Using VMware Horizon View Client for Windows

Horizon View 5.3

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001158-00
You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com
Contents

Using VMware Horizon View Client for Windows  5

1 System Requirements and Setup for Windows-Based View Clients  7
   System Requirements for Windows Clients  7
   Hardware Requirements for Local Mode Desktops  9
   Requirements for Using Multimedia Redirection (MMR)  10
   Supported View Desktop Operating Systems  11
   Requirements for Using Microsoft Lync with Horizon View Client  11
   Client Browser Requirements for View Portal  12
   Smart Card Authentication Requirements  12
   Preparing View Connection Server for View Client  13
   View Client Data Collected by VMware  13

2 Installing View Client for Windows  15
   Install the Windows-Based View Client or View Client with Local Mode  15
   Install View Client by Using View Portal  16
   Configure the View Client Download Links Displayed in View Portal  18
   Installing View Client Silently  19

3 Configuring View Client for End Users  25
   Using URIs to Configure View Client  25
   Configuring Certificate Checking for End Users  29
   Running View Client from the Command Line  31

4 Managing Server Connections and Desktops  35
   Log In to a View Desktop  35
   Switch Desktops  37
   Log Off or Disconnect from a Desktop  38

5 Working in a View Desktop  39
   Feature Support Matrix  39
   Internationalization  41
   Connect USB Devices  41
   Configure Clients to Reconnect When USB Devices Restart  42
   Copying and Pasting Text and Images  43
   Printing from a View Desktop  44
   Control Adobe Flash Display  45
   Using the Relative Mouse Feature for CAD and 3D Applications  46

6 Working with Desktops in Local Mode  47
   Checking Out a Local Mode Desktop for the First Time  47
Using VMware Horizon View Client for Windows

This guide, Using VMware Horizon View Client for Windows, provides information about installing and using VMware® Horizon View™ software on a Microsoft Windows client system to connect to a View desktop in the datacenter.

The information in this document includes system requirements and instructions for installing and using Horizon View Client for Windows.

This information is intended for administrators who need to set up a Horizon View deployment that includes Microsoft Windows client systems, such as desktops and laptops. The information is written for experienced system administrators who are familiar with virtual machine technology and datacenter operations.
System Requirements and Setup for Windows-Based View Clients

Systems running View client components must meet certain hardware and software requirements.

View Client on Windows systems uses Microsoft Internet Explorer Internet settings, including proxy settings, when connecting to View Connection Server. Ensure that your Internet Explorer settings are accurate and that you can access the View Connection Server URL through Internet Explorer. You can use Internet Explorer 7, 8, or 9.

This chapter includes the following topics:

- “System Requirements for Windows Clients,” on page 7
- “Hardware Requirements for Local Mode Desktops,” on page 9
- “Requirements for Using Multimedia Redirection (MMR),” on page 10
- “Supported View Desktop Operating Systems,” on page 11
- “Requirements for Using Microsoft Lync with Horizon View Client,” on page 11
- “Client Browser Requirements for View Portal,” on page 12
- “Smart Card Authentication Requirements,” on page 12
- “Preparing View Connection Server for View Client,” on page 13
- “View Client Data Collected by VMware,” on page 13

System Requirements for Windows Clients

You can install View Client for Windows on PCs or laptops that use a Microsoft Windows 8, Windows 7, Vista, or XP operating system.

The PC or laptop on which you install View Client, and the peripherals it uses, must meet certain system requirements.

**Model**
Standard x86 or x86 64-bit compatible desktop or laptop computer

**Memory**
At least 1GB of RAM

**Operating systems**

<table>
<thead>
<tr>
<th>OS</th>
<th>Version</th>
<th>SP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 8 Desktop</td>
<td>32- or 64-bit</td>
<td>N/A</td>
</tr>
<tr>
<td>Windows 7</td>
<td>32- or 64-bit</td>
<td>None or SP1</td>
</tr>
<tr>
<td>Windows XP</td>
<td>32-bit</td>
<td>SP3</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>32-bit</td>
<td>SP1 or SP2</td>
</tr>
</tbody>
</table>
For Windows 7 and Windows Vista, the following editions are supported: Home, Enterprise, Professional/Business, and Ultimate. For Windows XP, Home and Professional editions are supported.

For Windows 8, the following editions are supported: Windows 8 Pro - Desktop and Windows 8 Enterprise - Desktop.

### View Connection Server, Security Server, and View Agent

4.6.1 or later

If client systems connect from outside the corporate firewall, VMware recommends that you use a security server. With a security server, client systems will not require a VPN connection.

### Display protocol for Horizon View

PCoIP or RDP

### Hardware Requirements for PCoIP

- x86-based processor with SSE2 extensions, with a 800MHz or higher processor speed.
- ARM processor with NEON (preferred) or WMMX2 extensions, with a 1Ghz or higher processor speed.
- Available RAM above system requirements to support various monitor setups. Use the following formula as a general guide:

  \[20MB + (24 \times (# \text{ monitors}) \times \text{monitor width} \times \text{monitor height})\]

  As a rough guide, you can use the following calculations:
  
  - 1 monitor: 1600 x 1200: 64MB
  - 2 monitors: 1600 x 1200: 128MB
  - 3 monitors: 1600 x 1200: 256MB

### Hardware Requirements for RDP

- x86-based processor with SSE2 extensions, with a 800MHz or higher processor speed.
- ARM processor with NEON (preferred) or WMMX2 extensions, with a 600MHz or higher processor speed.
- 128MB RAM.

