table's contents as CSV: **The file cannot be exported because a file of the same**

name is currently open. Close the file and try again or use a different file name.

Workaround: Use Horizon Administrator on Chrome in normal mode to export the table.

- In Horizon Console, the options to select or deselect HTML Access are available in IPv6 mode when HTML Access is not installed.

Workaround: None.

- When you use Sysprep to customize Windows 10 linked clones on vCenter Server 6.7, the linked-clone desktops get stuck indefinitely in the customization state during provisioning or recomposing operations.

Workaround: Use vCenter Server 6.5 U2 or earlier. If you must use vCenter Server 6.7, then use the Quickprep customization method.

- In Horizon Console, the desktop pool settings for a desktop pool that contains full virtual machines shows the default value for 3D Renderer as “Manage using vSphere Client” instead of “Disabled”.

Workaround: Use Horizon Administrator to create a desktop pool that contains full virtual machines that shows the default value for 3D Renderer as "Disabled".

- In Horizon Console, you can select vGPU-enabled snapshots during the push-image operation for an instant-clone desktop pool that is not enabled to use vGPU.

Workaround: Use Horizon Administrator to perform the push-image operation.

- In Horizon Console, an internal error occurs or inconsistent behavior is displayed, if you select the Microsoft RDP display protocol and do not allow users to choose a display protocol during the creation or editing of vGPU enabled instant-clone desktop pools and vGPU enabled desktop pools that contain full virtual machines.

Workaround: Use Horizon Administrator to create or edit vGPU enabled instant-clone desktop pools or vGPU enabled desktop pools that contain full virtual machines.

- If you create an automated instant-clone farm in Horizon Console, the corresponding published instant-clone desktop pool shows View Storage Accelerator as disabled in the desktop pool summary page even though vCenter Server has View Storage Accelerator enabled.

Workaround: Use Horizon Administrator to create the automated instant-clone farm so that the corresponding published instant-clone desktop pool has View Storage Accelerator enabled.

- In Horizon Console, the behavior for selecting data stores is different from Horizon Administrator.

- The “Select the Datastore type” menu disappears after sometime when you create or edit an instant-clone desktop pool or farm in Horizon Console.

- Horizon Console does not have the icons to indicate a shared or local data store for an automated desktop pool or automated farm.

Workaround: Use Horizon Administrator to see the type of data stores available for selection in the window for browsing data stores.

- Horizon Console does not have the refresh functionality for browsing data stores for an automated desktop pool or automated farm.

Workaround: To get the latest list of data stores in Horizon Console, close and

reopen the window for browsing data stores.

- Horizon Console does not display a Help icon for the “Show all datastores” button for an instant-clone desktop pool or farm.

Workaround: For more information, see the Help text available in the window for browsing data stores in Horizon Administrator.

- Horizon Console does not display the text “Show all datastores (including local datastores)” for the “Show all datastores” button for an instant-clone desktop pool or farm.

Workaround: Use Horizon Administrator or see the specific workarounds listed with the known issues.

- In Horizon Console, the following information is missing when you select a data store for an instant-clone desktop pool or farm:

- Data Type
- Selected Free Space (GB)
- Min Recommended (GB)
- 50% Utilization (GB)
- Max Recommended (GB)

In Horizon Console, the following information is missing when you select a data store for a desktop pool that contains full virtual machines:

- Free Space Selected

Workaround: Use Horizon Administrator to see all the data store related information when creating instant-clone desktop pools or farms or desktop pools that contain full virtual machines.

- In Horizon Console, when you create an automated desktop pool or farm, the Submit button is still enabled when you select a supported data store and then select an unsupported data store.

Workaround: Use Horizon Administrator to create the automated desktop pool or farm.

- In Horizon Console, the following issues occur when you create or edit an automated desktop pool that contains full virtual machines enabled to use NVIDIA GRID vGPU:

- When you create the desktop pool, you can choose “Suspend” for the remote machine power policy in the desktop pool settings, and when you click Submit, an internal error occurs in the “Ready to Complete” step.
- When you edit the desktop pool, you can choose “Suspend” for the remote machine power policy in the desktop pool settings even though the value “Suspend” is not actually saved for the remote machine policy in the desktop pool settings.

Workaround: Use Horizon Administrator to create or edit an automated desktop pool that contains full virtual machines enabled to use NVIDIA GRID vGPU.

- In Horizon Console, after you select the “Disabled” option for 3D Renderer in the desktop pool settings while editing an instant-clone desktop pool, an unexpected error message popup appears and does not go away.

Workaround: Use Horizon Administrator to edit the desktop pool settings for an instant-clone desktop pool.

- In Horizon Console, an internal error occurs if you use a non-ASCII character in the “Specify names manually” field for a desktop pool that contains full virtual machines.
Workaround: Use only alphanumeric characters, spaces, underscores, and dashes in the “Specify names manually” field for a desktop pool that contains full virtual machines.
- In Horizon Console, there are no user interface options to publish applications and desktops to the client Start Menu as shortcuts.
Workaround: Use Horizon Administrator to publish applications and desktops to the client Start Menu.
- In Horizon Console, the “App Shortcuts” column is missing from the desktop pool properties for all desktop pool types.
Workaround: Use Horizon Administrator to view the “App Shortcuts” column for all desktop pools.
- When you schedule maintenance for a vGPU enabled instant-clone farm, you cannot select a snapshot with a different vGPU profile. This issue occurs in both Horizon Administrator and Horizon Console.
Workaround: None.
- In Horizon Console, the current snapshot is not highlighted in the select image step when you schedule maintenance for an automated farm.
Workaround: Use Horizon Administrator to schedule maintenance for an automated farm.
- In Horizon Console, there is no “Show all images” checkbox to filter and see unsupported snapshots when you schedule a push-image operation for an instant-clone desktop pool or when you schedule maintenance for an automated instant-clone farm. Horizon Console displays only the supported snapshots.
Workaround: Use Horizon Administrator to see unsupported snapshots when you schedule a push-image operation for an instant-clone desktop pool or when you schedule maintenance for an automated instant-clone farm.
- In Horizon Console, you cannot schedule a push-image operation with a different vGPU profile on a vGPU-enabled instant-clone desktop pool.
Workaround: Use Horizon Administrator to schedule the push-image operation.
- In Horizon Administrator, a server error dialog box appears when you navigate to Monitoring > Sessions or Users and Groups > User Profile > Sessions and click on pool name for a session entry that has a different display name than the desktop pool id.
Workaround: Navigate to the desktop pool summary page from Catalog > Desktops.
- When you use Horizon Console with the Internet Explorer Web browser, the button texts in the Desktops page disappear after reloading the Desktops page. This issue occurs in Internet Explorer version 11.966.15063.0, Update version: 11.0.56.
Workaround: Use another browser such as Chrome, Microsoft Edge, Safari, or Firefox that does not have this issue. Or, navigate to another page in Internet Explorer and then navigate back to the Desktops page to fix this issue.
- In Horizon Administrator, you can add a remote access user as an unauthenticated access user. However, unauthenticated access users cannot get remote access from external gateways. The user will not be able to access virtual desktops and can only launch

applications as an unauthenticated access user. If the user tries to login with normal access, an “Incorrect authentication type requested” error message appears.

