



# Release Notes for VMware Horizon 6 version 6.2.8

Released 14 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](#)
- [Prior Releases of View](#)
- [Resolved Issues](#)
- [Known Issues](#)

## What's New in This Release

- VMware Horizon 6 version 6.2.8 is a maintenance release that contains new user authentication security improvements that resolve CVE-2019-5513 which is documented in [VMSA-2019-0003](#).

## Before You Begin

- **Important note about installing VMware View Composer**  
If you plan to install or upgrade to View Composer 6.2.8, 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)**.
- The Horizon 6 release includes new configuration requirements that differ from past releases. Read the [Readme](#) document. This short overview can help you to avoid potential pitfalls when you install or upgrade to this release. The *View Upgrades* document provides upgrade instructions.
- If you intend to upgrade a pre-6.2 installation of View, 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 6 features such as Virtual SAN 6.1, GRID vGPU, and Virtual Volumes, install vSphere 6.0 and subsequent patch releases.
- If your deployment uses RDS Per Device Client Access Licenses (CALs), follow the configuration guidelines in KB 2076660, [Managing RDS Per Device CALs in View](#), before your end users begin connecting to RDS desktops and applications.
- When you upgrade to this release, upgrade all View Connection Server instances in a pod before you begin upgrading View Agent, as described in the *View Upgrades* document.
- The download page in this release includes a Horizon View 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* guide.
- Selecting the Scanner Redirection setup option with View 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 View Agent.) For the particular users who need the Scanner Redirection feature, configure a separate desktop pool and select the setup option only in that pool.

- The Modify option has been removed from the View Agent installer version included in this release. To change custom setup options after you install this version of View Agent, you must uninstall and reinstall View Agent. For patches and upgrades, you can run the new View Agent installer and select a new set of options without uninstalling the previous version.
- FIPS mode requires the use of TLS 1.2. If you install View in FIPS mode, you will not be able to connect to vSphere 5.x, which does not support TLS 1.2.
- FIPS mode is not supported on releases earlier than 6.2. If you enable FIPS mode in Windows and upgrade View Composer or View Agent from a release earlier than 6.2 to 6.2.7, the FIPS mode option is not shown. You must do a fresh install instead to install View 6.2.7 in FIPS mode.
- For Linux desktops, the port that is used for the Blast protocol is 22443 in this release. In Horizon View 6.1.1 and earlier, the port was 5443.

[Top of Page](#)

## Internationalization

The View Administrator user interface, View Administrator online help, and Horizon 6 product

documentation are available in Japanese, French, German, simplified Chinese, traditional Chinese, and Korean. For the documentation, see the [Documentation for VMware Horizon 6](#).

[Top of Page](#)

## Compatibility Notes

- For the supported guest operating systems for View Agent on single-user machines and RDS hosts, see [Supported Operating Systems for View Agent](#) in the *View Installation* document.
- If you use Horizon 6.2.7 servers with an older version of View Agent, such as View Agent 6.1.x, and if the PCoIP Secure Gateway is enabled (in View Administrator), you will need to enable TLS 1.0 for PCoIP connections on the servers. View Agent versions that are older than 6.2 support the security protocol TLS 1.0 only. Horizon 6.2.7 servers, including connection servers and security servers, have TLS 1.0 disabled by default for PCoIP connections. You can enable TLS 1.0 for PCoIP connections on these servers by following the instructions in KB 2130798, [Configure security protocols for PCoIP for Horizon 6 version 6.2 and later, and Horizon Client 3.5 and later](#).
- By default, TLS 1.1 and TLS 1.2 are enabled in View components. TLS 1.0 is enabled for outgoing connections to support vSphere 5.x, but it is disabled for incoming connections. If the vSphere version is 6.x, or 5.5 U4 or later, VMware recommends that TLS 1.0 be disabled for outgoing connections, see [Configuring Security Protocols and Cipher Suites on a View Connection Server Instance or on a Security Server](#) in the *View Security* document.
- If you use Horizon clients that do not have TLS 1.2 enabled, you can enable TLS 1.2, see [Configuring Security Protocols and Cipher Suites](#) in the *Horizon Client and Agent Security* document. If you cannot easily upgrade or reconfigure clients, you can re-enable TLS 1.0 for incoming connections to a View Connection Server or security server, see [Configuring Security Protocols and Cipher Suites on a View Connection Server Instance or on a Security Server](#) in the *View Security* document.
- RC4 and SSLv3 are disabled by default in View components, in accordance with RFC 7465, "Prohibiting RC4 Cipher Suites," and RFC 7568, "Deprecating Secure Sockets Layer Version 3.0." If you need to re-enable RC4 or SSLv3, on View Connection Server, security server, View Composer, or a View Agent machine, see [Older Protocols and Ciphers Disabled in View](#) in the *View Security* document.
- For the supported Linux guest operating systems for View Agent, see [System Requirements for Horizon 6 for Linux](#) in the *Setting Up Horizon 6 for Linux Desktops* document.
- For the supported operating systems for View Connection Server, security server, and View Composer, see [System Requirements for Server Components](#) in the *View Installation* document.
- Horizon 6 functionality is enhanced by an updated set of Horizon Clients provided with this release.  
For example, Horizon Client 3.3 or later is required for IPv6 and USB redirection of storage devices to RDS desktops and Hosted Apps. See the [VMware Horizon Clients Documentation](#) page for information about supported Horizon Clients.
- See the [VMware Product Interoperability Matrix](#) for information about the compatibility of View with current and previous versions of VMware vSphere. For vSphere 5.5 and 5.1, certain minimum express patches are recommended:

- vSphere 5.5 Update 1a with Express Patch 4 or later
  - vSphere 5.1 Update 2 with Express Patch 5 or later
- For the supported Active Directory Domain Services (AD DS) domain functional levels, see [Preparing Active Directory](#) in the *View Installation* document.
- For more system requirements, such as the supported browsers for View Administrator and View Portal, see the *View Installation* 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 View 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 *Setting Up Desktop and Application Pools in View* document.
- The USB Redirection setup option in the View 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 *View Security* document.
- The Global Policy, Multimedia redirection (MMR), defaults to **Deny**. To use MMR, you must open View 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 View Administrator, VMware recommends that the security implications be understood. For guidance, see the KB article, [Security considerations and disallowing inter-Virtual Machine Transparent Page Sharing \(2080735\)](#).
- 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 6 does not support vSphere Flash Read Cache (formerly known as vFlash).
- With the upcoming release of Workspace Portal, the product name will change from Workspace Portal to VMware Identity Manager. The Horizon 6 version 6.2 documents refer to Workspace Portal, but VMware Identity Manager is also supported.
- In Horizon (with View) version 6.0 and later releases, the View PowerCLI cmdlets Get-TerminalServer, Add-TerminalServerPool, and Update-TerminalServerPool have been deprecated.
- Kiosk mode clients are not supported in a Cloud Pod Architecture implementation.
- Native NFS snapshot technology (VAAI) is not supported in pools that are enabled for View Storage Accelerator.

# 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 Agent](#).

## Prior Releases of View

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

## Known Issues

The known issues are grouped as follows.

- [Installation, Upgrade, and Uninstall Operations](#)
- [RDS Desktops and Applications](#)
- [Access Point](#)
- [Configuration and View Administrator](#)
- [Horizon Client and Remote Desktop Experience](#)
- [Horizon 6 for Linux Desktops](#)
- [Windows Media MMR](#)
- [3D Graphics Acceleration](#)
- [Smart Card](#)
- [Client Drive Redirection](#)
- [Scanner Redirection](#)
- [Serial Port Redirection](#)
- [View Persona Management](#)
- [vSphere Platform Support](#)
- [View Composer](#)
- [Windows 10 and Windows 8.x Support](#)
- [Windows Server for Desktop Use](#)
- [Workspace Portal Integration](#)
- [Virtual SAN and Virtual Volumes](#)
- [Cloud Pod Architecture](#)
- [Miscellaneous](#)

### Installation, Upgrade, and Uninstall Operations

- When you upgrade View Agent 6.1.1 to View Agent 6.2.x on an RDS host running on Windows Server 2012 or 2012 R2, the upgrade fails with an "Internal Error 25030" message.  
**Workaround:** Uninstall View Agent 6.1.1, restart the RDS host, and install View Agent 6.2.x.
- The USB HUB device driver might not be installed properly when you install View Agent on a desktop in a manual desktop pool. This issue can occur if, during the View Agent installation, you restart the system before the USB HUB device driver is fully installed.  
**Workaround:** When you install View 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 View 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 View 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:\Program Files\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 View Agent, upgrade the operating system from Windows 8 to Windows 8.1, and then reinstall View Agent. Alternatively, you can perform a fresh installation of Windows 8.1 and then install View Agent.
- 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.
- USB redirection fails in linked-clone images after you upgrade the master image from View Agent 5.1.x or earlier to the current View Agent version. This issue does not occur if you upgrade from View Agent 5.2 or later to the current version.