### Software Requirements for RDP

- RDC 6.0 or later is required for multiple monitors.
- For Windows XP and Windows XP Embedded systems, use Microsoft RDC 6.x.
- Windows Vista includes RDC 6.x, though RDC 7 is recommended.
- Windows 7 includes RDC 7. Windows 7 SP1 includes RDC 7.1.
- For Windows XP desktop virtual machines, you must install the RDP patches listed in Microsoft Knowledge Base (KB) articles 323497 and 884020. If you do not install the RDP patches, a Windows Sockets failed error message might appear on the client.
- The View Agent installer configures the local firewall rule for inbound RDP connections to match the current RDP port of the host operating system, which is typically 3389. If you change the RDP port number, you must change the associated firewall rules.

You can download RDC versions from the Microsoft Web site.
Hardware Requirements for Local Mode Desktops

When you check out a View desktop to run on your local computer, the hardware on the client computer must support both the local system and the virtual machine that now runs on it.

**PC Hardware**

Table 1-1 describes the hardware requirements for various View desktop operating systems.

<table>
<thead>
<tr>
<th>Client Computer Requirement</th>
<th>Description</th>
</tr>
</thead>
</table>
| PC                          | x86 64-compatible  
|                             | LAHF/SAHF support in long mode |
| Number of CPUs              | Multiprocessor systems are supported |
| CPU speed                   | For a Windows XP local desktop, 1.3GHz or faster; 1.6GHz recommended  
|                             | For a Windows 7 or 8 desktop, 1.3GHz or faster; for Aero effects, 2.0GHz or faster |
| Intel processors            | Pentium 4, Pentium M (with PAE), Core, Core 2, Core i3, Core i5, and Core i7 processors  
|                             | For Windows 7 or 8 Aero: Intel Dual Core |
| AMD processors              | Athlon, Athlon MP, Athlon XP, Athlon 64, Athlon X2, Duron, Opteron, Turion X2, Turion 64, Sempron, Phenom, and Phenom II  
|                             | The AMD CPU must have segment-limit support in long mode.  
|                             | For Windows 7 or 8 Aero: Athlon 4200+ and above |
| 64-bit operating systems on View desktops | Intel Pentium 4 and Core 2, and Core i7 processors with EM64T and Intel Virtualization Technology  
|                             | The Intel CPU must have VT-x support enabled in the host system BIOS. The BIOS settings that must be enabled for VT-x support vary depending on the system vendor. See the VMware knowledge base article at http://kb.vmware.com/kb/1003944 for information about how to determine if VT-x support is enabled.  
|                             | Most AMD64 processors (except the earliest revision C Opteron processors) |
| GPU for Windows 7 or 8 Aero | nVidia GeForce 8800GT and above  
|                             | ATI Radeon HD 2600 and above |

Although the operating system on the client computer can be 32-bit or 64-bit, the hardware must be 64-bit compatible and must have the Intel or AMD virtualization assist technologies enabled to run a View desktop with a 64-bit operating system. If these requirements are met, you should be able to run a View desktop with a 64-bit operating system on a client that has either a 32-bit or 64-bit operating system.

**Disk Space**

If you use a default setup for the operating system in the View desktop, the actual disk space needs are approximately the same as those for installing and running the operating system and applications on a physical computer.

For example, Microsoft recommends 16GB of hard disk space for a machine that runs a 32-bit Windows 7 or 8 operating system. If you configure a 16GB virtual hard disk for a 32-bit Windows 7 or 8 virtual machine, only the amount of disk space actually used is downloaded when you check out the local desktop. For a desktop that is allocated 16GB, the actual download size might be 7GB.
After the desktop is downloaded, the amount of disk space used can grow to 16GB if you configured a 16GB hard disk. Because a snapshot is taken during replication, an additional equivalent amount of disk space is required. For example, if 7GB of disk space is currently being used for the local desktop, the snapshot consumes an additional 7GB on the client computer.

IDE and SCSI hard drives are supported.

**Memory**

You need enough memory to run the host operating system on the client computer, plus the memory required for the View desktop’s operating system and for applications on the client computer and the View desktop. VMware recommends that you have 2GB and above for Windows XP and Windows Vista, and 3GB and above for Windows 7 or 8. For more information on memory requirements, see your guest operating system and application documentation.

The total amount of memory you can assign to all virtual machines running on a single computer is limited only by the amount of RAM on the computer. The maximum amount of memory for each View desktop on 64-bit computers is 32GB.

**Display**

A 32-bit display adapter is recommended. 3D benchmarks, such as 3DMark ’06, might not render correctly or at all when running Windows Vista or Windows 7 or 8 virtual machines on some graphics hardware.

View Client with Local Mode supports DirecX9c, which becomes enabled automatically on client systems with capable GPUs. DirecX9c includes 3D capabilities such as Google Earth with 3D building turned on, Windows 7 or 8 Aero effects, and some 3D games.

To play video at 720p or higher requires a multiprocessor system.

For CPU and GPU requirements to support Windows 7 or 8 Aero, see Table 1-1.

**Requirements for Using Multimedia Redirection (MMR)**

Multimedia redirection (MMR) delivers the multimedia stream directly to client computers by using a virtual channel.

With MMR, the multimedia stream is processed, that is, encoded and decoded, on the client system. Local hardware formats and plays media content, thereby offloading the demand on the ESX/ESXi host.

View Client and View Client with Local Mode support MMR on the following operating systems:

- Windows XP
- Windows XP Embedded
- Windows Vista

The MMR feature supports the media file formats that the client system supports, since local decoders must exist on the client. File formats include MPEG2-1, MPEG-2, MPEG-4 Part 2; WMV 7, 8, and 9; WMA; AVI; ACE; MP3; and WAV, among others.

