Horizon Air 15.3.2 VMware Desktop Protocols

A VMware Technical Note

This document describes the two desktop connection protocols supported by the View Agent Direct Connect Plug-in.

July 2015

Revision History

Date	Version	Description
07/30/2015	1.0	Initial release

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

1 Overview

1.1 About Desktop Protocols

The VMware View Agent has a very small footprint (90Kb) and supports the full View Client capabilities: PCoIP, RDP, HTTPS, SSL, SSO, USB Redirection, printer support, and session management. The View Agent Connect Direct Plug-in supports two desktop connection protocols: PCoIP and HTML Access.

1.1.1 PCoIP

PCoIP is a high performance display protocol. The protocol contains both WAN optimization and support for 3D graphics, resulting in a far superior end user experience when compared to RDP.

To use the PCoIP protocol:

- Each virtual desktop must have View Agent 6.0.1 or later and View Agent Direct Connect (VADC) Plug-in 6.0.1 or higher services installed and running. It is recommended that these components are upgraded to version 6.1.1.
- Virtual Desktops must be running DaaS Agent version 6.1.1 or later. It is always recommended to use the latest version of the DaaS Agent.
- End users must have the VMware Horizon View Client installed on their end point device.

1.1.2 HTML Access (Blast)

HTML Access (formerly known as Blast) enables access to a desktop via any HTML5 compliant web browser.

To use HTML Access:

- Each virtual desktop must have Horizon (View) Agent 6.0.1 or later and View Agent Direct Connect (VADC) Plug-in service installed and running. Horizon Agent 6.1.1 and VADC 6.1.1 are required in order to support HTML Access for RDSH Applications.
- Virtual Desktops must be running the DaaS Agent 15.3.2.
- For internal access not via Access Point, SSL certificate install automation must be configured as described in Appendix A.
- There are additional requirements for launching remote applications. See HTML Access (Blast) Support for RDSH Applications below for more information.

1.1.2.1 System Requirements for Using HTML Access (Blast)

Browser on client system:

- Chrome 41, 42, and 43
- Internet Explorer 10 and 11
- Safari 7 and 8 (Mobile Safari is not supported for this release.)
- Firefox 36, 37, and 38

Client operating systems:

- Windows 7 SP1 (32- or 64-bit)
- Windows 8.x Desktop (32- or 64-bit)
- Windows 10 desktop (32- or 64-bit)
- Mac OS X Mavericks (10.9)
- Mac OS X Yosemite (10.10)
- Chrome OS 28.x or later

1.1.2.2 HTML Access (Blast) Support for RDSH Applications

Launching RDSH applications is supported in HTML Access 3.4.

To enable this functionality:

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

Note the following:

- Horizon Agent 6.1.1 and the View Agent Direct-Connection (VADC) Plug-In 6.1.1 must be installed on the desktops.

  Note: When you enable HTML Access for RDSH applications in Enterprise Center as described below, users will no longer be able to connect to VMs running older versions of the Horizon (View) Agent via Blast.

- Access Point 2.0 remote access gateway must be deployed (confirm with your Service Provider).
- This functionality does not work for iOS or Android.

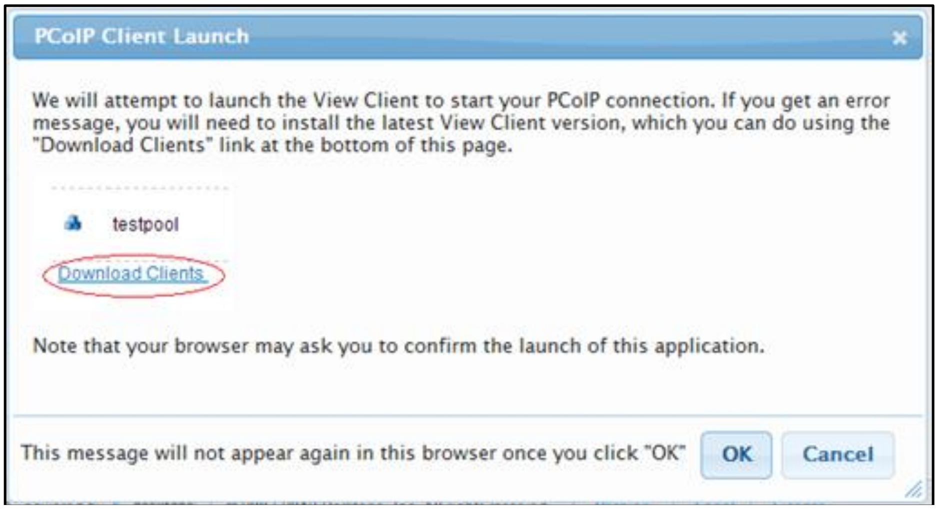
Note: Attempts to launch applications via HTML Access (Blast) fail with an error when the older version of the HTML Access client is still selected. To prevent this error, verify that the HTML Access for RDSH Remote Applications option is enabled and that the prerequisites have been met as described above.

1.2 Using the VMware Horizon View Client in the DaaS Environment

This section lists some of the View Client features you should understand and any environment characteristics unique to the DaaS integration. For complete documentation on the View Client, refer to the VMware Knowledgebase.

1.2.1 View Client Download Link Available within DaaS User Portal

If a user launches the DaaS User Portal and then attempts to connect to a desktop using the PCoIP protocol, the Horizon View Client is launched and the user is seamlessly signed in. The first time a user launches a PCoIP connection from the Desktop Portal they see the following:



PCoIP Client Launch

We will attempt to launch the View Client to start your PCoIP connection. If you get an error message, you will need to install the latest View Client version, which you can do using the "Download Clients" link at the bottom of this page.

testpool

Download Clients

Note that your browser may ask you to confirm the launch of this application.

This message will not appear again in this browser once you click "OK"

If you launch the DaaS User Portal and then attempt to connect to a desktop using the HTML Access (Blast) protocol, you are informed that you need to download the View Client by clicking the link in the information dialog. First enable pop-ups in your browser, then initiate an HTML Access connection.

1.2.2 Accessing Desktops and Applications

Note the following regarding launching desktops and remote applications.

- If you log into the View Client and have an active application session, you may be prompted to reconnect depending on the View Client settings. The View Client will only prompt to reconnect to an application session once. It will not prompt again until you logout and log back in. If the session fails to connect, users should attempt to launch applications normally.
- You cannot have an active RDS desktop and active remote application session at the same time.
- PCoIP supports only RDS-based remote applications.
- Idle timeouts are based on the activity on the endpoint device, not on the desktop or application.
- RDP is not a compatible protocol if you are logged in via PCoIP on another device. You must log out of the PCoIP session before attempting to connect via RDP.
- The View Client displays RDS desktops and remote applications as launchable items. If you do not see an option to connect to your RDS pool as a desktop, confirm that the RDSH service is enabled for full desktop access and that you have View Client 3.0 or higher.

- The remote application name displayed is the name assigned in the pool, so it is important to make the names meaningful in order to distinguish between the applications when multiple pools are mapped to them.
- The Reset Application function will log you off of all application sessions regardless of the session host you are using.
- USB re-direction is not supported for RDS-based servers.
- Launching RDSH applications is supported in HTML Access 3.4. See HTML Access (Blast) Support for RDSH Applications above for more information.

1.2.3 Session Timeout

The session begins when the user authenticates. This timeout can be changed in the Enterprise Center (**Configuration ► General**).

- **User Activity Heartbeat interval:** This value controls the interval between View Client heartbeats. These heartbeats report to the Tenant the amount of idle time that has passed. Idle time occurs when there is no interaction with the end point device, as opposed to idle time in the desktop session. In large desktop deployments, it may reduce network traffic and increase performance to have the activity heartbeats at longer intervals.
- **User Idle timeout:** This value controls the maximum time that a user can be idle while connected to the Tenant. When this time is reached, the user is disconnected from all active View Client Desktop sessions. Additionally, when the user returns, they will be required to re-authenticate in order to access the View Client.

  Note: The User Idle timeout should always be greater than the User Activity Heartbeat interval, and is recommended to be at least double the User Activity Heartbeat Interval to avoid unexpected disconnects from desktops.
- **Broker Session timeout:** This value controls the maximum time that a View Client can be connected to the Tenant before its authentication expires (timeout count starts each time you authenticate). When this timeout occurs, you will not be automatically disconnected from the desktop and are able to keep working, but if you then perform an action that causes communication to the broker (for example, changing settings), the system requires you to re-authenticate and also to log back into the desktop.