Workaround: None.

- In Horizon Console, changing the data store to non-vSAN for an automated desktop pool that was created with a vSAN data store does not work and an error message appears that states vSAN must be enabled to select data stores of type vSAN.

Workaround: Use Horizon Administrator to change the data store from vSAN to non-vSAN for an automated desktop pool.

- In Horizon Console, the session timeout value does not match the session timeout value added in the Horizon Administrator interface in View Configuration > Global Settings.

Workaround: None.

- In Horizon Console, after you click Submit during the desktop pool or farm creation or deletion process, the list of desktop pools or farms might not be correctly updated. This issue can occur intermittently.

Workaround: Click the refresh icon to verify the changes.

- Horizon Console does not display icons for different types in entitlements in Users and Groups > Entitlements.

Workaround: Use Horizon Administrator to navigate to Users and Groups > Entitlements to see the icons for different types of entitlements.

- In Horizon Console, when scheduling monthly maintenance for an instant-clone farm, the “Day of Month” field is set to empty and when the “Repeat Interval” field is set, cleared, and set again, the “Next” button is enabled.

Workaround: None.

- In Horizon Console, during the instant-clone desktop pool or farm creation process, the value of port binding in the browse network window does not match the value shown in Horizon Administrator. However, the desktop pool or farm gets created.

Workaround: None.

- In Horizon Console, clicking on the Users and Groups tab from the Remote Access or Unauthenticated Access window does not redirect you to Users and Groups > Entitlements.

Workaround: Click any other tab and then click on the Users and Groups tab.

- Horizon Single Sign On fails when the scope of the trust authentication setting is set to “Selective Authentication”.

Workaround: Use one of the following workarounds to resolve this issue.

- Use domain-wide authentication.
- Continue to use the “Selective Authentication” security setting, but explicitly grant each Horizon Connection Server host (local system) accounts the "Allowed to Authenticate" permission on all the domain controllers of the computer objects (resource computers) that reside in the trusting domain or forest. For information on how to grant the "Allowed to Authenticate" permission, see the Microsoft article [Grant the Allowed to Authenticate permission on computers in the trusting domain or forest.](#)
- In Horizon Console, when you create an instant-clone desktop pool, the 3D Renderer field is missing from the Browse Snapshot window.

Workaround: Use Horizon Administrator to see the 3D Renderer value of the snapshot.

- User/groups search fails in Horizon Console when selective authentication is configured with trusted domain.

Workaround: Configure secondary credentials on Connection Server. To configure secondary credentials, see "Providing Secondary Credentials for Administrators Using the -T option" in the *Horizon Administration* document.

- In Horizon Console, when you create an automated instant-clone desktop pool, the snapshot settings show SVGA settings for vGPU-enabled snapshots. Additionally, when you schedule a push-image operation on an automated instant-clone vGPU-enabled desktop pool, the SVGA settings are shown.

Workaround: Use Horizon Administrator to see snapshot settings that do not include SVGA settings for vGPU-enabled snapshots.

- In Horizon Console, the session status is incorrectly displayed as "Available" instead of "Disconnected" before the timer for the pending session expires.

Workaround: Use Horizon Administrator to view the session status.

- In Horizon Console, an automatic refresh that occurs after adding entitlements to the application pool from the Entitlements tab does not contain the latest entitlements.

Workaround: Click the refresh icon to see the latest entitlements.

- In Horizon Console, the following issues appear when you navigate to Users and Groups > Select a Group > Summary page:

- "Update General User Information" button appears.
- The "Number of Users" field does not appear.
- The "Number of Subgroups" field does not appear.
- The "Phone" and "Email" fields appear.
- The "Find Machines" button does not appear.

Workaround: Use Horizon Administrator to navigate to the Summary page from Users and Groups.

- When you use Sysprep to customize Windows 10 linked clones on vCenter Server 6.7 U1, the linked-clone desktops get stuck indefinitely in the customization state during provisioning.

Workaround: While creating the linked-clone desktop pool, on the View Composer Disks page, select the "Do not redirect Windows profile" and "Do not redirect disposable files" settings. Leave all other settings as the default.

- When you use VMware PowerCLI to perform an update on the event database, the following error occurs: [ViewAPI] Server raised fault: 'Encountered unexpected error during execution' during EventDatabase_Update request.

Workaround: Use Horizon Administrator to update the event database.

Horizon Agent for Linux

This section describes issues that might occur with Horizon Agent for Linux or when you configure a Linux desktop.