**Workaround:** See [KB 2062215: USB redirection fails in linked-clone images after you upgrade to View Agent 5.3](#).

- When you run the View 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 View Agent. See [Microsoft KB article 2836988](#).

- When you run any View 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 View 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 View Agent. As a best practice, ensure that all RDS sessions are logged off before you uninstall View Agent.

- During a View 6.2.x View Connection Server Hot Patch deployment, you will see a generic icon instead of the correct VMware icon for VMware Horizon 6 HTML Access in the Programs and Features applet in the Control Panel. This is a cosmetic issue and does not affect the functionality of the HTML Access feature.

**Workaround:** Uninstall earlier version of Connection Server and then install the Hot Patch.

- During the upgrade of View Agent 6.2 to View Agent 6.2.x on an RDS host running Windows Server 2008, you may see a message asking you to close the "VMware Horizon View Agent and Server Manager" application and click Retry to continue. You can safely

ignore this message and click Retry. The upgrade will proceed and be successful.

**Workaround:** Not required.

- When you install View Agent silently, you are unable to install the Flash URL Redirection feature.

**Workaround:** You must include the VDM\_FLASH\_URL\_REDIRECTION=1 property in a silent installation to enable the View Agent installer to install the Flash URL Redirection feature.

For example: VMware-viewagent-x86\_64-6.2.1-3284564.exe /a /s /v"/qn VDM\_VC\_MANAGED\_AGENT=1 VDM\_FLASH\_URL\_REDIRECTION=1

ADDLOCAL=Core,SVIAgent,ThinPrint,USB,HTMLAccess,FlashURLRedirection,RTAV"

- View Composer 6.2.4 fails to install when you use a View Composer database that supports TLS 1.2 as the transport protocol.

**Workaround:** Apply the database client patches that support TLS 1.2 on the machine on which you install View Composer.

- In FIPS mode, the View Agent fails to pair with the View Connection Server and the pool status is not available when the View Agent is installed to a drive other than the C drive.

**Workaround:** When operating in the FIPS mode, install the View Agent on the C drive.

- When you upgrade from Horizon View Agent 6.2.3 to Horizon View Agent 6.2.4 on Windows 7 guest operating systems, the Files in Use dialog appears. The dialog states that the VMware Horizon View Agent application is using files that need to be updated by the setup.

**Workaround:** Click **Ignore** to continue with the upgrade.

- When upgrading from Horizon Agent 6.2.4 to Horizon Agent 6.2.5 on a Windows 10 guest operating system, a "Files in Use" dialog appears. The dialog states that the VMware Horizon View Agent application is using files that need to be updated by the setup.

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

## RDS Desktops and Applications

- 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>.

- 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.

- View Agent cannot install the virtual printing feature on RDS hosts that are physical

machines. Virtual printing is supported on RDS desktops when View Agent is installed on RDS hosts that are virtual machines.

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

- A single client device connecting to RDS desktops and applications over PCoIP can use up more than one RDS Per Device Client Access License (CAL). This issue does not occur if your deployment uses RDS Per User CALs, if the clients connect to View through RDP, or if you deploy only one license server and all your RDS hosts run the same guest operating system.

**Workaround:** Follow the configuration guidelines in KB 2076660, [Managing RDS Per Device CALs in View](#), before your end users begin connecting to RDS desktops and applications.

- In a desktop session running on a Windows Server 2008 R2 SP1 RDS host, you cannot play back an H.264 video file, or play back 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 taskbar 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](#).

## Access Point

- In Access Point 2.0, smart card authentication is a Tech Preview feature, meaning that you can use smart card authentication in a test environment but not in a production environment, and technical support is not available for this Tech Preview feature. If you use smart card authentication, smart cards are required. Setting smart cards to be optional does not work.
- If Access Point is configured to use smart card authentication and you also set an idle

session timeout for View Connection Server, then after the idle session timeout period elapses, you can no longer log in again. For example, if the idle session timeout is set to 3 minutes and you leave the session idle for more than 3 minutes, when the session timeout dialog box appears and you click "Continue," you are prompted to enter Active Directory credentials rather than a smart card PIN. Even if you enter AD credentials, the status displays "Authenticating ..." and freezes.