  Note: The Broker Session timeout should always be greater than the User Idle timeout, and is recommended to be at least equal to the sum of the User Activity Heartbeat interval and the User Idle timeout.

General notes:

- **In previous releases, you could use the userportal.session.timeout policy to set this timeout, but this is no longer the case beginning with the 6.1 release.**
- **View Clients running on the Android OS have been known to override this policy setting, resulting in a session timeout of approximately ten minutes.**

1.2.4 Resetting Password

When logging in to the View Client, a user might be prompted to change their password:

- After entering the new password, the View Client displays a message indicating that the password reset was successful. However, the password is not actually updated until the connection to the Horizon (View) Agent has occurred. So if the session times out before the connection occurs or the user never launches a desktop session, the password will not be updated.

- If the new password does not conform to AD rules, the log in will be unsuccessful. The user then needs to exit the View Client and attempt to reset the password again.

Note that the following character combinations cannot be used in View Client passwords:

<

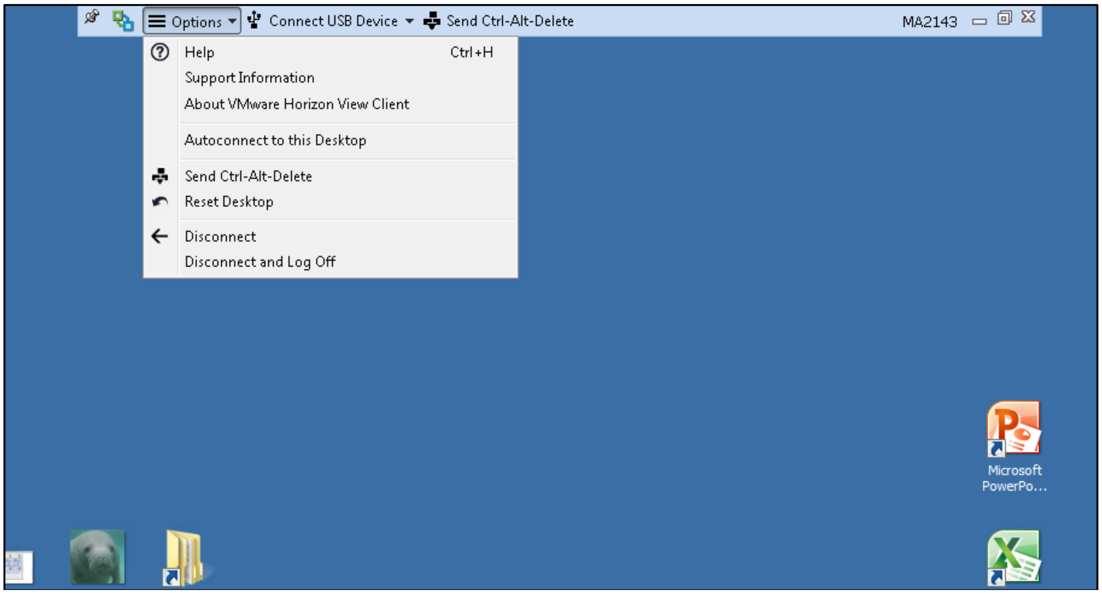
>

<!–

&amp;

1.2.5 Desktop Options

Once logged in to a desktop, a user can click **Options**:



The following table explains the functionality available from the Options menu.

Switch Desktop	Allows the User to access the Desktop Selection Screen or Switch between open desktop sections. See the Desktop Selection Screen Section for controls and info. This will not work if your session has timed out.
Autoconnect to this Desktop	For PC and thin clients, makes the specified desktop the user's default desktop when the desktop is part of a dynamic pool. On the next login, the desktop will immediately be displayed as long as: • The user has only one desktop mapped to them. • There is not a problem with the login credentials or desktop state. If a user selects Autoconnect and then logs in with multiple desktops, the Autoconnect to this Desktop setting is set to off/false. If the session times out, the Autoconnect setting is not saved and the user cannot autoconnect at the next log in.

Reset Desktop	Triggers a reboot on the desktop. This will not work if the session has timed out.
Disconnect	Disconnects the current user from their active session.
Disconnect and Logoff	Disconnects and logs off the user from their active session.

1.2.6 Triggering a Desktop Logoff from the View Client

Logging off initiates a call to the DaaS Agent which can take up to 30 seconds to complete. As a result, if a user attempts to log back in before the 30 seconds elapses, the log off dialog might still be present.

1.2.7 VRAM/Pool Provisioning Using PCoIP

When a desktop model uses the PCoIP protocol, to prevent black screen, the platform provisions pools of these desktops with the video RAM (VRAM) size set to 128. The service provider can change this policy in the Service Center.

Procedure

1. Log in to the Service Center.
2. Select **tenants ► policy**.
3. Select the Tenant Name from the drop-down.

On the Policy Configuration page, find the policy element.provision.esx.vram.size and adjust the value. The policy sets the VRAM size in KB for provisioning PCoIP protocol desktops and must be divisible by 64. The minimum is 8MB x 1024 and the default/maximum is 128MB x 1024.

2 Install the Required Software

2.1 Install Software for PCoIP

Prerequisite: If you are using PCoIP, the Windows firewall must be enabled and support PCoIP traffic.

2.1.1 Create Snapshot

Important: Prior to installing VMware Software, use the VMware vSphere Client to create a snapshot of the template (gold pattern). Remove the snapshot prior to attempting to seal the gold pattern.

2.1.2 Create Backup

Important: Prior to installing VMware software on the reserved desktop to become a template (gold pattern), consider backing up the desktop first. This functionality is available on the Reserved Desktops page of the Enterprise Center.

2.1.3 Install Correct View Clients

End users must have VMware Horizon View Clients installed (compatible with VMware View 5.2 or higher for personal desktops, or compatible with Horizon View 6.0 for RDS-based pools) for one of the following supported platforms:

- Windows, Mac, or Linux personal desktop
- iOS
- Android
- PCoIP thin and zero clients

View Clients for each device can be downloaded from https://www.vmware.com/go/viewclients

2.1.4 Prepare Desktops to Support Protocol

Before installing the software required for connecting to connect to desktops, complete the following pre-installation steps.

Procedure

1. Uninstall all software components related to all other protocols.

   Important: You must uninstall all software components related to all other protocols (e.g. HDX, RGS). If you do not uninstall these other protocol components, your template will be corrupted and you will no longer successfully boot into Windows. This warning does not apply to RDP; the presence of RDP components does not cause problems.

2. Update VMware Tools.
3. Make sure that port 443 is not being used by any other software, or use a non-standard port configured at the time of VADCP installation.

4. Make sure that the following ports are open to TCP and/or UDP traffic as indicated:

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

2.1.5 Install DaaS Agent

Procedure

1. Copy the most recent executable file (file name will be DaaSAgent_<*version*#>.msi) to each VM.
2. Run the executable file.

2.1.6 Install Horizon (View) Agent

There are three possible scenarios when installing the Horizon Agent:

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

Note: If you have not installed the most recent version of the Horizon Agent, this can cause problems with creating RDS pools. In this case, when you create a new RDS pool, the system can allow you to select HTML Access (Blast) as a protocol, but this selection will not be applied to the pool even though it appears to have been applied successfully.

2.1.6.1 Install on Desktop (Windows 7, Windows 8, Windows 8.1)

Procedure

1. Download the latest Horizon Agent from VMware's website (https://my.vmware.com). Note that there are separate downloads for 32-bit and 64-bit operating systems.
2. Double-click the Horizon Agent installation file (file name is: `VMware-viewagent-x86_64-`*`x.y.z-nnnnnnn`*`.exe` for the 64-bit installer).
3. Follow the steps in the wizard and accept default settings.
4. Restart the virtual machine when prompted.

2.1.6.2 Install on Windows Server 2008 R2 or 2012 R2 as Personal Desktop (Non-RDSH)

Procedure

1. Download the latest Horizon Agent from VMware's website (https://my.vmware.com).
2. Double-click the Horizon Agent installation file (file name is: `VMware-viewagent-x86_64-`*`x.y.z-nnnnnnn`*`.exe` for the 64-bit installer).
3. Follow the steps in the wizard.
    - ○ Select the **Install View Agent in 'desktop mode'** option.
    - ○ Accept all other default settings.
4. Restart the virtual machine when prompted.