Use Windows Media Player 10 or later, and install it on both the local computer, or client access device, and the View desktop.

You must add the MMR port as an exception to your firewall software. The default port for MMR is 9427.

**NOTE** The View Client video display hardware must have overlay support for MMR to work correctly.

Windows 7 and 8 clients and Windows 7 and 8 View desktops do not support MMR. For these clients and agents, use Windows media redirection, included with RDP 7 and later.
Supported View Desktop Operating Systems

Administrators create virtual machines with a guest operating system and install View Agent in the guest operating system. End users can log in to these virtual machines from a client device.

For a list of the supported guest operating systems, see the “Supported Operating Systems for View Agent” topic in the Horizon View 4.6.x or 5.x installation documentation.

Requirements for Using Microsoft Lync with Horizon View Client

With Horizon View 5.2, customers can now use a Microsoft Lync 2013 client on their View desktops to participate in Unified Communications (UC) VoIP (voice over IP) and video chat calls with Lync certified USB audio and video devices. A dedicated IP phone is no longer required.

This new architecture requires the installation of a Microsoft Lync 2013 client on the View desktop and a Microsoft Lync VDI plug-in on the client endpoint. Customers can use the Microsoft Lync 2013 client for presence, instant messaging, Web conferencing, and Microsoft Office functionality.

Whenever a Lync VoIP or video chat call occurs, the Lync VDI plug-in offloads all the media processing from the datacenter server to the client endpoint, and encodes all media into Lync-optimized audio and video codecs. This optimized architecture is highly scalable, results in lower network bandwidth used, and provides point-to-point media delivery with support for high-quality real-time VoIP and video.

**NOTE** Recording audio is not yet supported. This integration is supported only with the PCoIP display protocol.

This feature has the following requirements.

**Operating system**
- Client operating system: Full support for 32- or 64-bit Windows 7 SP1
- 32-bit and 64-bit Windows 8 is a Tech Preview.
- Virtual machine (agent) operating system: 32- or 64-bit Windows 7 SP1

**Client system software**
- Horizon View Client for Windows 5.3
- 32-bit version of Microsoft Lync VDI Plug-in

**View desktop (agent) software**
- Horizon View Agent 5.2
- Microsoft Lync 2013 Client
  - The Lync 2013 client bit-level should match the bit-level of the virtual machine operating system.
- Security certificate generated during Microsoft Lync Server 2013 deployment must be imported into the Trusted Root Certificate Authorities directory

**Required servers**
- A server running View Connection Server 5.2
- A server running Microsoft Lync Server 2013

**IMPORTANT** The 64-bit version of Microsoft Office must not be installed on the client machine. The 32-bit Microsoft Lync VDI plugin that is required is not compatible with 64-bit Microsoft Office 2013.
A vSphere infrastructure to host the virtual machines
The vCenter Server and ESXi hosts must be running vSphere 5.0 or later.

Hardware
- Hardware that supports each of the required software components previously listed
- Client endpoint: 1.5GHz or faster CPU and a minimum of 2GB of RAM for the Microsoft Lync 2013 Plug-in

Client Browser Requirements for View Portal
From a client system, you can open a browser and browse to a View Connection Server instance. The Web page that appears is called View Portal, and it contains links for downloading the installer file for View Client.

To use View Portal, you must have one of the following Web browsers:
- Internet Explorer 8
- Internet Explorer 9
- Internet Explorer 10 (from a Windows 8 system in Desktop mode)
- Firefox 6 and later releases
- Safari 5 (on a Mac)
- Chrome 14 or later

Smart Card Authentication Requirements
Client systems that use a smart card for user authentication must meet certain requirements.

Each client system that uses a smart card for user authentication must have the following software and hardware:
- View Client
- A Windows-compatible smart card reader
- Smart card middleware
- Product-specific application drivers

You must also install product-specific application drivers on the View desktops.

View supports smart cards and smart card readers that use a PKCS#11 or Microsoft CryptoAPI provider. You can optionally install the ActivIdentity ActivClient software suite, which provides tools for interacting with smart cards.

Users that authenticate with smart cards must have a smart card or USB smart card token, and each smart card must contain a user certificate.

To install certificates on a smart card, you must set up a computer to act as an enrollment station. This computer must have the authority to issue smart card certificates for users, and it must be a member of the domain you are issuing certificates for.

IMPORTANT When you enroll a smart card, you can choose the key size of the resulting certificate. To use smart cards with local desktops, you must select a 1024-bit or 2048-bit key size during smart card enrollment. Certificates with 512-bit keys are not supported.

The Microsoft TechNet Web site includes detailed information on planning and implementing smart card authentication for Windows systems.
In addition to meeting these requirements for View Client systems, other View components must meet certain configuration requirements to support smart cards:

- For information about configuring View servers to support smart card use, see the topic “Configure Smart Card Authentication,” in the *VMware Horizon View Administration* document.
- For information on tasks you might need to perform in Active Directory to implement smart card authentication, see the topics about preparing Active Directory for smart card authentication, in the *VMware Horizon View Installation* document.

**Preparing View Connection Server for View Client**

Administrators must perform specific tasks to enable end users to connect to View desktops.

Before end users can connect to View Connection Server or a security server and access a View desktop, you must configure certain pool settings and security settings:

- If you are using a security server, as VMware recommends, verify that you are using View Connection Server 4.6.1 and View Security Server 4.6.1 or later. See the *VMware Horizon View Installation* documentation.
- If you plan to use a secure tunnel connection for client devices and if the secure connection is configured with a DNS host name for View Connection Server or a security server, verify that the client device can resolve this DNS name.