**Workaround:** If you plan to use smart card authentication, do not configure an idle session timeout.

- Smart card authentication does not work if you use View Administrator to configure a pre-login message. If a pre-login message is configured in View Administrator, when you log in using smart card authentication and you are prompted to confirm the pre-login message, after you confirm the message, the pre-login message reappears.

**Workaround:** If you plan to use smart card authentication, do not configure a pre-login message.

- When you use the Access Point REST administration API, you cannot use the "/v1/config/settings" resource to update authentication settings.

**Workaround:** Use the resource for the specific authentication method, such as "/v1/config/authmethod/certificate-auth".

- When deploying the Access Point appliance, either by using the command-line VMware OVF Tool or by using the deployment wizard, you must enter only one DNS address. If you enter multiple addresses, DNS resolution will not work.
- If you set the View Edge Setting "blastEnabled" to False, you will not be able to access remote desktops and applications through HTML Access. Generally, because Access Point is deployed in a DMZ, the "blastEnabled" option is set to True, and this issue does not occur.

**Workaround:** If you want to set "blastEnabled" to False and also use HTML Access, you must also set the "proxyPattern" option to "/\*portal(.\*)".

## Configuration and View Administrator

- When using View 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 VMware View Blast Secure Gateway (absg.log) log level on a View 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 View 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.

- The View PCoIP ADM (pcoip.adm) group policy setting, **Configure SSL connections to satisfy Security Tools**, is not supported in this release of View. If you attempt to implement certain options in this group policy setting, unexpected results might occur in your View deployment.

**Workaround:** Do not use this setting in this release of View.

- 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. Most important, do not set the TCP or UDP port value to 4172. Resetting this value to 4172 will adversely affect PCoIP performance in RDS sessions.

- On rare occasions, the system health status of Event Database may be displayed as red on the View 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 of time.

**Workaround:** None.

## Horizon Client and Remote Desktop Experience

- If a Linux client 2.3.4 connects to a Horizon 6.0.1 View Agent, and the status of the remote desktop is "available" (not "disconnected"), clipboard redirection between the desktop and client device does not work. This issue occurs even when the View PCoIP General Session Variable group policy setting, Configure clipboard redirection, is set to Enabled in both directions.  
**Workaround:** Disconnect and reconnect to the desktop, or upgrade the Linux client to version 3.1.

- Horizon clients cannot connect to View Connection Server if the server name or fully qualified domain name (FQDN) for View Connection Server contains non-ASCII characters.  
**Workaround:** None.

- On 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 host client system, resize the screen resolution on the second monitor to the desired resolution. Return to the View desktop and start the slide show on the second monitor.

- On 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.

- The virtual printing feature is supported only when you install it from View Agent. It is not supported if you install it with VMware Tools.
- When you play videos in Windows Media Player on a desktop, PCoIP disconnections might occur under certain circumstances.

**Workaround:** On the 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\_tera2800 DWORD registry value and set the value to 1.

- 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.

## Horizon 6 for Linux Desktops

- If you disconnect from a Linux desktop before the guest operating system has completed the log-in process, View Agent for Linux waits at least five minutes before logging off, even if the desktop pool setting, **Automatically logoff after disconnect**, is set to **Immediately** or to a waiting time that is less than five minutes.

**Workaround:** Disconnect from the Linux desktop after the log-in process is completed.

- If you resize a RHEL or CentOS desktop while it is in screensaver mode, the desktop displays a black screen, and no Unlock dialog is presented.

**Workaround:** Press the ESC key.

- 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**.

## Windows Media MMR

- Windows Media MMR does not work on Windows 10 desktops.

**Workaround:** None

- 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.

## 3D Graphics Acceleration

- 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

- 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.

- 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.

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

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

## Smart Card

- Using a smart card to log in to an RDS desktop takes longer than with a VDI, 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.
- Users running View Client 5.4.2 (the executable is wswc.exe) fail to login using smart card authentication.

**Workaround:** Install and run Horizon Client 3.0 or later.

## Client Drive Redirection

- If you disable client drive redirection with the Microsoft Remote Desktop Services group policy setting, **Do not allow drive redirection**, users can still select the **Options > Share Folders** option in Horizon Client and use the UI to select shared drives. The drives are not shared and do not appear in the remote desktop. This issue does not occur if you do not install the Client Drive Redirection option when you install View Agent.

**Workaround:** None.

## Scanner Redirection

- 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.

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

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

- Sometimes the scanner settings do not take effect on WIA scanners. For example, if you select grayscale 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 View desktop session. Launch a new desktop session and perform the scan using the selected scanner.