2.1.6.3 Install on Windows Server 2008R2/2012 as RDSH Role

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

Procedure

1. Download the latest Horizon Agent from VMware's website (https://my.vmware.com).
2. Run the following on the command line as an administrator user:

    ```
    VMware-viewagent-x86_64-x.y.z-nnnnnnn.exe /v "VDM_SKIP_BROKER_REGISTRATION=1"
    ```

3. Follow the steps in the wizard and accept default settings.
4. Restart the virtual machine when prompted.

2.1.7 Install VMware View Agent Direct Connect Plug-in

Procedure

1. Contact your customer support representative for the location from which to download the latest View Agent Direct Connect installer. Just as with the Horizon (View) Agent, there are separate downloads for 32-bit and 64-bit operating systems.
2. Double click on the View Agent Direct Connect Plug-in executable to start the installation. The VMware Horizon View Agent Direct Connect Plug-In Setup Wizard launches.
3. Click **Next** and Accept the terms of the license agreement.
4. Click **Next** and accept the default port settings.
5. Click **Next** and then click **Install** to begin the installation.
6. In the Windows Control Panel, verify that VMware View Agent Direct Connect appears in the list of installed programs (Control Panel\Programs\Programs and Features). If not, the installation did not complete properly and you will need to reinstall.

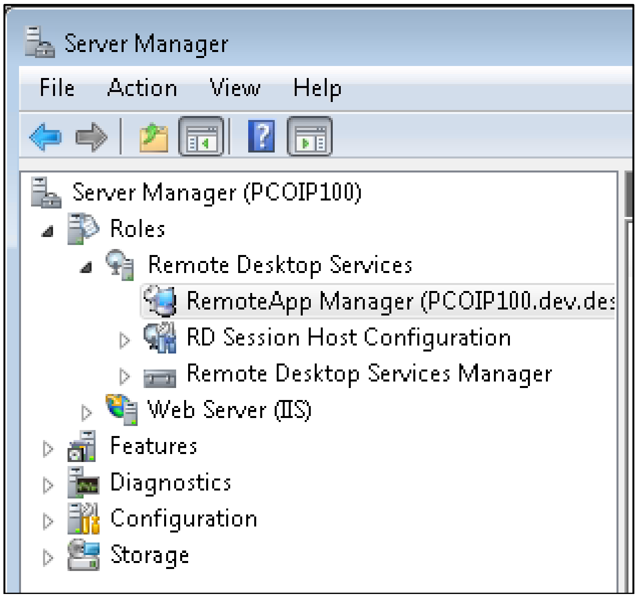
2.1.8 Configure Windows RDS Servers (for RD Session Hosts only)

RD WebAccess is a component required by the Horizon (View) Agent for connections.

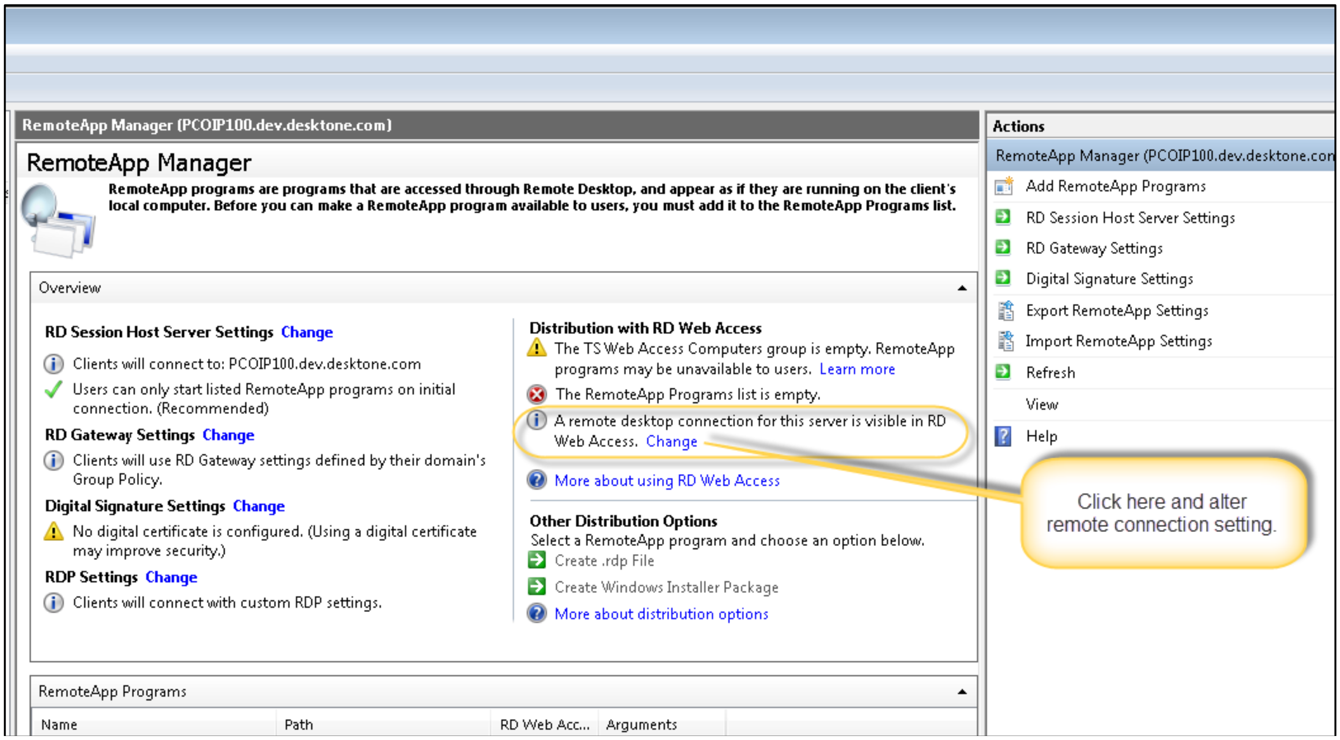
Note: To use this functionality, you must have version 6.1 or higher of the agent installed.

Procedure

1. Add Role RD WebAccess
2. In Server Manager, click the RemoteApp Manager option:


Server Manager
File
Action
View
Help
Server Manager (PCOIP100)
Roles
Remote Desktop Services
RemoteApp Manager (PCOIP100.dev.des
RD Session Host Configuration
Remote Desktop Services Manager
Web Server (IIS)
Features
Diagnostics
Configuration
Storage

3. Select the **Change** link as shown below.



RemoteApp Manager (PCOIP100.dev.desktone.com)

RemoteApp Manager

RemoteApp programs are programs that are accessed through Remote Desktop, and appear as if they are running on the client's local computer. Before you can make a RemoteApp program available to users, you must add it to the RemoteApp Programs list.

Overview

RD Session Host Server Settings Change

Clients will connect to: PCOIP100.dev.desktone.com

Users can only start listed RemoteApp programs on initial connection. (Recommended)

RD Gateway Settings Change

Clients will use RD Gateway settings defined by their domain's Group Policy.

Digital Signature Settings Change

No digital certificate is configured. (Using a digital certificate may improve security.)

RDP Settings Change

Clients will connect with custom RDP settings.

Distribution with RD Web Access

The TS Web Access Computers group is empty. RemoteApp programs may be unavailable to users. Learn more

The RemoteApp Programs list is empty.

A remote desktop connection for this server is visible in RD Web Access. Change

More about using RD Web Access

Other Distribution Options

Select a RemoteApp program and choose an option below.