To enable or disable the secure tunnel, in View Administrator, go to the Edit View Connection Server Settings dialog box and use the check box called **Use secure tunnel connection to desktop**.

- Verify that a virtual desktop pool has been created and that the user account that you plan to use is entitled to access this View desktop. See the topics about creating desktop pools in the *VMware Horizon View Administration* documentation.
- To use two-factor authentication with View Client, such as RSA SecurID or RADIUS authentication, you must enable this feature on View Connection Server. RADIUS authentication is available with View 5.1 or later View Connection Server. For more information, see the topics about two-factor authentication in the *VMware Horizon View Administration* documentation.

**View Client Data Collected by VMware**

If your company participates in the customer experience improvement program, VMware collects data from certain Horizon View Client fields. Fields containing sensitive information are made anonymous.

**Note**  This feature is available only if your Horizon View deployment uses View Connection Server 5.1 or later. Client information is sent for View Client 2.0 and later clients.

VMware collects data on the clients to prioritize hardware and software compatibility. If your company’s administrator has opted to participate in the customer experience improvement program, VMware collects anonymous data about your deployment in order to improve VMware’s response to customer requirements. No data that identifies your organization is collected. View Client information is sent first to View Connection Server and then on to VMware, along with data from Horizon View servers, desktop pools, and View desktops.

Although the information is encrypted during while in transit to View Connection Server, the information on the client system is logged unencrypted in a user-specific directory. The logs do not contain any personally identifiable information.

To participate in the VMware customer experience improvement program, the administrator who installs View Connection Server can opt in while running the View Connection Server installation wizard, or an administrator can set an option in View Administrator after the installation.
### Table 1-2. Data Collected from View Clients for the Customer Experience Improvement Program

<table>
<thead>
<tr>
<th>Description</th>
<th>Is This Field Made Anonymous?</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company that produced the View Client application</td>
<td>No</td>
<td>VMware</td>
</tr>
<tr>
<td>Product name</td>
<td>No</td>
<td>VMware Horizon View Client</td>
</tr>
<tr>
<td>Client product version</td>
<td>No</td>
<td>The format is \textit{x.x.x-yyyyyy}, where \textit{x.x.x} is the client version number and \textit{yyyyyy} is the build number.</td>
</tr>
<tr>
<td>Client binary architecture</td>
<td>No</td>
<td>Examples include the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\begin{itemize}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item i386</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item x86_64</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item arm</td>
</tr>
<tr>
<td>Client build name</td>
<td>No</td>
<td>Examples include the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\begin{itemize}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item VMware-wswc-viewclient-x86_64</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item VMware-Horizon-View-Client-Linux</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item VMware-Horizon-View-Client-iOS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item VMware-Horizon-View-Client-Mac</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item VMware-Horizon-View-Client-Android</td>
</tr>
<tr>
<td>Host operating system</td>
<td>No</td>
<td>Examples include the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\begin{itemize}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item Windows 7, 64-bit Service Pack 1 (Build 7601)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item iPhone OS 5.1.1 (9B206)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item Ubuntu 10.04.4 LTS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item Mac OS X 10.7.5 (11G63)</td>
</tr>
<tr>
<td>Host operating system kernel</td>
<td>No</td>
<td>Examples include the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\begin{itemize}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item Windows 6.1.7601 SP1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item Darwin Kernel Version 11.0.0: Sun Apr 8 21:52:26 PDT 2012; rootxnu-1878.11.10-1/RELEASE_ARM_S5L8945X</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item Darwin 11.4.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item Linux 2.6.32-44-generic #98-Ubuntu SMP Mon Sep 24 17:27:10 UTC 2012</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item unknown (for Windows Store)</td>
</tr>
<tr>
<td>Host operating system architecture</td>
<td>No</td>
<td>Examples include the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\begin{itemize}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item x86_64</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item i386</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item armv71</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item ARM</td>
</tr>
<tr>
<td>Host system model</td>
<td>No</td>
<td>Examples include the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\begin{itemize}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item Dell Inc. OptiPlex 960</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item iPad3,3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item MacBookPro8,2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item Dell Inc. Precision WorkStation T3400 (A04 03/21/2008)</td>
</tr>
<tr>
<td>Host system CPU</td>
<td>No</td>
<td>Examples include the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\begin{itemize}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item unknown (for iPad)</td>
</tr>
<tr>
<td>Number of cores in the host system's processor</td>
<td>No</td>
<td>For example: 4</td>
</tr>
<tr>
<td>MB of memory on the host system</td>
<td>No</td>
<td>Examples include the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\begin{itemize}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item 4096</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\item unknown (for Windows Store)</td>
</tr>
</tbody>
</table>
Installing View Client for Windows

You can obtain the Windows-based View Client installer either from the VMware Web site or from View Portal, a Web access page provided by View Connection Server. You can set various startup options for end users after View Client is installed.

This chapter includes the following topics:

- “Install the Windows-Based View Client or View Client with Local Mode,” on page 15
- “Install View Client by Using View Portal,” on page 16
- “Configure the View Client Download Links Displayed in View Portal,” on page 18
- “Installing View Client Silently,” on page 19

Install the Windows-Based View Client or View Client with Local Mode

End users open View Client to connect to their virtual desktops from a physical machine. You can run a Windows-based installer file to install all components of View Client.

View Client with Local Mode lets end users download a copy of their virtual desktop to their local computer. End users can then use the virtual desktop even when they do not have a network connection. Latency is minimized and performance is enhanced.

View Client with Local Mode is the fully supported feature that in earlier releases was an experimental feature called View Client with Offline Desktop.

This procedure describes installing View Client by using an interactive installation wizard. If instead you would like to use the command-line, silent installation feature of the Microsoft Windows Installer (MSI), see “Install View Client Silently,” on page 20.