- When you configure a Linux virtual desktop for multi-monitor support with a maximum 2560x1600 screen resolution, the submenu dialog boxes do not open.
- If you configure two monitors with different resolutions, and the resolution of the primary screen is lower than that of the secondary screen, you might not be able to move the mouse or drag application windows to certain areas of the screen.
Workaround: Make sure that the primary monitor's resolution is at least as large as the secondary monitor's.
- Configuring four monitors at 2560x1600 resolution on RHEL 6.6 or CentOS 6.6 virtual machines in vSphere 6.0 is not supported.
Workaround: Use 2048x1536 resolution or deploy this configuration in vSphere 5.5.
- If you configure two or more monitors at 2560x1600 resolution on RHEL 6.6 virtual machines in a vDGA environment, desktop performance is poor. For example, application windows do not move smoothly. This issue occurs when RHEL Desktop Effects are enabled.
Workaround: Disable Desktop Effects by going to **System > Preference > Desktop Effects** and selecting **Standard**.
- The Linux agent's keyboard layout and locale do not synchronize with the client if the Keyboard Input Method System is set to fcitx.
Workaround: Set the Keyboard Input Method System to iBus.
- Single Sign On (SSO) does not work well on a RHEL/CentOS 7.2 desktop when you add a domain using System Security Services Daemon (SSSD).
Workaround: After you add a domain using SSSD, modify the `/etc/pam.d/password-auth` file using the information in the VMware Knowledge Base article 2150330 [SSO configuration changes required when using SSSD to join AD on RHEL/CentOS 7.2 Desktops](#).
- The following issues occur with the Horizon Agent for Linux installer when FIPS mode is selected:
 - If the FIPS mode is selected during an interactive installation process, there are some instances when the warning dialog about the FIPS validation status is not displayed and the administrator is unable to confirm whether to proceed with the installation. This occurs when the EULA confirmation is bypassed.
 - If the FIPS mode is specified to be installed on a platform other than RHEL, the FIPS mode installation fails silently. The feature does not get installed and no error message is displayed.**Workaround:** None known.
- The single sign-on (SSO) feature does not work when you try to connect to a remote desktop that has Horizon for Linux installed with the FIPS feature enabled.
Workaround: Manually log in to your Active Directory (AD) user account.

Horizon Agent

- The USB HUB device driver might not be installed properly when you install Horizon Agent on a desktop in a manual desktop pool. This issue can occur if, during the Horizon Agent installation, you restart the system before the USB HUB device driver is fully installed.
Workaround: When you install Horizon Agent and you are prompted to restart the system,

check the system tray to see if the USB HUB device driver software is still being installed. Wait until the device driver software is completely installed (typically about 30 seconds) before you restart the system. If you use a command-line script to install Horizon Agent silently, make sure to wait or sleep the script for long enough to allow the driver installation to complete before you restart the system. If you encounter this issue after Horizon Agent is installed, or you could not delay the system restart during a silent installation, update the USB HUB device driver by taking these steps:

1. In the Device Manager, under **Other Devices**, right-click **VMware View Virtual USB Hub**.
 2. Click **Update Driver Software > Browse my computer for driver software**
 3. Go to C:\ProgramFiles\VMware\VMware View\Agent\bin\drivers and click **Next** to let Windows install the driver.
- To upgrade a desktop from Windows 8 to Windows 8.1, you must uninstall Horizon Agent, upgrade the operating system from Windows 8 to Windows 8.1, and then reinstall Horizon Agent. Alternatively, you can perform a fresh installation of Windows 8.1 and then install Horizon Agent.
 - When you run the Horizon Agent installer on a Windows 8 virtual machine, the Windows desktop appears black when the video driver is being installed. The Windows desktop might appear black for several minutes before the installation completes successfully.
Workaround: Apply the Windows 8.0 May 2013 roll-up before you install Horizon Agent. See [Microsoft KB article 2836988](#).
 - When you run any Horizon 7 installer on a Windows 8.1 or Windows Server 2012/2012 R2 virtual machine (deployed as an RDS host or VDI desktop), the installer can take an unusual amount of time to finish. This problem occurs if the virtual machine's domain controller, or another domain controller in its hierarchy, is unresponsive or unreachable.
Workaround: Verify that the domain controllers have the latest patches, enough free disk space, and can communicate with each other.
 - When you uninstall Horizon Agent from an RDS host, an error dialog can be displayed, which prevents the uninstall operation from being completed. The dialog states that the uninstall operation failed to stop an RDS video driver. This issue can occur when disconnected desktop sessions are still running on the RDS host.
Workaround: Reboot the RDS host to complete the uninstallation of Horizon Agent. As a best practice, ensure that all RDS sessions are logged off before you uninstall Horizon Agent.
 - In FIPS mode, Horizon Agent fails to pair with Connection Server and the pool status is not available when Horizon Agent is installed to a drive other than the C drive.
Workaround: When operating in the FIPS mode, install Horizon Agent on the C drive.
 - A warning message about applications in use appears when you uninstall Horizon Agent on Windows Server 2016.
Workaround: Click "Ignore" in the dialog box that appears when you use Windows Add or Remove Programs to uninstall Horizon Agent. If you uninstall Horizon Agent from the command line, use the command `msiexec /x /qn {GUID of Agent}` instead of the command `msiexec /x {GUID of Agent}`.
 - When you uninstall the Horizon Agent, the mouse speed becomes slow and jerky. Uninstalling Horizon Agent also uninstalls the vmkbd.sys driver.
Workaround: Repair VMware Tools on the Horizon Agent virtual machine.
 - When upgrading from Horizon Agent 7.1 to Horizon Agent 7.2 on a Windows 7 guest

operating system, a "Files in Use" dialog appears. The dialog states that the VMware Horizon Agent application is using files that need to be updated by the setup.

Workaround: Click "Ignore" to proceed with the upgrade.

- Horizon Agent cannot install the virtual printing feature on RDS hosts that are physical machines. Virtual printing is supported on RDS desktops when Horizon Agent is installed on RDS hosts that are virtual machines.

Workaround: Configure RDS hosts on virtual machines and install Horizon Agent.

- The virtual printing feature is supported only when you install it from Horizon Agent. It is not supported if you install it with VMware Tools.
- If vDGA is enabled on a Windows 7 virtual machine that is configured to use NVIDIA driver version 347.25, the desktop session can be disconnected. This issue does not occur on Windows 8.1 or on other NVIDIA driver versions.

Workaround: Do not use NVIDIA driver version 347.25.

- Selecting the Scanner Redirection setup option with Horizon Agent installation can significantly affect the host consolidation ratio. By default, the Scanner Redirection option is not selected when you install Horizon Agent.

Workaround: Make sure that the Scanner Redirection setup option is not selected for most users. For users who need the Scanner Redirection feature, configure a separate desktop pool and select the setup option only in that pool.

- When you uninstall Horizon Agent with the Scanner Redirection feature installed, the uninstall process requires you to close any running applications.

Workaround: None. You must close the listed applications before you continue to uninstall Horizon Agent.

- Client drive redirection does not work with Horizon Agent installed on a 32-bit Windows 10 operating system.

Workaround: None. This is a Microsoft Windows Server issue.