Create .rdp File

Create Windows Installer Package

More about distribution options

RemoteApp Programs

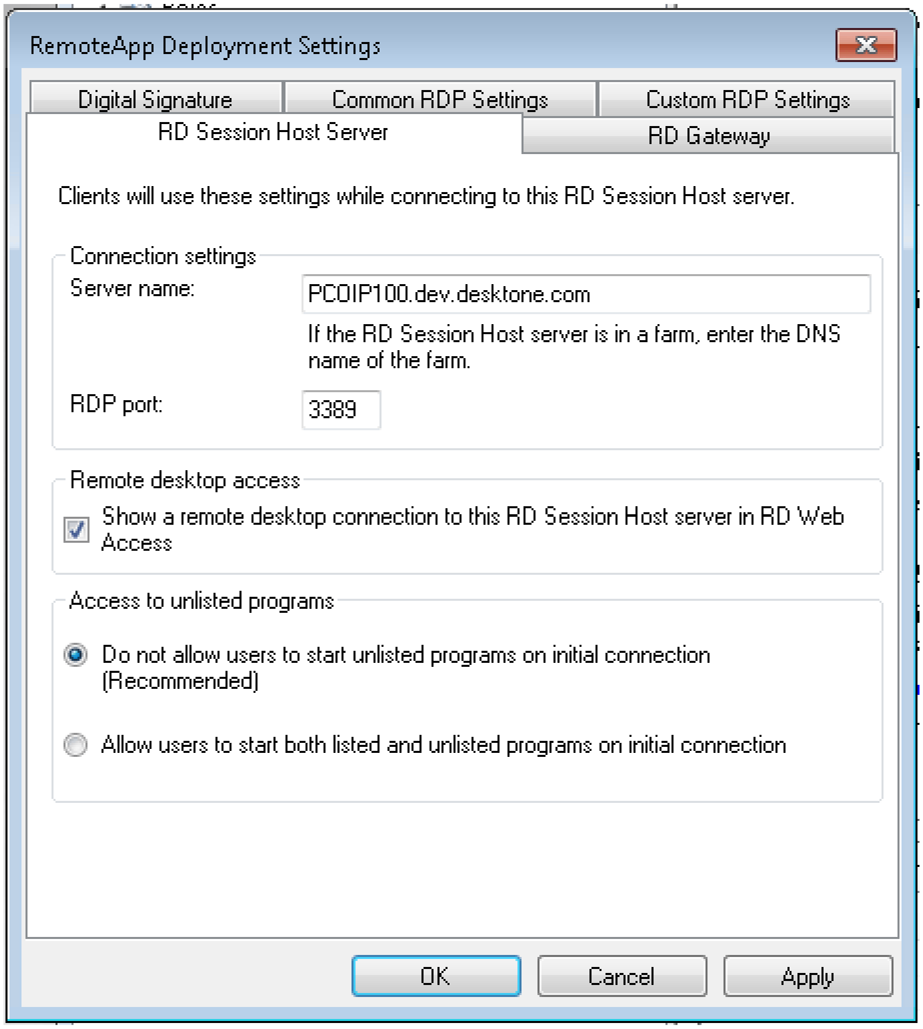
Name	Path	RD Web Acc...	Arguments

Actions
RemoteApp Manager (PCOIP100.dev.desktone.com
Add RemoteApp Programs
RD Session Host Server Settings
RD Gateway Settings
Digital Signature Settings
Export RemoteApp Settings
Import RemoteApp Settings
Refresh
View
Help

Click here and alter remote connection setting.

The RemoteApp Deployment Settings dialog box appears.

4. On the RD Session Host Server tab of the dialog box, select the check box under **Remote desktop access**:



Clients will use these settings while connecting to this RD Session Host server.

Connection settings

Server name: PCOIP100.dev.desktone.com

If the RD Session Host server is in a farm, enter the DNS name of the farm.

RDP port: 3389

Remote desktop access

☑ Show a remote desktop connection to this RD Session Host server in RD Web Access

Access to unlisted programs

● Do not allow users to start unlisted programs on initial connection (Recommended)

○ Allow users to start both listed and unlisted programs on initial connection

5. Click **OK**.

2.1.9 Using PCoIP with vSphere 5.1 ESXi Hosts

There are a few special requirements in order to use PCoIP with virtual desktops running on vSphere v5.1. The vSphere v5.1 build number must be 838463 or later. Please refer to the following VMware KB for specific details: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2035268.

To enable a virtual desktop, perform the following steps.

Procedure

1. If VMware Tools v5.1 is installed, uninstall it.
2. Start the VMware Tools 5.1 installation.
3. Choose a Custom Install.

4. Disable the SVGA drivers and complete the install.
5. Install the latest Horizon (View) Agent.
6. Install the latest View Agent Direct Connect plugin-in.

2.2 Install Software for HTML Access (Blast)

2.2.1 Create Snapshot

Important: Prior to installing VMware Software, use the VMware vSphere Client to create a snapshot of the template (gold pattern). Remove the snapshot prior to attempting to seal the gold pattern.

2.2.2 Install Correct Browser

See list of supported browsers in System Requirements for Using HTML Access.

2.2.3 Prepare Desktops to Support Protocol

Before installing the software required to connect to desktops, complete the following pre-installation steps.

Procedure

1. Uninstall all software components related to all other protocols

   Important: You must uninstall all software components related to all other protocols (e.g. HDX, RGS). If you do not uninstall these other protocol components, your template will be corrupted and you will no longer successfully boot into Windows. This warning does not apply to RDP; the presence of RDP components does not cause problems.

2. Update VMware Tools.
3. Make sure that port 443 is not being used by any other software.
4. For HTML Access (Blast), enable the Windows Firewall if not already enabled.
5. Make sure that the following ports are open to TCP and/or UDP traffic as indicated:

Port(s)	Source	Destination	TCP	UDP
4172	Access Point	VM	✓	✓
443	Tenant Appliance	VM	✓	
22443	Access Point	VM	✓	
443 (Blast and Enterprise Center)	Access Point	T/VM	✓	
8443 (Blast)	Access Point	VM	✓	
4172 (PCoIP)	Access Point	VM	✓	✓
80 (redirects to 443)	Access Point	T/VM	✓	

2.2.4 Install DaaS Agent

Procedure

1. Copy `VMware-DaaS-Agent-`*`xxxx`*`.msi` to each VM. This is an executable file.
2. Run `VMware-DaaS-Agent-`*`xxxx`*`.msi`

   Note: You must use the DaaS Agent 6.1.1 or later for HTML Access (Blast) functionality.

2.2.5 Install Horizon (View) Agent

There are three possible scenarios when installing the Horizon Agent:

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

Note: If you have not installed the most recent version of the Horizon Agent, this can cause problems with creating RDS pools. In this case, when you create a new RDS pool, the system can allow you to select HTML Access (Blast) as a protocol, but this selection will not be applied to the pool even though it appears to have been applied successfully.

2.2.5.1 Install on Desktop (Windows 7, Windows 8, Windows 8.1)

Procedure

1. Download the latest Horizon Agent from VMware's website (https://my.vmware.com). Note that there are separate downloads for 32-bit and 64-bit operating systems.
2. Double-click the Horizon Agent installation file (file name is: `VMware-viewagent-x86_64-`*`x.y.z-nnnnnnn`*`.exe` for the 64-bit installer).
3. Follow the steps in the wizard and accept default settings.
4. Restart the virtual machine when prompted.

2.2.5.2 Install on Windows Server 2008 R2 or 2012 R2 as Personal Desktop (Non-RDSH)

Procedure

1. Download the latest Horizon Agent from VMware's website (https://my.vmware.com).
2. Double-click the Horizon Agent installation file (file name is: `VMware-viewagent-x86_64-`*`x.y.z-nnnnnnn`*`.exe` for the 64-bit installer).
3. Follow the steps in the wizard.
   - Select the option to install the Agent in 'desktop mode'.
   - Accept all other default settings.
4. Restart the virtual machine when prompted.