Prerequisites

- Verify that the client system uses a supported operating system. See “System Requirements for Windows Clients,” on page 7.
- Verify that you can log in as an administrator on the client system.
- Verify that View Agent is not installed.
- Local mode prerequisites:
  - Verify that your license includes View Client with Local Mode.
  - Verify that none of the following products is installed: VMware Horizon View Client, VMware Player, VMware Workstation, VMware ACE, VMware Server.
Prerequisites for USB redirection:

- Determine whether the person who uses the client device is allowed to access locally connected USB devices from a virtual desktop. If not, you can either deselect the **USB Redirection** component that the wizard presents or install the component but disable it using GPOs.

  VMware recommends that you always install the **USB Redirection** component and use GPOs to control USB access. This way, if you later want to enable USB redirection for a client, you will not need to re-install View Client. For information, see the topic “View Client Configuration ADM Template Settings” in the chapter about configuring policies in the *VMware Horizon View Administration* document.

- If you plan to install the **USB Redirection** component, verify that the Windows Automatic Update feature is not turned off on the client computer.

- Determine whether to use the feature that lets end users log in to View Client and their virtual desktop as the currently logged in user. Credential information that the user entered when logging in to the client system is passed to the View Connection Server instance and ultimately to the virtual desktop. Some client operating systems do not support this feature.

- If you do not want to require end users to supply the fully qualified domain name (FQDN) of the View Connection Server instance that hosts their virtual machine, determine the FQDN so that you can supply it during installation.

**Procedure**

1. Log in to the client system as a user with administrator privileges.
2. On the client system, download the View Client installer file from the Horizon View Client Downloads page at [http://www.vmware.com/go/viewclients](http://www.vmware.com/go/viewclients). Select the appropriate installer file, where $xxxxxx$ is the build number and $y.y.y$ is the version number.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Client on 64-bit operating</td>
<td>Select <em>VMware-viewclient-x86_64-y.y.y-xxxxxx.exe</em> for View Client.</td>
</tr>
<tr>
<td>systems</td>
<td>Select <em>VMware-viewclientwithlocalmode-x86_64-y.y.y-xxxxxx.exe</em> for</td>
</tr>
<tr>
<td></td>
<td>View Client with Local mode.</td>
</tr>
<tr>
<td>View Client on 32-bit operating</td>
<td>Select <em>VMware-viewclient-y.y.y-xxxxxx.exe</em> for View Client.</td>
</tr>
<tr>
<td>systems</td>
<td>Select <em>VMware-viewclientwithlocalmode-y.y.y-xxxxxx.exe</em> for View</td>
</tr>
<tr>
<td></td>
<td>Client with Local Mode.</td>
</tr>
</tbody>
</table>

3. To start the View Client installation program, double-click the installer file.
4. Follow the prompts to install the components you want.

The VMware View Client service is installed on the Windows client computer. The service name for View Client is `wsnm`. The service names for the USB components are `VMUSBArbService` and `vmware-view-usbd`.

**What to do next**

Start the View Client and verify that you can log in to the correct virtual desktop. See “**Log In to a View Desktop**,” on page 35 or “**Install View Client by Using View Portal**,” on page 16.

**Install View Client by Using View Portal**

An expedient way of downloading and installing the View Client or View Client with Local Mode application is to open a browser and browse to the View Portal Web page. You can use View Portal to download the full View Client installer for both Windows and Mac client computers.

As an alternative to browsing to a VMware Download page to download View Client, you can browse to a View Connection Server URL. You can also configure settings so that the links on View Portal point to a different location than the VMware Download page.
Prerequisites

- If the links on View Portal must point to a different location than the VMware Downloads page, see “Configure the View Client Download Links Displayed in View Portal,” on page 18.
- Verify that you have the URL for the View Connection Server instance.
- Verify that you can log in as an administrator on the client system.
- Verify that the client system uses a supported operating system. See “System Requirements for Windows Clients,” on page 7.
- Verify that View Agent is not installed.
- Local mode prerequisites:
  - Verify that your license includes View Client with Local Mode.
  - Verify that none of the following products is installed: VMware Horizon View Client, VMware Player, VMware Workstation, VMware ACE, VMware Server.
- Prerequisites for USB redirection:
  - Determine whether the person who uses the client device is allowed to access locally connected USB devices from a virtual desktop. If not, you can either deselect the USB Redirection component that the wizard presents or install the component but disable it using GPOs.
    VMware recommends that you always install the USB Redirection component and use GPOs to control USB access. This way, if you later want to enable USB redirection for a client, you will not need to re-install View Client. For information, see the topic “View Client Configuration ADM Template Settings” in the chapter about configuring policies in the VMware Horizon View Administration document.
  - If you plan to install the USB Redirection component, verify that the Windows Automatic Update feature is not turned off on the client computer.

Procedure

1. Log in to the client system as a user with administrator privileges.
2. Open a browser and enter the URL of the View Connection Server instance that provides access to the virtual desktop.
   In the URL, be sure to use https rather than http.
3. Click the appropriate link for the type of operating system you have (32-bit or 64-bit) and the type of View Client to install (with or without Local Mode).
4. When prompted, save the installer file to your client system.
5. To start the View Client installation program, double-click the installer file.
6. Follow the prompts to install the components you want.

What to do next

Connect to the View desktop. See “Log In to a View Desktop,” on page 35.
Configure the View Client Download Links Displayed in View Portal

By default, when you open a browser and enter the URL of a View Connection Server instance, the View Portal page that appears contains links to the VMware Download site for downloading View Client. You can change the default.