- Windows 10 32-bit Horizon Agent installation throws "the arguments are invalid" exception and the installation continues after you click OK. This error occurs because the print spooler service is disabled.

Workaround: Enable the print spooler service for the installation to work as expected.

- If you install Horizon Agent on a Windows 10 or Windows Server 2016 operating system, and the scaling is not set to 100%, you cannot drag and drop applications from the primary monitor in a multi-monitor setup to another monitor. This issue can occur because of incorrect cursor input.

Workaround: Set the Horizon Agent DPI setting to 100% scaling.

- With the Session Collaboration feature, if a session owner grants control to a collaborator, and the collaborator experiences connection loss and network recovery while the session owner is attempting to regain control of the session, both the session owner and collaborator might have input control of the session at the same time.

Workaround: Disconnect and reconnect the collaborative session, or toggle the input check box in the Session Collaboration user interface.

- When you set a timeout value for HKLM\Software\VMware, Inc.\VMware VDM\Agent\USB\UemTimeouts, it fails to take effect.

Workaround: Reboot the Agent VM.

- The HTML5 Multimedia Redirection feature cannot redirect HTML multimedia content from <http://huffingtonpost.com>. The HTML5 Multimedia Redirection feature can redirect HTML5 multimedia content from <http://www.yahoo.com>, but you might see a "Page Unresponsive" message.

Workaround: None.

- If you set URL Content Redirection rules to `.*.acme.com`, all URLs that include `acme.com` are redirected, but the URLs `.acme.com` and `acme.com` are not redirected.

Workaround: To redirect the URLs `acme.com` and `.acme.com`, set the URL Content Redirection rule to `acme.com`, not `.*.acme.com`.

- If a session owner is watching a video that has been accelerated using MMR during a collaboration session, the collaborators see a black screen instead of the video.

Workaround: As a session owner, if you need to play a video during a collaboration session, do not use Windows Media Player or Internet Explorer to play the video, or disable MMR on pools where collaboration is enabled.

- If a collaborator joins a multimonitor session and enables relative mouse mode on their client, it is possible for the mouse to move to a secondary monitor that the collaborator cannot see.

Workaround: Move the mouse back on to the screen. Alternatively, don't use relative mouse mode in a multimonitor session.

- If you use Chrome with URL Content Redirection, and you set `.*.google.*` for the https protocol in filtering rules and you set Google as your home page in Chrome, redirection to `google.com` occurs each time you open a new tab.

Workaround: Change the home page or the filtering rules.

- When setting up a collaborative session, adding a collaborator by the email address from a two-way trusted domain fails.

Workaround: Add the collaborator by using `domain\user`.

- If you include the URL of a Microsoft Edge trusted site in the list of websites in the **Enable URL list for VMware HTML5 Multimedia Redirection** group policy setting, HTML5 Multimedia Redirection does not work for that URL. To view trusted sites, select **Internet options**, click the **Security** tab, click **Trusted sites**, and click **Sites**.

Workaround: Run the command `CheckNetIsolation LoopbackExempt -a -n="Microsoft.MicrosoftEdge_8wekyb3d8bbwe"`, which makes the host less secure.

- With the Microsoft Edge browser, the HTML5 Multimedia Redirection feature cannot redirect HTML multimedia content from websites that use the m3u8 video format, such as `ted.com`.

Workaround: Use the Chrome browser.

- With the HTML5 Multimedia Redirection feature, if a user plays an HTML5 video that uses a static video URL in a remote desktop, their client machine does not have access to the static URL and the playback falls back to the remote desktop.

Workaround: None. This issue is a network limitation.

- With the HTML5 Multimedia Redirection feature, when the Scanner Redirection setup option is enabled in Horizon Agent in a remote desktop, the VMware Horizon HTML5 Redirection Extension for Edge extension sometimes crashes after the Microsoft Edge browser is launched in the remote desktop. This issue typically occurs in large-monitor environments and under stress.

Workaround: Close the launched Microsoft Edge browser and launch the Microsoft Edge browser again.

- HTML5 Multimedia Redirection works for Edge in a pre-1803 Windows 10 virtual desktop, but after updating to the latest Windows 10 1803 version, such as 17133, redirection does not work, particularly for websites that use autoplay, such as youtube.com.

Workaround: Force restart the Windows 10 virtual desktop.

- When you connect to Horizon Client using a Unified Access Gateway appliance and configure the appliance using a non-English locale or an arbitrary name such as "UAG 2" instead of the machine's FQDN, then the field does not map to a URL. During a session collaboration, the generated URI invite has the wrong hostname.

Workaround: When you configure the Unified Access Gateway name, use English and FQDN.

- If you installed Scanner Redirection as a default selection on a Windows 10 1709 agent and vCPU is greater than 1, after each login, several dmp files such as backgroundTaskHost.exe, ctfmon.exe, RuntimeBroker.exe, are generated in %LocalAppData%/CrashDumps.

Workaround: Delete the dmp files from the CrashDumps directory.

- Published applications do not get disconnected when the client session is idle, even when Idle Session Timeout is set with MaxIdleTime using the GPO or non-GPO method. A disconnect warning message appears, but the application is not disconnected.

Horizon GPO Bundle

- Computer-based global policy objects (GPOs) that require a reboot to take effect are not applied on instant clones.

Workaround: See the VMware Knowledge Base (KB) article, [2150495](#).

- Setting the size of the retry port range to 0 when configuring the "Configure the TCP port to which PCoIP Server binds and listens" or "Configure the UDP port to which PCoIP Server binds and listens" group policy causes a connection failure when users log in to the desktop with the PCoIP display protocol. Horizon Client returns the error message The Display protocol for this desktop is currently not available. Please contact your system administrator. The help text for the group policies incorrectly states that the port range is 0 through 10.

Note: On RDS hosts, the default base TCP and UDP port is 4173. When PCoIP is used

with RDS hosts, a separate PCoIP port is used for each user connection. The default port range that is set by the Remote Desktop Service is large enough to accommodate the expected maximum of concurrent user connections.