2.2.5.3 Install on Windows Server 2008R2/2012 as RDSH Role

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

Procedure

1. Download the latest Horizon (View) Agent from VMware's website (https://my.vmware.com).
2. Run the following on the command line as an administrator user:

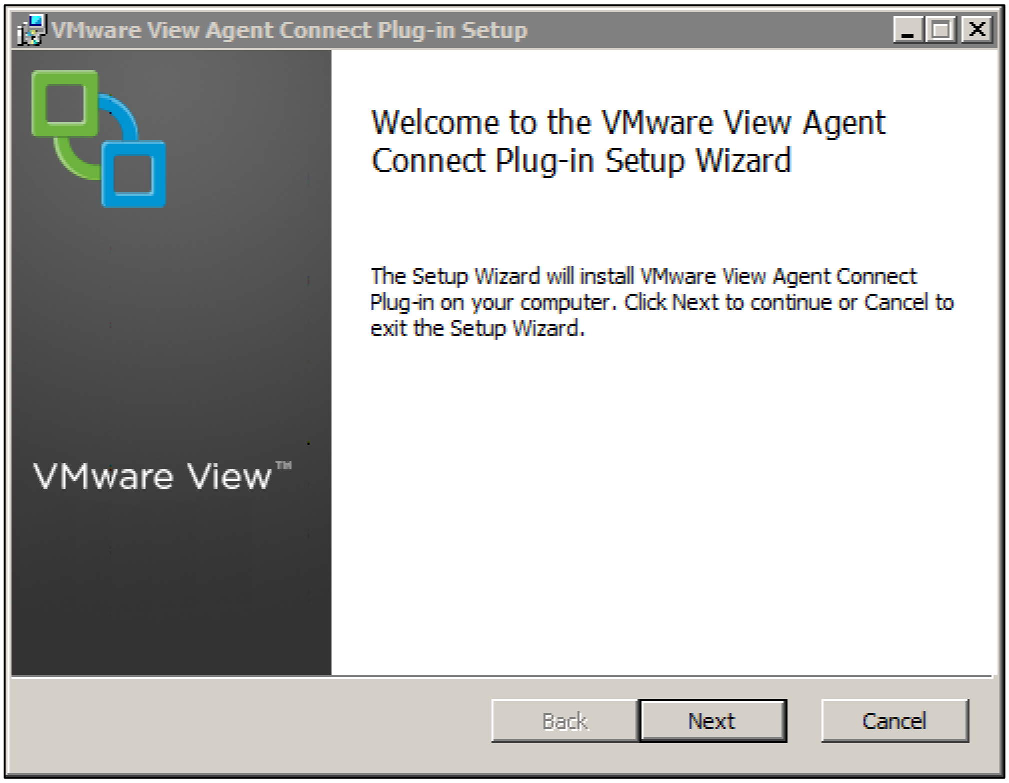
   ```
   VMware-viewagent-x86_64-x.y.z-nnnnnnn.exe /v "VDM_SKIP_BROKER_REGISTRATION=1"
   ```

3. Follow the steps in the wizard and accept default settings.
4. Restart the virtual machine when prompted.

2.2.6 Install VMware View Agent Direct Connect Plug-in

Procedure

1. Contact your customer support representative for the location from which to download the latest VMware View Agent Direct Connect installer. Just as with the View Agent, there are separate downloads for 32-bit and 64-bit operating systems.
2. Double click on the View Agent Direct Connect Plug-in executable to start the installation. The VMware Horizon View Agent Direct Connect Plug-In Setup Wizard launches:



VMware View Agent Connect Plug-in Setup

Welcome to the VMware View Agent Connect Plug-in Setup Wizard

The Setup Wizard will install VMware View Agent Connect Plug-in on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

3. Click **Next** and accept the terms of the license agreement.
4. Click **Next** and accept the default port settings.
5. Click **Next** and then click **Install** to begin the installation.

6. In the Windows Control Panel, verify that VMware View Agent Direct Connect appears in the list of installed programs (Control Panel\Programs\Programs and Features). If not, the installation did not complete properly and you will need to reinstall.

3 Validate Installation

To validate the installation, try to connect to the desktop using the View Client. Trying to connect will verify that:

- Video RAM and driver are sufficient to avoid black screen.
- There are no conflicts in port usage.
- The View Agent installation was successful.
- The View Client version is correct.

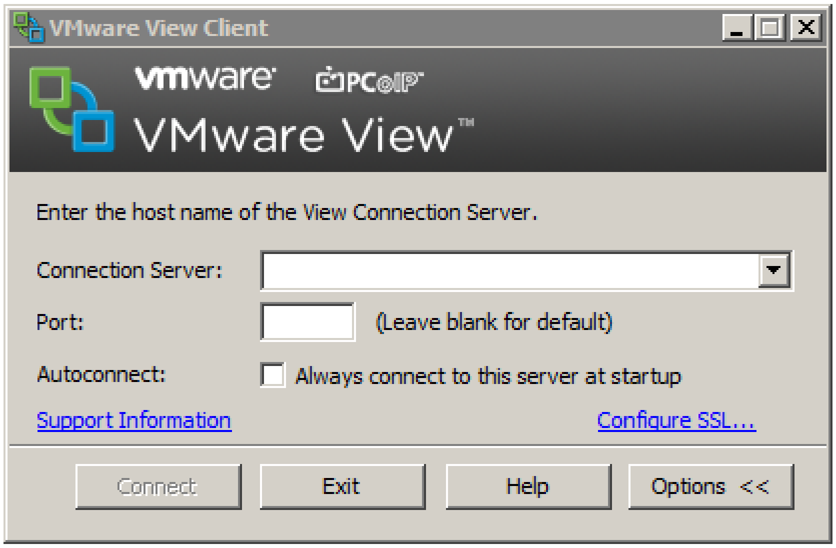
3.1 Connect to Desktop using View Client

Note: Do not use the VMware Horizon View Client for Windows with Local Mode Option.

After installing the required software, you should be able to connect to a desktop using the View Client:

Procedure

1. Launch the VMware Horizon View Client.
2. In the Connection Sever field, enter the IP address or DNS name of the Desktop Portal:



Enter the host name of the View Connection Server.

Port: (Leave blank for default)

Autoconnect: □ Always connect to this server at startup

3. Click **Connect**.
4. Enter User Name and Password.
5. Click **Login**. The View Client displays the list of available desktops.

   Note: The connection is established using the default display protocol. The default can be set in either the Desktop Portal or by the System Administrator in the Enterprise Center when creating pools.

   Note: If you cannot log in, refer to Section 3.2.

6. Select a desktop and click **Connect**.

Note: Right-mouse click on a desktop to see the following additional desktop operations:

- Connect: Connects to the desktop using the default display protocol.
- Display Protocol: Overrides the default display protocol.
- Logoff: Ends your desktop session. Any unsaved work will be lost.
- Reset Desktop: Restarts Windows OS.

Note: If you cannot connect to the desktop, refer to Section 3.2.

3.2 Troubleshoot View Client Problems

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

- **Login Problems**: If you cannot log in to the View Client, verify that the version of the VMware Horizon View Client you are using is compatible with VMware View 5.1 or higher.
- **Desktop Does Not Launch**: If the Desktop does not launch, verify that no other software in the environment is using port 443.
- **Unable to Connect to Desktop**: If you receive the error message "Unable to Connect to Desktop," it means that the View Agent is not running. In the Windows Control Panel programs, verify that Horizon (View) Agent and View Agent Direct Connect appear in the list of installed programs. If they do not, the installation did not complete properly and you will need to reinstall. If the View Agent software is installed, verify that the View Agent Service is running.
- **Desktop Disconnects**: If a View Client session ends too quickly when idle, this means that View Client Session Timeout settings are configured to allow only a very short idle period. You can configure the View Client Session Timeout settings in Enterprise Center under **configuration ► general**.
- **Black Screen**: If you experience black screen using the View Client, refer to the troubleshooting instructions in Section 5.1.1.

3.3 Troubleshoot HTML Access (Blast) Connect Problems

There are several configuration/setup problems that can result in an inability to launch a HTML Access (Blast) connection successfully:

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

4 Optimize Your Display

4.1 Add the PCoIP Group Policy Settings to the Local Computer Policy Environment

To configure the group policies for a gold pattern, you must first add the .adm template file to the Local Computer Policy configuration on this VM.

Procedure

1. On the gold pattern VM, click **Start** ► **Run**.
2. Type gpedit.msc, and click **OK**.

   This opens the Local Group Policy Editor console in Windows.
3. Make sure you can connect to the View Connection Server from this VM.
4. In the navigation pane, select **Local Computer Policy** ►**Computer Configuration**.
5. Right-click **Administrative Templates**.

   Note: Do not select Administrative Templates under User Configuration.
6. Select **Add/Remove Templates**.
7. In the Add/Remove Templates dialog, click **Add**.
8. Download the following file from the Horizon DaaS Library on salesforce.com:

   `pcoip_policies.adm`
9. Click **Open**.
10. Close the Add/Remove Templates window.

    The PCoIP group policy settings are added to the Local Computer Policy environment on the desktop system and are available for configuration.

4.2 Add the HTML Access (Blast) Group Policy Settings to the Local Computer Policy Environment

1. Download the View GPO Bundle .zip file from the VMware Horizon 6 download site at:

   http://www.vmware.com/go/downloadview

   The file is named VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyyy.zip, where x.x.x is the version and yyyyyyy is the build number. All ADM and ADMX files that provide group policy settings for View are available in this file.
2. Copy the file to your Active Directory server and unzip the file.