The default View Client links on View Portal ensure that you are directed to the latest compatible View Client installers. In some cases, however, you might want to have the links point to an internal Web server, or you might want to make specific client versions available on your own View Connection Server. You can reconfigure the page to point to a different URL.

**IMPORTANT** If you customize the View Portal links, as described in this topic, and later install VMware Horizon View HTML Access on the server, your customized View Portal page is replaced by an HTML Access page.

**Prerequisites**

- Download the installer files for the types of View Client you want to use in your environment. The URL to the View Clients download page is https://www.vmware.com/go/viewclients.
- Determine which HTTP server will host the installer files. The files can reside on a View Connection Server instance or on another HTTP server.

**Procedure**

1. On the HTTP server where the installer files will reside, create a folder for the installer files.
   
   For example, to place the files in a `downloads` folder on the View Connection Server host, in the default installation directory, use the following path:
   
   C:\Program Files\VMware\VMware View\Server\broker\webapps\downloads
   
   The links to the files would then use URLs with the format https://server-name/downloads/client-installer-file-name. For example, a server with the name view.mycompany.com would use the following URL for View Client for Windows: https://view.mycompany.com/downloads/VMware-viewclient.exe. In this example, the folder named downloads is located in the webapps root folder.

2. Copy the View Client installer files into the folder.
   
   If the folder resides on View Connection Server, you can replace any files in this folder without having to restart the VMware View Connection Server service.

3. On the View Connection Server machine, copy the `portal-links.properties` file and the `portal.properties` file located in `install-path\Server\Extras\PortalExamples`.

4. Create a `portal` folder the directory C:\ProgramData\VMware\VDM, and copy the `portal-links.properties` and `portal.properties` files into the `portal` folder.

5. Edit C:\ProgramData\VMware\VDM\portal\portal-links.properties file to point to the new location of the installer files.
   
   You can edit the lines in this file and add to them if you need to create more links. You can also delete lines.

   The following examples show properties for creating two links for View Client for Windows and two links for View Client for Linux:

   ```properties
   link.win=https://server-name/downloads/VMware-viewclient-x86_64-y.y.y-XXXX.exe#win
   link.win.1=https://server-name/downloads/VMware-viewclient-y.y.y-XXXX.exe#win
   link.linux=https://server-name/downloads/VMware-viewclient-x86_64-y.y.y-XXXX.rpm#linux
   link.linux.1=https://server-name/downloads/VMware-viewclient-y.y.y-XXXX.tar.gz#linux
   ```
In this example, \textit{y.y.y-XXXX} indicates the version and build number. The \textit{win} text at the end of the line indicates that this link should appear in the browser if the client has a Windows operating system. Use \textit{win} for Windows, \textit{linux} for Linux, and \textit{mac} for Mac OS X.

6 Edit \texttt{C:\ProgramData\VMware\VDM\portal\portal.properties} file to specify the text to display for the links. These lines appear in the section of the file called \textit{# keys based on key names in portal-links.properties}.

The following example shows the text that corresponds to the links specified for \textit{link.win} and \textit{link.win.1}:

\begin{verbatim}
1:
text.win=View Client for Windows 32 bit Client users
text.win.1=View Client for Windows 64 bit Client users
\end{verbatim}

7 Restart the VMware View Connection Server service.

When end users enter the URL for View Connection Server, they see links with the text you specified. The links point to the locations you specified.

\section*{Installing View Client Silently}

You can install View Client silently by typing the installer filename and installation options at the command line. With silent installation, you can efficiently deploy View components in a large enterprise.

\subsection*{Set Group Policies to Allow Silent Installation of View Client with Local Mode}

Before you can install View Client with Local Mode silently, you must configure Microsoft Windows group policies to allow installation with elevated privileges.

You do not have to set these group policies to install View Client silently. These policies are required only for View Client with Local Mode.

You must set Windows Installer group policies for computers and for users on the client computer.

\subsection*{Prerequisites}

Verify that you have administrator privileges on the Windows client computer on which you will install View Client with Local Mode.

\subsection*{Procedure}

1 Log in to the client computer and click \textbf{Start} > \textbf{Run}.

2 Type \texttt{gpedit.msc} and click \textit{OK}.

3 In the Group Policy Object Editor, click \textbf{Local Computer Policy} > \textbf{Computer Configuration}.

4 Expand \textit{Administrative Templates}, expand \textit{Windows Components}, open the \textit{Windows Installer} folder, and double-click \textit{Always install with elevated privileges}.

5 In the \textit{Always Install with Elevated Privileges Properties} window, click \textit{Enabled} and click \textit{OK}.

6 In the left pane, click \textit{User Configuration}.

7 Expand \textit{Administrative Templates}, expand \textit{Windows Components}, open the \textit{Windows Installer} folder, and double-click \textit{Always install with elevated privileges}.

8 In the \textit{Always Install with Elevated Privileges Properties} window, click \textit{Enabled} and click \textit{OK}.

\subsection*{What to do next}

Install View Client with Local Mode silently.
Install View Client Silently

You can use the silent installation feature of the Microsoft Windows Installer (MSI) to install View Client or View Client with Local Mode on several Windows computers. In a silent installation, you use the command line and do not have to respond to wizard prompts.