Workaround:

- **PCoIP on single-user machines:** Set the retry port range to a value between 1 and 10. (The correct port range is 1 through 10.)
- **PCoIP on RDS hosts:** As a best practice, do not use these policy settings to change the default port range on RDS hosts, or change the TCP or UDP port value from the default of 4173. Do not set the TCP or UDP port value to 4172. Resetting this value to 4172 will adversely affect PCoIP performance in RDS sessions.
- For Windows 2008 R2 SP1 desktop pools hosted on an RDS host, the language sync setting (from client to guest) is turned on by default and cannot be turned off. Therefore, disabling the group policy "Turn on PCoIP user default input language synchronization" for Horizon Agent has no effect. The remote desktop language always synchronizes with the language used on the client system.

Workaround: None.

- A GSSAPI_ERROR message appears when you initially login with username and password and try to recursively unlock using smart card authentication to login to a local machine that has the group policy setting "Unlock remote sessions when the client machine is unlocked" enabled, and then Log In As Current User from Horizon Client.

Workaround: Disable Log In As Current User from Horizon Client and manually unlock the virtual desktop using the username and password.

- The "Bandwidth limit" group policy setting does not take effect. The value you enter in the setting is ignored, and the existing bandwidth is used for serial port redirection. The bandwidth consumption depends on the number of concurrently used serial port devices and the baud rate used by each device.

Workaround: None.

- In a nested mode configuration where the first-level desktop (the machine where Horizon Client and Horizon Agent are installed) is a virtual desktop and the second-level desktop is a published desktop, the "Specify a filter in redirecting client printers" group policy setting does not affect the second-level desktop if you configure it in the first-level virtual desktop.

Workaround: If you want to filter printers for the second-level desktop, configure the "Specify a filter in redirecting client printers" group policy in the second-level desktop.

Horizon Client

This section describes problems that end users might encounter when using Horizon Client or HTML Access to connect to remote desktops and applications. For problems that occur only in a specific Horizon Client platform, see the Horizon Client release notes on the [Horizon Clients Documentation page](#).

- If you use Horizon Client 3.5.x or earlier for Linux, Mac OS X, or Windows with USB auto-connection enabled, and you connect to a remote desktop for which USB redirection has been disabled with Smart Policies, USB devices attached to the client system disappear from the client system.

Workaround: Upgrade to Horizon Client 4.0 or later, or implement one of the workarounds described in VMware Knowledge Base (KB) article 2144334, [USB devices on your local](#)

[system disappear when you connect to a remote desktop with Horizon Client 3.5.x or earlier.](#)

- When multiple connections are made consecutively to a single RDS host, a few users (for example, one or two of 120 users) might not be able to start or restart RDS desktop sessions.

Workaround: Increase the number of vCPUs and the RAM size on the RDS host.

- The first connection to an RDS desktop or application fails if it has been more than 120 days since the RDS role was configured on the RDS host, and no previous connection was made. This issue also occurs with RDP.

Workaround: Wait a few seconds and connect to the RDS desktop or application again.

- Persistent settings for location-based printers are not supported if the settings are saved in the printer driver's private space and not in the DEVMODE extended part of the printer driver, as recommended by Microsoft.

Workaround: Use printers that have the user preference settings saved in the DEVMODE part of the printer driver.

- In a desktop session running on a Windows Server 2008 R2 SP1 RDS host, you cannot play back an H.264 video file, or playback AAC audio with a video file, in Windows Media Player. This is a known third-party issue.

Workaround: Go to the [Microsoft KB article 2483177](#) and download the Desktop Experience Decoder Update for Windows Server 2008 R2 package.

- When you play a YouTube video in a Chrome browser in a desktop session running on a Windows Server 2012 R2 RDS host, the video display can be corrupted. For example, black boxes might pop up in the browser window. This issue does not occur on any other browser or on Windows Server 2008 R2 SP1 RDS hosts.

Workaround: In your Chrome browser, select **Chrome > Settings > Show advanced settings > System**, and deselect **Use hardware acceleration when available**.

- If you play a video in a desktop running on a Windows 2008 R2 SP1 physical RDS host, and you move the video display from the main monitor to another monitor, the video stops playing or the visual frames stop updating (although the audio might continue to play). This issue does not occur on a virtual machine RDS host or in a single monitor configuration, and it only occurs on Windows Server 2008 R2 SP1.

Workaround: Play videos on the main monitor only, or configure your RDS desktop pool on a virtual machine RDS host.

- If you launch a remote application that becomes unresponsive and then launch another application, the second application's icon is not added to the task bar on the client device.

Workaround: Wait for the first application to become responsive. (For example, an application might be unresponsive while large files are being loaded.) If the first application continues to be unresponsive, terminate the application process on the RDS virtual machine.

- The application Lync 2013 that does not have the February, 2013 update and is hosted on an RDS host running Windows Server 2012 R2 will crash shortly after launch with the error message "Microsoft Lync has stopped working." This is a known issue with Lync 2013.

Workaround: Apply the February, 2013 update of Lync. The update is available at [Microsoft KB article 2812461](#).

- For RDS host farms that are created with VMware Blast display protocol support, enabling the UDP network protocol for VMware Blast sessions reduces Blast Secure Gateway scale and sessions might fall back to the TCP network protocol.

Workaround: Do not enable the UDP network protocol for VMware Blast sessions on RDS

hosts.

- Customized application icons with the .ico file extension do not appear on the Shortcut and Start Menu on a Windows desktop.
Workaround: Use the .png file extension when you save the customized application icon.
- Customized application icons with the .ico file extension do not display correctly in Horizon Client on an Android device.
Workaround: Do not use the .ico file extension when you save the customized application icon.
- The profile data is missing for multiple user sessions on RDS hosts. This issue occurs when the sessions are in the disconnected state but the task manager on the RDS host still shows these sessions.
Workaround: Delete the sessions from the RDS host or log the user off from the published desktop or application.
- When you log in to Workspace ONE, the pre-launch application session is not triggered. Pre-launch sessions are triggered only when there is a successful login to Connection Server from Horizon Client.
Workaround: Manually start an application or desktop from Workspace ONE to trigger the applications enabled for pre-launch to be started.
- Horizon Client cannot connect to a Connection Server instance if the server name or fully qualified domain name (FQDN) for the Connection Server instance contains non-ASCII characters.
Workaround: None.
- On remote desktops that connect using PCoIP and are configured with multiple monitors, if a user plays a slide show in Microsoft PowerPoint 2010 or 2007, specifies a resolution, and plays the slides on the second monitor, part of each slide appears on each monitor.
Workaround: On the client system, resize the screen resolution on the second monitor to the desired resolution. Return to the remote desktop and start the slide show on the second monitor.
- On remote desktops that connect using PCoIP, if users play slides in Microsoft PowerPoint 2010 or 2007 and specify a resolution, the slides are played at that chosen resolution and are not scaled to the current resolution.
Workaround: Choose "Use current resolution" as the playback resolution.
- When you play videos in Windows Media Player on a desktop, PCoIP disconnections might occur under certain circumstances.
Workaround: On the remote desktop, open the Windows registry and navigate to the HKLM\Software\Wow6432Node\Policies\Teradici\PCoIP\pcoip_admin_defaults registry key for 64-bit Windows or the HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin_defaults registry key for 32-bit Windows. Add the pcoip.enable_tera2800DWORD registry value and set the value to 1.
- Copying and pasting an image from a remote desktop to the client system, or from the client system to a remote desktop, can fail because the clipboard memory size is not large enough to accommodate the image, even though the configured clipboard memory size is greater than or the same as the size of the image on disk. This problem occurs because the image size on disk is less than the image size in clipboard memory. For example, the size of the image in the clipboard memory can be two to three times size of the image on disk.
Workaround: Increase the clipboard memory size until it can accommodate the image.
- Using the VMware Blast display protocol and with Blast Secure Gateway (BSG) disabled,