   The HTML Access GPOs are included in the Blast-enUS.adm ADM Template file.

3. On the Active Directory server, edit the GPO.

Option	Description
Windows 2008 or 2012	a) Select **Start > Administrative Tools > Group Policy Management**. b) Expand your domain, right-click the GPO that you created for the group policy settings, and select **Edit**.
Windows 2003	a) Select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**. b) Right-click the OU that contains your View desktops and select **Properties**. c) On the Group Policy tab, click **Open** to open the Group Policy Management plug-in. d) In the right pane, right-click the GPO that you created for the group policy settings and select **Edit**.

   The Group Policy Object Editor window appears.

4. In the Group Policy Object Editor, right-click **Administrative Templates** under Computer Configuration and then select **Add/Remove Templates**.
5. Click **Add**, browse to the `Blast-enUS.adm` file, and click **Open**.
6. Click **Close** to apply the policy settings in the ADM Template file to the GPO.

   The VMware Blast folder appears in the left pane under **Administrative Templates > Classic Administrative Templates**.

7. Configure the HTML Access group policy settings.
8. Make sure your policy settings are applied to the remote desktops.
   a. Run the `gpupdate.exe` command on the desktops.
   b. Restart the desktops.

4.3 Configure Settings

Set in the following in the Overrideablepolicy group:

1. Enable “Turn off Build-to-Lossless feature”

   Mark the check box to turn it off the feature.

2. Enable “Configure PCoIP image quality levels”
   - Set Minimum Image Quality to 30
   - Set Maximum Image Quality to 70
   - Set Maximum Frame Rate to 16

4.4 Enable 3D Graphics

3D graphics can now be enabled on a per pool basis. Support for 3D graphics is provided using Soft 3D, also known as vSGA (see pages 3-4 of the VMware white paper on Graphics Acceleration for more information). In order for you to use 3D graphics feature, the following must be true:

- The virtual hardware version must be 8 or higher.
- Desktop must have the Windows Aero theme
- Servers must have appropriate hardware installed

Note: Consult the latest PCoIP recommendations when configuring desktops with this feature.

5 Troubleshooting

This chapter presents the most common problems you might need to troubleshoot. For information on other problems that might occur when using VMware software, refer to the VMware Knowledge Base at http://kb.vmware.com.

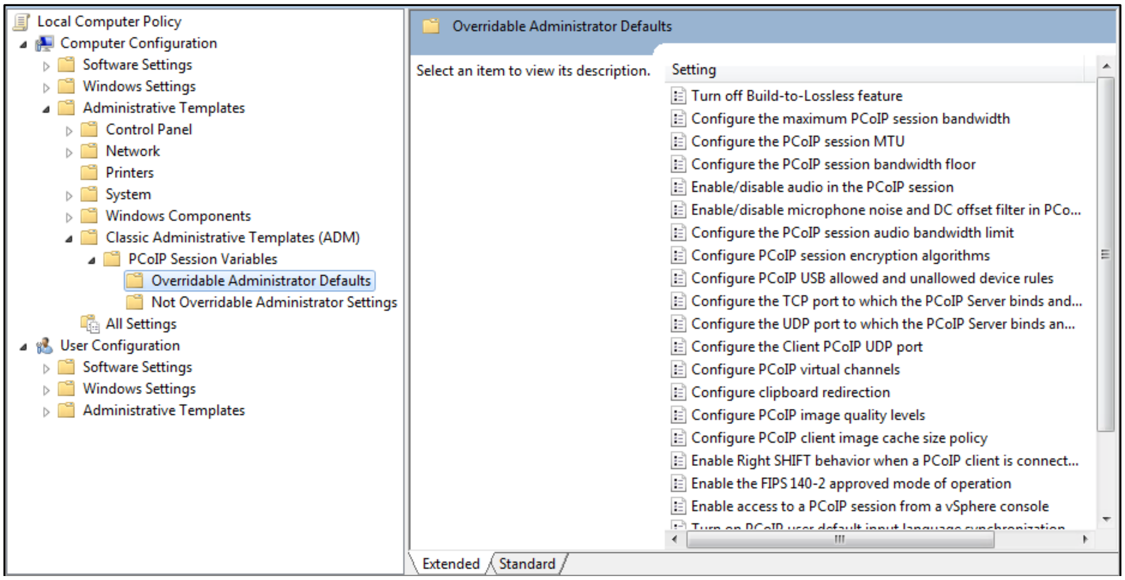
5.1 Protocol Problems

5.1.1 Black Screen

- Normally, the View Client will expand the desktop image to encompass the entire View Client display. If the View Client does not fully expand the display, showing black panels along the sides, it might be due to a limit in the Video RAM available. Increasing the Virtual Desktop's Video RAM might cause the black panels to be removed.
- When you update VMware Tools, the update can in some cases install the wrong video driver, resulting in black screen. The workaround is to log into the session using RDP and install the correct driver.
- If the System Administrator moves a desktop from a non-PCoIP pool to a PCoIP pool and users experience a black screen when trying to connect to the desktop, solutions can be found in the VMware Knowledge Base at kb.vmware.com:
  - Refer to the steps outlined in the VMware Knowledge Base article Black screen when logging into a VMware View virtual desktop using PCoIP.
  - Verify that the Video RAM (VRAM) settings in the Virtual Machine settings (.vmx) file are set properly for multi-monitor access when using the PCoIP protocol. Refer to the VMware Knowledge Base article Determining display and screen resolution settings for PCoIP.
  - Verify that the Video driver is correct for the VMware View Agent and operating system. Refer to the VMware Knowledge Base article "The PCoIP server log reports the error: Error attaching to SVGADevTap, error 4000: EscapeFailed."

5.1.2 Override ADM PCoIP Defaults

ADM can be configured on the Domain Controller or the master desktop image being used to create a gold pattern. On the master desktop image, the System Administrator can override ADM defaults by running gpedit.msc on the desktop and navigating to the **Administrative Template ► Classic Administrative Templates (ADM) ► PCoIP** folder:



- Turn off Build-to-Lossless feature
- Configure the maximum PCoIP session bandwidth
- Configure the PCoIP session MTU
- Configure the PCoIP session bandwidth floor
- Enable/disable audio in the PCoIP session
- Enable/disable microphone noise and DC offset filter in PCo...
- Configure the PCoIP session audio bandwidth limit
- Configure PCoIP session encryption algorithms
- Configure PCoIP USB allowed and unallowed device rules
- Configure the TCP port to which the PCoIP Server binds and...
- Configure the UDP port to which the PCoIP Server binds an...
- Configure the Client PCoIP UDP port
- Configure PCoIP virtual channels
- Configure clipboard redirection
- Configure PCoIP image quality levels
- Configure PCoIP client image cache size policy
- Enable Right SHIFT behavior when a PCoIP client is connect...
- Enable the FIPS 140-2 approved mode of operation
- Enable access to a PCoIP session from a vSphere console
- Turn on PCoIP user default input language synchronization

5.2 Error Messages

5.2.1 Error 500

If a user receives Error 500 in the View Client, look in the tenant log and make a note of the exception before contacting support. The exception to look for will mention the ViewClientServlet.

5.2.2 Common Error Messages

The following table lists the most common error messages users can receive and the causes when using the using the View Client to connect to their desktop. The Error Details portion of the message provides information needed by customer support to troubleshoot the connection problem.

Message	Cause
View Agent Login Failed. Error Details: <*Message from Agent*>	The View Agent failed the login request sent.
Session has Expired, Please Restart View Client to Connect	Desktop Portal session timeout has occurred. The Desktop Portal timeout is based on a policy (userportal.session.timeout) set at the service provider, but may be overridden by a Configuration setting in Enterprise Center.