Prerequisites

- Verify that the client system uses a supported operating system. See “System Requirements for Windows Clients,” on page 7.
- Verify that you can log in as an administrator on the client system.
- Verify that View Agent is not installed.
- Local mode prerequisites:
  - Verify that the Windows Installer group policies that are required for silent installation are configured on the client computer. See “Set Group Policies to Allow Silent Installation of View Client with Local Mode,” on page 19.
  - Verify that your license includes View Client with Local Mode.
  - Verify that none of the following products is installed: VMware Horizon View Client, VMware Player, VMware Workstation, VMware ACE, VMware Server.
- Determine whether to use the feature that lets end users log in to View Client and their virtual desktop as the currently logged in user. Credential information that the user entered when logging in to the client system is passed to the View Connection Server instance and ultimately to the virtual desktop. Some client operating systems do not support this feature.
- Familiarize yourself with the MSI installer command-line options. See “Microsoft Windows Installer Command-Line Options,” on page 22.
- Familiarize yourself with the silent installation (MSI) properties available with View Client. See “Silent Installation Properties for View Client,” on page 21.
- Determine whether to allow end users to access locally connected USB devices from their virtual desktops. If not, set the MSI property, `ADDLOCAL`, to the list of features of interest and omit the USB feature. For details, see “Silent Installation Properties for View Client,” on page 21.
- If you do not want to require end users to supply the fully qualified domain name (FQDN) of the View Connection Server instance that hosts their virtual machine, determine the FQDN so that you can supply it during installation.

Procedure

1. On the client system, download the View Client installer file from the VMware product page at http://www.vmware.com/products/.
   Select the appropriate installer file, where `xxxxx` is the build number and `y.y.y` is the version number.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Client on 64-bit operating systems</td>
<td>Select <code>VMware-viewclient-x86_64-y.y-y-xxxxx.exe</code> for View Client. Select <code>VMware-viewclientwithlocalmode-x86_64-y.y-y-xxxxx.exe</code> for View Client with Local mode.</td>
</tr>
<tr>
<td>View Client on 32-bit operating systems</td>
<td>Select <code>VMware-viewclient-y.y-y-xxxxx.exe</code> for View Client. Select <code>VMware-viewclientwithlocalmode-y.y-y-xxxxx.exe</code> for View Client with Local mode.</td>
</tr>
</tbody>
</table>

2. Open a command prompt on the Windows client computer.
3  Type the installation command on one line.

This example installs View Client with single sign-on and USB redirection features. A default View
Connection Server instance is configured for View Client users: `VMware-viewclient-y.y.y-
xxxxxx.exe /s /v"/qn REBOOT=ReallySuppress VDM_SERVER=cs1.companydomain.com
ADDLOCAL=Core,TSSO,USB"

This example installs View Client with Local Mode: `VMware-viewclientwithlocal-y.y.y-
xxxxxx.exe /s /v"/qn ADDLOCAL=Core,MVDI"

**Note**  The Core feature is mandatory.

The VMware View Client service is installed on the Windows client computer.

**What to do next**

Start the View Client and verify that you can log in to the correct virtual desktop. See “Log In to a View
Desktop,” on page 35 or “Install View Client by Using View Portal,” on page 16.

**Silent Installation Properties for View Client**

You can include specific properties when you silently install View Client from the command line. You must
use a `PROPERTY=value` format so that Microsoft Windows Installer (MSI) can interpret the properties and values.

Table 2-1 shows the View Client silent installation properties that you can use at the command-line.

**Table 2-1. MSI Properties for Silently Installing View Client**

<table>
<thead>
<tr>
<th>MSI Property</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTALLDIR</td>
<td>The path and folder in which the View Client software is installed.</td>
<td>%ProgramFiles%/VMware/VMware View\Client</td>
</tr>
<tr>
<td></td>
<td>For example: <code>INSTALLDIR=&quot;D:\abc\my folder&quot;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The sets of two double quotes that enclose the path permit the MSI</td>
<td></td>
</tr>
<tr>
<td></td>
<td>installer to interpret the space as a valid part of the path.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This MSI property is optional.</td>
<td></td>
</tr>
<tr>
<td>VDM_SERVER</td>
<td>The fully qualified domain name (FQDN) of the View Connection Server instance to which View Client users connect by default. When you configure this property, View Client users do not have to supply this FQDN. For example: <code>VDM_SERVER=cs1.companydomain.com</code></td>
<td>None</td>
</tr>
<tr>
<td>DESKTOP_SHORTCUT</td>
<td>Configures a desktop shortcut icon for View Client. A value of 1 installs the shortcut. A value of 0 does not install the shortcut. This MSI property is optional.</td>
<td>1</td>
</tr>
<tr>
<td>QUICKLAUNCH_SHORTCUT</td>
<td>Configures a shortcut icon on the quick-launch tray for View Client. A value of 1 installs the shortcut. A value of 0 does not install the shortcut. This MSI property is optional.</td>
<td>1</td>
</tr>
<tr>
<td>STARTMENU_SHORTCUT</td>
<td>Configures a shortcut for View Client in the Start menu. A value of 1 installs the shortcut. A value of 0 does not install the shortcut. This MSI property is optional.</td>
<td>1</td>
</tr>
</tbody>
</table>

In a silent installation command, you can use the MSI property, `ADDLOCAL=`, to specify features that the View Client installer configures. Each silent-installation feature corresponds to a setup option that you can select during an interactive installation.
Table 2-2 shows the View Client features you can type at the command line and the corresponding interactive-installation options.

### Table 2-2. View Client Silent Installation Features and Interactive Custom Setup Options

<table>
<thead>
<tr>
<th>Silent Installation Feature</th>
<th>Custom Setup Option in an Interactive Installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core</td>
<td>During an interactive installation, the core View Client functions are installed by default.</td>
</tr>
<tr>
<td>MVDI</td>
<td>When you install View Client with Local Mode interactively, the MVDI functions are installed by default.</td>
</tr>
<tr>
<td>ThinPrint</td>
<td>Virtual Printing</td>
</tr>
<tr>
<td>TSSO</td>
<td>Single Sign-on (SSO)</td>
</tr>
<tr>
<td>USB</td>
<td>USB Redirection</td>
</tr>
</tbody>
</table>

Microsoft Windows Installer Command-Line Options

To install View components silently, you must use Microsoft Windows Installer (MSI) command-line options and properties. The View component installers are MSI programs and use standard MSI features. You can also use MSI command-line options to uninstall View components silently.