Horizon Client sometimes cannot recover from a brief (about 1 minute) network outage and the connection to the desktop is disconnected. This issue does not occur when BSG is enabled.

Workaround: Reconnect the session.

- After a brief network outage and the VMware Blast session between Horizon Client and a remote desktop has recovered or has been reconnected, certain features might stop working, such as:
 - Smart card
 - Client Drive Redirection (CDR) and File Association
 - Multimedia Redirection (MMR)
 - Lync/Skype for Business

Workaround: Disconnect and reconnect the session.

- Sometimes, when using Lync VDI to make a video call, the local image is not displayed.

Workaround: Update Microsoft Lync VDI to the latest version.

- If a user connects to an F5 server to access a remote desktop, and the F5 server is configured to use an RSA server, the user must input an RSA username and passcode. If the RSA user's PIN is not set, Horizon Client might fail to submit the passcode for the user. This problem is an F5 limitation.

Workaround: Users must contact their RSA administrator to set their PINs before using their PINs in an F5 and RSA setup.

- Data transfer is slow when copying and pasting text and images between Horizon Client and a remote desktop.

Workaround: Reduce the effective clipboard size so that less data is transferred at one time.

- The first time a user connects to a remote desktop or application on a Workspace ONE mode-enabled server, Horizon Client caches the Workspace ONE hostname on the client. From then on, Horizon Client always redirects to the Workspace ONE portal for that server. If the Workspace ONE server goes down, or if the Workspace ONE mode is changed or disabled, Horizon Client cannot connect to the server again because it always redirects to the Workspace ONE portal.

Workaround: Remove the Connection Server instance from server selector in Horizon Client, or use HTML Access to connect to the remote desktop or application.

- Skype for Business VDI optimized solution is not compatible for inter-operability with Lync 2010 clients.
- The RDS host stores only one set of application data for the first application launch of a session. Any subsequent application launch data is lost.

Workaround: Log off the session and launch another application to store that data.

- Desktops fail to start when you use HTML Access from Internet Explorer or Microsoft Edge Web browsers to connect to Connection Server, security server, or replica server on a Windows 10 client operating system. This issue affects desktops with Windows 10 N, Windows 10 KN, Windows 7 N and Windows 7 KN guest operating systems.

Workaround: Use Firefox or Google Chrome Web browsers for HTML Access.

- Sometimes after a call ends, you might see a message:
Skype for Business has stopped working.

Workaround: Apply Skype for Business updates. See <https://support.microsoft.com/en-us/help/3158521/lync--skype-for-business--or-outlook-2016-or-2013-crash> for details.

- Changing the ringer volume level in audio settings of Skype for Business (in optimized mode) does not change the ringing volume when receiving a call in Windows, Mac, and Linux Horizon Clients.

Workaround: When you receive a call, manually change the volume of the output device or speaker connected to the Horizon Client to change the output volume.

- If you switch browser tabs while playing a redirected video in Internet Explorer, part of the video window continues to be displayed behind or next to the browser window. This issue only occurs on Windows 7 desktops.

Workaround: Use Windows 8.1 desktops. Alternatively, do not switch to another tab while a redirected video is playing.

- An action script error occurs when you play a YouTube Flash video on a remote desktop that has Flash MMR enabled.

Workaround:

- Option 1. Open the script support for the YouTube Web site and add appMode=1 with the URL of the YouTube site to the Url WhiteList.
 - Option 2. Open Internet Explorer > Tools > Internet Options > General. Under “Browsing history” click the “Settings” button. In the next window, click the “View files” button. Delete all files from the INet Cache folder.
- When you play a flash video in a Windows 10 agent, Flash Redirection does not work.
- For Intel vDGA, multiple-monitor support is limited to no more than 3 monitors. The Intel driver supports only up to 3 monitors with a resolution of up to 3840 X 2160. If you try to connect with 4 monitors, the connection shows 3 black screens with just one screen working.
- When 4K monitors are configured on machines where 3D Rendering and vSGA are enabled, moving, resizing, or toggling the Windows Media Player window to full screen mode can be very slow. This issue does not occur with 2D, software 3D Rendering, or monitors with 2560x1440 resolution.

Workaround: None

- On Windows 8/8.1 desktops, 3D screen savers operate even when the 3D Renderer setting is disabled, and the screen savers do not render correctly. This issue does not occur on Windows 7 desktops.

Workaround: Make sure your end users do not use 3D screen savers, or enable the 3D Renderer setting for the desktop pool.

- With NVIDIA M60 GPU and driver version 361.89 or 361.94, users might see a blur red screen when they first connect to the Windows desktop, or when they right click on the desktop and then select **NVIDIA Control Panel > System Information**.

Workaround: Changing the resolution of the display or changing to full-screen mode fixes the problem and you can revert to the original resolution or screen mode. The problem disappears after the first time it occurs. Also, the problem does not occur with NVIDIA driver 361.51.

- Using a smart card to log in to an RDS desktop takes longer than with a virtual, single-user desktop. This issue is less acute on Windows clients than other clients.

Workaround: None.