Unable to allocate a desktop - pool refresh is in progress.	Wait a few minutes and try again. Dynamic pool refresh is underway. This means that desktops are being destroyed and recreated based on a new or altered Gold Pattern. Once the refresh completes, users will be able to log into their desktop.
Error communicating with desktop. Please contact your Administrator. Error Details: Desktop Agent Communication Error	Unable to parse error from Authentication Error Response due to interrupted communication between the View Client, Tenant and View Agent Connect. There might be a warning or error in the desktone.log file related to ViewClientServlet.
Could not parsed XML	DataView Client or Agent returned XML which could not be read by the DaaS platform.
Desktop is not ready for connection (may be powering off or on). Please wait a few minutes or try again. If problem persists, please contact your Administrator. Error Details: Power state < *current power state of the VM* >	Desktop is not in a "powered_on" state. If the system is powered off, the admin or user will need to power on the system in the Enterprise Center or Desktop Portal, respectively.
Desktop is not ready for connection (DaaS Agent may be starting up). Please wait a few minutes or try again. If problem persists, please contact your Administrator.	DaaS Agent is reported as offline. Reboot the desktop if the problem persists and console access is too long. The DaaS Agent should come up when the desktop comes up (within a few minutes).
Desktop is not ready for connection (may be shutting down or rebooting). Please wait a few minutes or try again. If problem persists, please contact your Administrator.	OS state is not running. Wait until it is running or reboot from Desktop Portal or Enterprise Center.
Desktop is not ready for connection (currently in maintenance mode). Please wait a few minutes or try again. If problem persists, please contact your Administrator.	Domain rejoin maintenance is occurring for a dynamic desktop. This can also occur during dynamic pool refresh.
Unable to Connect to Desktop. Please contact your Administrator. Error Details: View Agent is not running	The DaaS Agent has reported that the View Agent service is not running or listening on the require ports. Make sure that the View Agent is installed and that the firewall ports are open (4172, 32111, 443). Reboot machine or check service "View Agent Connect" through RDP (User Portal) if possible.
Unable to Connect to Desktop. Please contact your Administrator. Error Details: VMware Tools is not running	VMware Tools are offline. See troubleshooting/solution on VMware tools.
Unable to Connect to Desktop. Please contact your Administrator. Error Details: VMware Tools is not installed	VMware Tools are not installed. See troubleshooting/solution on VMware tools.
Unable to Connect to Desktop. Please wait a few minutes and try again. If problem persists, please contact your Administrator	Desktop Unavailable. This is a generic message from the Allocator Service. Try checking the state of the machine and the tenant system to see if there are other issues.
Unable to Connect to Desktop. Desktop has been allocated to a different user. Please Contact your Administrator. Error Details: Desktop Already in Allocated State.	Another user has been allocated this desktop. A session exists with a GUID different from the current user.

Login Failure. Please contact your Administrator. Error Details: Unable to lookup user GUID using credentials	An exception was raised by the Horizon DaaS software during a GUID lookup. Possible reasons include: Domain controller is offline; the Fabric node had failures; general tenant problems.
Unable to Connect to Desktop. Please wait a few minutes and try again. If problem persists, please contact your Administrator. Error Details: Unknown IP Address	IP Address is null or invalid. The IP address can be null if the DaaS Agent is in the middle of logging in or the VM is starting up.
Unable to Connect to Desktop. Please contact your Administrator. Error Details: Invalid IP Address <IP_address>	The IP address is listed only if it is known.
Unable to Connect to Desktop. Please contact your Administrator. Error Details: Unable to retrieve Tenant Domain information	There is no Domain information logged in the database. The DaaS platform cannot associate the tenant with any Domain.
Login Failure: Unknown user name or bad password. Please try again.	User name or password are invalid for the given domain.
Unable to Allocate Desktop, No Desktops Available. All desktops in pool are currently in use.	Dynamic pool has no desktops that are available to the user.
Unable to Connect to Desktop (current connected protocol incompatible). Please log off previous session and try again.	The Allocator Service is indicating the current session is using a non-compatible protocol.
Unable to complete log off. If problem persists, please contact your Administrator. Error Details: Invalid session id	This error occurs if the DaaS platform cannot parse the XML, the session-id key returned in the XML is null, or if the key is malformed.
Unable to complete log off. If problem persists, please contact your Administrator. Error Details: Unable to Associate Session Id with Active Sessions	There are no active sessions for the current user.
Unable to complete log off. If problem persists, please contact your Administrator. Error Details: Error communicating with Desktop Manager	This error occurs if when the DaaS platform throws an exception.
The desktop <*x*>,<*n*> is not in the list of entitled desktops	In this message, <x> is the application name you are attempting to launch and <*n*> is a number. This message indicates that you may be using an incompatible View Client and should reference the client's release notes to confirm it supports Remote Application functionality.

5.2.3 Error Messages Associated with Password Changes

The following table lists the error messages a user can receive and the causes when attempting to change their password in the View Client.

Message	Cause
Please Enter the Old Password and the New Password.	Some or all of the password fields are blank.
Provided Old Password is invalid, please try again.	If the password you logged in with is different from the "Old Password".

Provided New Passwords do not match, please try again.	The user mistyped the password.
Please Enter a New Password that is different from the Old Password	The new password the user entered is the same as their old password.
Unable to Change Password. Please restart View Client and try again. Error Detail <*message from View Agent*>	After the user selected desktop, completing password change screen, and clicked connect, the View Agent was unable to change the Domain password. **Note: A user confirmation dialog after the password change screen incorrectly indicates "You successfully changed your password and should use it in the future."**

Note that the following character combinations cannot be used in View Client passwords:

<

>

<!—

&amp;

For example, none of the following passwords are supported:

Desktone<

Desktone>

Desktone <!—

Desktone&amp;

6 Known Limitations and Workarounds

6.1 General

- When logging in, you might see the Windows Security screen rather than your desktop. If this happens, set the registry key SoftwareSASGeneration on the VM to the value 2. The SoftwareSASGeneration registry key is in the following directory:
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- You might see a pop-up indicating that the TPAutoConnect User Agent has crashed. TPAutoConnect is the VMware ThinPrint service. You can safely disable this service to suppress the error. However, disabling this service will not allow any locally attached printers to pass through and be used in the session.
- If you have disabled the ability to lock the workstation, black screen occurs for approximately 10 – 15 seconds after login.
- There can be up to a three minute delay between turning on USB Redirection and seeing an external storage device show up on the file system.
- When using a USB re-directed headset, the audio quality is choppy.
- When using two or more monitors:
- Maximizing the PCoIP View Client window results in a black screen.
- If the resolutions are different, the desktop with the lower resolution appears as a small piece of the desktop with the higher resolution and is unusable.
- When logging into a desktop using the View Client, the login screen can be displayed for a few seconds. You do not need to (and should not try to) enter your credentials again.
- The Android Mobile device client exits on Session Timeout and the user will need to re-launch the View Client to access their desktop.
- Users cannot see unmanaged desktops in the View Client. Unmanaged desktops appear only in the User Portal.
- The View Agent supports only copy/paste of text, you cannot copy/paste files or images.
- The View Client does not currently support hard drive redirection.
- Autoconnect functionality works only on PC and thin clients, not on mobile devices or Macs.
- Print jobs redirected from a Chrome browser print text with lower quality.
- On Android devices, after a user clicks reset desktop, the user is prompted to reenter their login credentials. After the user is re-authenticated, the desktop is then reset.
- By default, when the USB Autoconnect setting is enabled from the View Client, only USB devices plugged in after the connection to the VM is brokered will auto-connect. This is a limitation of the View Client, not the DaaS platform. The workaround on a PC is as follows:

  a. Add the vdm_client.adm template file to the Local Computer Policy configuration. This template file is located on the system running the View Client in the following directory:

     C:\Program Files\VMware\VMware View\Client\extras

b. Enable the "Connect all USB devices to the desktop on launch" policy.

- Some GPOs are ignored. Regardless of the GPO setting, users can do any of the following:

Reset Desktop	Users can reset a Static desktop that has no active sessions or that has an active session attributed to that particular user.
USB Autoconnect	Users can set the policy to turn on/off USB Auto Connect.
Log Off from Active Session	Users can choose to log off from the active session. They cannot, however, log off other users from the machine
Autoconnect to a Desktop	Users can auto connect to their desktop.

- PCoIP does not display video from a redirected USB Webcam.
- When streaming media over Mobile devices, there are more skipped frames and frame freezes.
- From a PC or Wyse P20, Flash media will have an audio lag of approximately .25 – .5 seconds.

6.2 HTML Access (Blast) Specific

- Internet Explorer version 9 is no longer supported. Internet Explorer 10 or 11 is required. Newer versions of IE are not supported.
- An SSL certificate warning will be displayed upon connecting to the desktop. This is because the SSL certificate process was not performed correctly on a tenant gold pattern.
- Changing resolution to 2560x1920 ends the HTML Access session. This happens due to lack of vRAM allocation. For more information see Estimating Memory Requirements for Virtual Desktops in the View documentation.
- If your client system uses a super high resolution monitor (such as 2560 x 1600), HTML Access fails to display the desktop.