- When you uninstall View 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 View Agent.

## Serial Port Redirection

- 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 baudrate used by each device.

**Workaround:** None.

## View Persona Management

- View 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 View 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, View Persona Management no longer works for that user.

**Workaround:** See [KB 2058932: Granting domain administrators access to redirected folders for View Persona Management](#).

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

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

- 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 View Agent has no effect. The remote desktop language always synchronizes with the language used on the client system.

**Workaround:** None.

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

**Workaround:** None.

## vSphere Platform Support

- View Storage Accelerator might take tens of minutes to generate or regenerate the digest

files for large virtual disks (for example, a 100GB 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.

- 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 datastores for the OS disk and the user data disk and the datastore 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 datastore or by not changing the datastore selections before a View Composer rebalance operation.

- 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.

## View Composer

- When View 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 View Administrator. View Administrator will provision new machines as part of normal pool management.

- When deleting a large desktop pool, a number of folders containing an .hlog file and an empty subfolder 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 KB [Rebalance operation leaves VM folders in previous datastores \(2108928\)](#).

- 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 clones 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 message Polling 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.

## Windows 10 and Windows 8.x Support

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

- If you upgrade from a Windows 8.1 desktop to Windows 10, log in to the desktop, and press a key on the login screen, Windows displays a black screen and the desktop is unusable.

**Workaround:** Take these steps:

1. Connect to the machine from a vSphere Web Client console or RDP (not from Horizon Client) and use the on-screen keyboard to log in to the Windows 10 guest operating system.
2. Open Device Manager, logging in with administrator credentials when prompted.
3. Select **Keyboards**.
4. Right-click the displayed keyboard device and select **Properties**.
5. Click the Driver tab. The current driver should be the Lenovo ThinkPad PS/2 keyboard driver.
6. Click **Roll Back Driver** to go back to using the Microsoft keyboard driver.
7. Reboot the Windows 10 system.

- Windows 10 unmanaged machines are displayed as Windows 8 on the Registered Machines page in View Administrator. vCenter Server-managed Windows 10 machines that are in manual desktop pools and Windows 10 machines in automated pools are displayed correctly as Windows 10.

**Workaround:** None

- 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

- 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.

- 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.

- 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 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 View Administrator, the navigation panel might be displayed in Simplified Chinese.

**Workaround:** Use an alternate browser to log in to View Administrator.

- If a user of a Windows 8 View 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 View 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.

- 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.

- 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 app cleanup"`

- 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 is caused by a characteristic of Windows 10 applications. This problem affects the following desktop types:
  - Linked-clone dedicated desktops with a persistent disk.
  - 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 Windows 10 version 1607 desktop pools where 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.

- RDP connections from the View client fail when upgrading View agents on Windows 10 desktop.

**Workaround:** Configure the SecurityLayer registry key.

1. Start the Windows Registry Editor.
  2. Navigate to **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp**.
  3. Set the **SecurityLayer** value to 1.
- In Horizon View 6.2.3 or 6.2.4, printer icons are not visible in Devices and Printers folder when the Agent operating system is Windows 10 1607 CBB.

**Workaround:** Restart the Device service and add the printers back. See VMware KB article 2149788, [Printer icons are not visible in Devices and Printers folder when Agent operating system is Windows 10 1607 CBB in Horizon View 6.2.3 or 6.2.4](#), for more information.

## Windows Server for Desktop Use

- 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. Note: 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.

## Workspace Portal Integration

- If you change the default HTTPS port, 443, on a View Connection Server instance or security server, and Horizon 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 View 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.

## Virtual SAN and Virtual Volumes

- 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 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 datastore, 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.
- Virtual SAN datastores 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 datastore to another Virtual SAN datastore in a different cluster is not supported.
- In an environment where a large VDI desktop pool (for example, 2,000 desktops) is created on Virtual Volumes datastores that reside on a NetApp storage system running ONTAP 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.

## Cloud Pod Architecture

- Cloud Pod Architecture configuration changes made by another View administrator while you are logged in to View Administrator are not visible in your current View Administrator session.  
**Workaround:** Log out of View Administrator and log in again to see the changes.

## Miscellaneous

- 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.
- 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 View 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 View Administrator (Pool Settings page) and not through vSphere Client.  
**Workaround:** Either upgrade the hardware version of the virtual machines in vSphere Client, or use View Administrator to set the proper value for video memory based on the current virtual machine hardware version.