- On Windows 7 client machines, Horizon Client exits when the smart card removal policy is triggered.
- If a VDI desktop is in a remote location and experiencing high network latency, then a recursive unlock using smart card authentication might not work.

Workaround: Unlock the desktop manually.

- If you change the default HTTPS port, 443, on a Connection Server instance or security server, and users try to start their desktops from the Horizon User Portal, the desktops fail to launch. This issue occurs when users attempt to access their desktops via Horizon Workspace with either Horizon Client or HTML Access.

Workaround: Keep the default HTTPS port 443.

- When you add a SAML Authenticator in Horizon Administrator, an "Invalid certificate detected" window might be displayed, even when the Metadata URL points to a trusted certificate in the Trusted Root Certificate Authorities folder in the Windows certificate store. This issue can occur when an existing SAML Authenticator with a self-signed certificate was using the same Metadata URL when the trusted certificate was added to the Windows certificate store.

Workaround:

1. Remove any trusted certificates for the Metadata URL from the Trusted Root Certificate Authorities folder in the Windows certificate store.
2. Remove the SAML Authenticator with the self-signed certificate.
3. Add the trusted certificate for the Metadata URL to the Trusted Root Certificate Authorities folder in the Windows certificate store.
4. Add the SAML Authenticator again.

- You cannot connect to a Windows Server 2008 R2 SP1 desktop, or you encounter a black screen the first time that you use Horizon Client, even though the desktop that you are connecting to is in the Available state.

Workaround: Shut down and power on the Windows Server 2008 R2 SP1 virtual machine. When the desktop is in the Available state, try to connect again. Resetting or restarting the virtual machine does not solve this problem. You must shut down the virtual machine first and then power it back on.

- On some occasions, when you reconnect to a Windows 8.x desktop session, you might not see the desktop display immediately. A black screen might be displayed for up to 20 seconds.

Workaround: None

- Adobe Flash optimization settings that use high quality and aggressive throttling are not fully enabled when end users use Internet Explorer 10 or Internet Explorer 11 on Windows 8 or Windows 8.1 desktops.

Workaround: None.

- If a user of a Windows 8 remote desktop logs in using Kerberos authentication, and the desktop is locked, the user account for unlocking the desktop that Windows 8 shows the user by default is the related Windows Active Directory account, not the original account from the Kerberos domain. The user does not see the account he or she logged in with. This is a Windows 8 issue, not directly a Horizon 7 issue. This issue could, but does not usually, occur in Windows 7.

Workaround: The user must unlock the desktop by selecting "Other user." Windows then shows the correct Kerberos domain and the user can log in using the Kerberos identity.

- Windows Media Player is not active and cannot be made visible when the Windows 10 remote desktop display is resized to one monitor and Windows Media Player is open on another monitor. This problem occurs regardless of whether the video is playing or not and whether MMR is enabled or not.
Workaround: Close and reopen Windows Media Player or resize the remote desktop to multi-monitor display.
- Microsoft Windows Fax and Scan does not work with Scanner Redirection on Windows 10 desktops.
Workaround: Use another scan application on Windows 10 desktops or change to another desktop platform.
- Sometimes the scanner settings do not take effect on WIA scanners. For example, if you select gray scale mode and select a partial area of the original image, the scanner might use color and scan the whole image.
Workaround: Use a TWAIN scanner.
- In some environments, if you switch to a different WIA scanner, the images might continue to be scanned from the original scanner.
Workaround: Log off the remote desktop session. Launch a new desktop session and perform the scan using the selected scanner.
- When you use the Ambir Image Scan Pro 490i to perform a scan on a remote desktop or application, the dialog box always displays "Scanning..." and does not complete.
Workaround: Perform a scan on the client. The client scan calibrates the scanner. After the calibrate operation is finished, run the scan within the remote desktop or application.
- When you use the TOPAZ signature pad for multiple remote desktop sessions on Windows Server 2012 remote desktops, you might get only one device for a session that is redirected successfully. This problem can occur because the TOPAZ signature pads have the same serial number.
Workaround: Use TOPAZ signature pad devices with different serial numbers. You can use the serial number modifier software provided by the TOPAZ manufacturer to modify the serial numbers.
- Unicode keyboard input does not work correctly with HTML Access in Horizon 7 for Linux Desktops.
- When you connect to a Linux desktop, some keyboard inputs do not work. For example, if you are using a non-English IME on both the client device and the remote desktop, some non-English keys are not displayed correctly.
Workaround: Set the English IME on the client device and set the non-English IME on the remote desktop.
- Sometimes an audio call does not start correctly from Skype to Skype for Business. The call status is "Connecting call..." on the Skype for Business client.
Workaround: None.
- If you use Skype for Business inside a non-persistent desktop, you might reach the Skype for Business limit of 16 device certificates. When this limit is reached and Skype for Business attempts a new logon, a new certificate will be issued and the oldest assigned certificate will be revoked.
- Microsoft Skype for Business 2016 Client displays a black screen instead of the shared desktop when a second user shares a desktop. The first user sees a black screen and an

error message: Someone else started presenting, which ended your presentation.

Workaround: None.

- If a user starts a Co-Author Office session in Office 365 during a Skype for Business video call, Microsoft Skype for Business 2016 Client displays a black screen instead of the second user's video display.

Workaround: None.

- The information that appears in the Pen and touch section of system information for a Windows 10 remote desktop is different when you use Horizon Client for Windows versus Horizon Client for Windows 10 UWP. When you connect with Horizon Client for Windows, the correct information is displayed. When you connect with Horizon Client for Windows 10 UWP, no information is displayed in the Pen and touch section.

Workaround: None.

- If you connect to a remote desktop with the RDP protocol, disconnect (but do not log off) from the remote desktop, and then reconnect to the same desktop with the VMware Blast or PCoIP display protocol, the client drive redirection feature does not work properly. A folder is redirected only as \\tsclient, and a network drive is not created.

Workaround: Log off from the remote desktop and reconnect.

Horizon JMP Server and JMP Integrated Workflow

- In an environment where multiple JMP servers are installed, conflicts might occur when creating or deleting JMP assignments if more than one JMP server refers to the same User Environment Manager configuration share.

Workaround: None.