  Workaround: Lower the resolution on your monitor and connect. The resolution on the client monitor must be less than 2560 x 1600 if the remote desktop resolution is 1920 x 1200.
- Sound playback quality is best on browsers that have Web Audio API support, such as Chrome, Safari, and Firefox 25. Browsers that do not have this support include Internet Explorer (up to and including Internet Explorer 11) and Firefox 24 and earlier.
- Black artifacts appear on the screen on ESXi 5.1 or 5.0 hosts. This is a known HTML Access issue when the desktop HW version is 9 (ESX 5.0/5.1) with 3D disabled and the Windows 7 basic theme is used. This is not an issue when Aero is turned on or when the VM uses HW version 10 (ESX 5.5).
- View Agent session timeout may occur before the Desktop Portal session timeout, resulting in “Authentication error” connecting to the desktop via HTML Access. The workaround for this this is to log out of Desktop Portal and log in again.

For additional known limitations, see Known Issues in the *HTML Access Release Notes*.

Appendix A Automate SSL Certificate Install for VMware Blast

The process described in this appendix is needed to facilitate internal access that is not via Access Point. If you do not have users requiring this type of access, you do not need to perform this procedure.

Note the following:

- **You must follow this process on the gold pattern before converting the VM as a gold pattern or reseal.**
- **You must repeat this process each time you open and re-seal a gold pattern.**

You can install the certificate using post sysprep script execution in order to avoid sysprep issues and duplicate certificate problems. You can also use your own own standard practice as well (for example, Active Directory GPO and scripts). Please read the Horizon View feature pack documentation for SSL certificate requirements.

Follow the steps below to configure post sysprep commands/scripts in the Horizon DaaS environment.

- Import certificate on test machine and note certificate thumbprint.
- Create post sysprep script/batch file on gold pattern image and copy certificate.
- Convert image to gold pattern or reseal.

Import Certificate and Record Certificate Thumbprint

Procedure

1. Add the certificate snap-in to MMC by performing the steps below.

   In order to add certificates to the Windows certificate store, you must first add the certificate snap-in to the Microsoft Management Console (MMC). Before you begin, verify that the MMC and certificate snap-in are available on the Windows guest operating system.

   a. On the desktop, click **Start** and type `mmc.exe`

   b. In the MMC window, select **File > Add/Remove Snap-in**.

   c. In the Add or Remove Snap-ins window, select **Certificates** and click **Add**.

   d. In the Certificates snap-in window, select Computer account, click **Next**, select local computer, and click **Finish**.

e. In the Add or Remove snap-in window, click **OK**.

2. Import a certificate for the HTML Access Agent into the Windows Certificate Store by performing the steps below.

   To replace a default HTML Access Agent certificate with a CA-signed certificate, you must import the CA-signed certificate into the Windows local computer certificate store. Before you begin, verify that the HTML Access Agent is installed, the CA-signed certificate was copied to the desktop, and the certificate snap-in was added to MMC (see Step 1 above).

   a. In the MMC window, expand the Certificates (Local Computer) node and select the Personal folder.

   b. In the Actions pane, select **More Actions > All Tasks > Import**.

   c. In the Certificate Import wizard, click **Next** and browse to the location where the certificate is stored.

   d. Select the certificate file and click **Open**.

      To display your certificate file type, you can select its file format from the File name drop-down menu.

   e. Type the password for the private key that is included in the certificate file.

   f. Select **Mark this key as exportable**.

   g. Select **Include all extendable properties**.

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

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

   i. Verify that the new certificate contains a private key.

      1) In the Certificates (Local Computer) > Personal > Certificates folder, double-click the new certificate.

      2) In the General tab of the Certificate Information dialog box, verify that the following statement appears: You have a private key that corresponds to this certificate.

3. Import root and intermediate certificates for the HTML Access Agent

   If the root certificate and intermediate certificates in the certificate chain are not imported with the SSL certificate that you imported for the HTML Access Agent, you must import these certificates into the Windows local computer certificate store.

   a. In the MMC console, expand the Certificates (Local Computer) node and go to the **Trusted Root Certification Authorities > Certificates** folder.

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

      - If your root certificate is not in this folder, proceed to step b.

   b. Right-click the **Trusted Root Certification Authorities > Certificates** folder and click **All Tasks > Import**.

   c. In the Certificate Import wizard, click **Next** and browse to the location where the root CA certificate is stored.

   d. Select the root CA certificate file and click **Open**.

   e. Click **Next**, click **Next**, and click **Finish**.

f. If your server certificate was signed by an intermediate CA, import all intermediate certificates in the certificate chain into the Windows local computer certificate store.

    1) Go to the **Certificates (Local Computer) > Intermediate Certification Authorities > Certificates** folder.

    2) Repeat steps c through f for each intermediate certificate that must be imported.

4. In the certificate MMC window, navigate to the Certificates (Local Computer) > Personal > Certificates folder.

5. Double-click the CA-signed certificate that you imported into the Windows certificate store.

6. In the Certificates dialog box, click the Details tab, scroll down, and select the Thumbprint icon.

7. Copy the selected thumbprint to a text file.

   For example:

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

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

Create Post Sysprep Script/Batch File on Gold Pattern Image and Copy Certificate

Windows 7 and Later

Use post build configuration script “SetupComplete.cmd “to import the SSL certificate and configure the VMware HTML Access registry.

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

For example:

- Copy the SSL certificate file under C: drive. For this example, the “C:\desktone_ca_cert” file.
- Create a file SetupComplete.cmd under "%WINDIR%\Setup\Scripts\" folder. Create “Scripts” folder if it does not exist.
- Add following commands in SetupComplete.cmd file. The thumbprint value is what you copied in Step 1.
- Note that if you have root certificate and intermediate certificates in the certificate chain, then you need to add appropriate CertUtil commands in batch file.

```
CertUtil  -importPFX -f  -p "<password>" "C:\desktone_ca_cert.pfx"

        reg add "HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config" /f /v "SslHash" /t REG_SZ /d "31 2a 32 50 1a 0b 34 b1 65 46 13 a8 0a 5e f7 43 6e a9 2c 3e"

del /F /Q "C:\desktone_ca_cert.pfx"

del /F /Q "%systemroot%\setup\scripts\SetupComplete.cmd"
```

- Save the SetupComplete.cmd file. You can test the SetupComplete.cmd file on test machine.

Windows XP

- Follow the Desktone post sysprep command execution approach to import the SSL certificate and configure the VMware HTML Access registry.
- Install the Administration Tools Pack for Windows XP as the CertUtil tool is not available with the OS install.

  http://www.microsoft.com/en-us/download/details.aspx?id=16770

  For example:

  - Copy the SSL certificate file under C: drive. For this example, the `C:\desktone_ca_cert.pfx` file.
  - Create a folder path `C:\Sysprep\i386\$OEM$\`
  - Now create `postprep-extra.bat` file under `C:\Sysprep\i386\$OEM$\` and add the following commands in the batch file. The thumbprint value is the one you recorded above after importing the certificate.
  - Note that if you have root certificate and intermediate certificates in the certificate chain, then you need to add appropriate CertUtil commands in the vbatch file.

    ```
    CertUtil  -importPFX -f  -p "<password>" "C:\desktone_ca_cert.pfx"

    del /F /Q "C:\desktone_ca_cert.pfx.pfx"

    reg add "HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config" /f /v "SslHash" /t
    REG_SZ /d "31 2a 32 50 1a 0b 34 b1 65 46 13 a8 0a 5e f7 43 6e a9 2c 3e"
    ```

  - Save the postprep-extra.bat file. You do not need a command to delete the batch `postprep-extra.bat` file as sysprep deletes the `C:\Sysprep` folder after successful deployment.
  - You can test the `SetupComplete.cmd` file on the test machine.

Convert Image to Gold Pattern or Reseal

Procedure

1. Convert the image as a gold pattern or reseal, and create a pool.
2. Verify the HTML Access connection for the certificate, or check certificates and HTML Access registry on desktops.

Note: If the HTML Access (Blast) service generates the self-signed certificate even after you set the valid CA certificate as described above, then you can troubleshoot this issue by looking at the logs located here: %ProgramData%\VMWare\Vmware Blast\Blast-worker.txt