- If you configured your JMP settings to use only one VMware App Volumes Manager and if during a JMP assignment creation you selected a desktop pool whose Horizon Agent is not pointing to that configured App Volumes Manager, you can still select AppStacks from the App Volumes Manager instance that is pointed to by the desktop pool's Horizon Agent. Also, if you configured your JMP Settings to use multiple App Volumes Manager instances, even if you select a desktop pool whose Horizon Agent points to one of those App Volumes Manager instances, you can still select the AppStacks from the other App Volumes Manager instances configured in your JMP settings. However, when the desktop pool is launched, the AppStacks selected from that other App Volumes Manager are unavailable.

Workaround: None.

- If an AppStack that is currently used by an existing JMP assignment is renamed using the App Volumes Manager or by editing the JMP assignment, the summary page of existing JMP assignments does not get updated with the new AppStack name.

Workaround: None.

- If you have two Horizon 7 instances that are registered with the same JMP Server instance

and use the same App Volumes Manager, deleting a JMP assignment from one Horizon 7 instance can delete the AppStacks assignments used by another JMP assignment in the other Horizon 7 instance.

Workaround: None.

- When adding or editing Active Directory information in the JMP Settings page, the operation fails if the value entered for **Bind User Name** contains one or more of a range of 30 triple-byte Chinese characters, such as the ' ' character, that cause the Active Directory authentication to fail.

Workaround: Use another bind user name from your Active Directory that has administrative privileges and does not contain any of the 30 triple-byte Chinese characters, such as the ' ' character.

- When adding or editing App Volumes Manager instance information in the JMP Settings page, the operation fails if the value entered for **Service Account User Name** contains one or more of a range of 30 triple-byte Chinese characters, such as the ' ' character, that causes the App Volumes Manager instance authentication to fail.

Workaround: Use another bind user name from your App Volumes Manager instance that has administrative privileges and does not contain any of the 30 triple-byte Chinese characters, such as the ' ' character.

- The Drive Mapping settings that were mapped using VMware User Environment Manager version 9.2.1 are not visible when Windows 10 1703 desktop pool is launched.

Workaround: After the Windows 10 1703 desktop pool is launched, execute the following command.

```
C:\Program Files\Immidio\Flex Profiles\FlexEngine.exe -UemRefreshDrives
```

See the VMware Knowledge Base (KB) article <https://kb.vmware.com/s/article/2113657> for additional information.

- If you access Horizon Console using localhost, the error message "JMP server is not reachable at the moment." is displayed on the JMP Settings pane of Horizon Console.

Workaround: Access Horizon Console using a fully qualified domain name (FQDN) only, instead of using localhost.

- While creating a new JMP assignment, the following warning message might appear in the **Applications** tab: "The App Volumes instance associated with the selected desktop pool does not match any of the registered App Volumes instances." This issue occurs when one of the following is true:
 - The App Volumes Agent used in the desktop pool was installed using an IP address instead of a fully qualified domain name (FQDN)
 - The App Volumes Agent used in the desktop pool was installed using an FQDN, but the App Volumes Manager instance's IP address was registered in the JMP settings instead.

Workaround: Re-install the App Volumes Agent using an FQDN and use the FQDN when

registering the App Volumes Manager instance in the **Settings (JMP) > App Volumes** tab.

- While installing VMware Horizon JMP Server, the JMP Server installer failed to continue because McAfee Antivirus detected NSSM.EXE as a threat.

Workaround: Add the following files to the McAfee Antivirus exclusion list before you reinstall JMP Server.

C:\Program Files (x86)\VMware\JMP\nssm-2.24\nssm-2.24\win32\nssm.exe

C:\Program Files (x86)\VMware\JMP\com\xmp\node_modules\winser\bin\nssm.exe

- If you selected the **Authorize the local Administrator group** option during the Horizon 7 Connection Server installation, which creates a BUILTIN\Administrators group instead of *<domainName>\Administrator*, adding the JMP Server information using Horizon Console fails with the error message "Insufficient Horizon Privileges".

Workaround: Using Horizon Administrator, register *<domainName>/administrator* with full administrator access. Log back in to Horizon Console and add the JMP Server information.

- While you are creating a JMP assignment and you hover over an instant-clone desktop pool, the value shown for the 3D Renderer option is **Disabled** instead of **Manage using vSphere Client**.

Workaround: None.

- JMP Server registration fails when the scope of the trust authentication setting is set to "Selective Authentication."

Workaround: Use one of the following workarounds to resolve this issue.

- Use domain-wide authentication.
- Continue to use the "Selective Authentication" security setting, but explicitly grant each Horizon Connection Server host (local system) accounts the "Allowed to Authenticate" permission on all the domain controllers of the computer objects (resource computers) that reside in the trusting domain or forest. For information on how to grant the "Allowed to Authenticate" permission, see the Microsoft article [Grant the Allowed to Authenticate permission on computers in the trusting domain or forest](#).
- The JMP login API, xmp\jmp\login, throws an insufficient Horizon privileges exception when you tried to register your JMP Server instance in Horizon Console, even though the user account you used to log in to Horizon Console belongs to an Active Directory (AD) security or distribution group, and the **View Configuration > Administrators** pane in Horizon Administrator shows that the AD security group has Administrators permissions.

Workaround: In Horizon Administrator, select **View Configuration > Administrators** to add the administrator user account you want to use to register your JMP Server instance. Assign that administrator user account with Administrators permissions. For more information, see "Managing Administrators" in the *Horizon 7 Administration* document. Once the administrator user account has been added successfully, you can register your JMP Server instance using Horizon Console.

- JMP assignments do not work as expected because information about the App Volume

Manager used by the desktop pool and the User Environment Manager version used by JMP Server could not be determined.

Workaround: When configuring a desktop pool, set the **Number of spare (powered on) machines** value to 1 or more in the Desktop Pool Sizing section of the Provisioning Settings pane. In addition, if you selected the **Provision machines on demand** option in the Provisioning Timing section, set the **Min number of machines** value to 1 or more.

- When the JMP Server version 1.0.2.x installer file is run on a host that currently has JMP Server version 1.0.0.516 installed, the installation process does not proceed.

Workaround: Use the Control Panel to uninstall JMP Server version 1.0.0.516. Run the installation file for JMP Server version 1.0.2.x and follow the wizard to complete the installation. Provide the same SQL Server database information during the installation process to preserve any data you had with the JMP Server version 1.0.0.516 installation.