For details about MSI, see the Microsoft Web site. For MSI command-line options, see the Microsoft Developer Network (MSDN) Library Web site and search for MSI command-line options. To see MSI command-line usage, you can open a command prompt on the View component computer and type `msiexec /?`.

To run a View component installer silently, you begin by disabling the bootstrap program that extracts the installer into a temporary directory and starts an interactive installation.

Table 2-3 shows the command-line options that control the installer’s bootstrap program.

### Table 2-3. Command-Line Options for a View Component’s Bootstrap Program

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/s</td>
<td>Disables the bootstrap splash screen and extraction dialog, which prevents the display of interactive dialogs. For example: <code>VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s</code> The /s option is required to run a silent installation. In the examples, <code>xxxxx</code> is the build number and <code>y.y.y</code> is the version number.</td>
</tr>
<tr>
<td>/v&quot;MSI_command_line_options&quot;</td>
<td>Instructs the installer to pass the double-quote-enclosed string that you enter at the command line as a set of options for MSI to interpret. You must enclose your command-line entries between double quotes. Place a double quote after the /v and at the end of the command line. For example: <code>VMware-viewagent-y.y.y-xxxxxx.exe /s /v&quot;command_line_options&quot;</code> To instruct the MSI installer to interpret a string that contains spaces, enclose the string in two sets of double quotes. For example, you might want to install the View component in an installation path name that contains spaces. For example: <code>VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v&quot;command_line_options&quot; INSTALLDIR=&quot;d:\abc\my folder&quot;&quot;</code> In this example, the MSI installer passes on the installation-directory path and does not attempt to interpret the string as two command-line options. Note the final double quote that encloses the entire command line. The <code>/v&quot;command_line_options&quot;</code> option is required to run a silent installation.</td>
</tr>
</tbody>
</table>
You control the remainder of a silent installation by passing command-line options and MSI property values to the MSI installer, `msiexec.exe`. The MSI installer includes the View component's installation code. The installer uses the values and options that you enter in the command line to interpret installation choices and setup options that are specific to the View component.

Table 2-4 shows the command-line options and MSI property values that are passed to the MSI installer.

<table>
<thead>
<tr>
<th>MSI Option or Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/qn</code></td>
<td>Instructs the MSI installer not to display the installer wizard pages. For example, you might want to install View Agent silently and use only default setup options and features: <code>VMware-viewagent-y.y.y-xxxxxx.exe /s /v&quot;/qn&quot;</code> In the examples, <code>xxxxxx</code> is the build number and <code>y.y.y</code> is the version number. Alternatively, you can use the <code>/qb</code> option to display the wizard pages in a noninteractive, automated installation. As the installation proceeds, the wizard pages are displayed, but you cannot respond to them. The <code>/qn</code> or <code>/qb</code> option is required to run a silent installation.</td>
</tr>
<tr>
<td><code>INSTALLDIR</code></td>
<td>Specifies an alternative installation path for the View component. Use the format <code>INSTALLDIR=path</code> to specify an installation path. You can ignore this MSI property if you want to install the View component in the default path. This MSI property is optional.</td>
</tr>
<tr>
<td><code>ADDLOCAL</code></td>
<td>Determines the component-specific features to install. In an interactive installation, the View installer displays custom setup options to select. The MSI property, ADDLOCAL, lets you specify these setup options on the command line. To install all available custom setup options, enter <code>ADDLOCAL=ALL</code> For example: <code>VMware-viewagent-y.y.y-xxxxxx.exe /s /v&quot;/qn ADDLOCAL=ALL&quot;</code> If you do not use the MSI property, ADDLOCAL, the default setup options are installed. To specify individual setup options, enter a comma-separated list of setup option names. Do not use spaces between names. Use the format <code>ADDLOCAL=value,value,value,...</code>. For example, you might want to install View Agent in a guest operating system with the View Composer Agent and PCoIP features: <code>VMware-viewagent-y.y.y-xxxxxx.exe /s /v&quot;/qn ADDLOCAL=Core,SVIAgent,PCoIP&quot;</code> **Note*: The Core feature is required in View Agent. This MSI property is optional.</td>
</tr>
<tr>
<td><code>REBOOT</code></td>
<td>You can use the <code>REBOOT=ReallySuppress</code> option to allow system configuration tasks to complete before the system reboots. This MSI property is optional.</td>
</tr>
<tr>
<td><code>/l*v log_file</code></td>
<td>Writes logging information into the specified log file with verbose output. For example: <code>/l*v &quot;&quot;%TEMP\vmmsi.log&quot;&quot;</code> This example generates a detailed log file that is similar to the log generated during an interactive installation. You can use this option to record custom features that might apply uniquely to your installation. You can use the recorded information to specify installation features in future silent installations. The <code>/l*v</code> option is optional.</td>
</tr>
</tbody>
</table>
Configuring View Client for End Users

View Client provides several configuration mechanisms to simplify the login and desktop selection experience for end users, but also to enforce security policies.

This chapter includes the following topics:
- “Using URIs to Configure View Client,” on page 25
- “Configuring Certificate Checking for End Users,” on page 29
- “Running View Client from the Command Line,” on page 31

Using URIs to Configure View Client

Using uniform resource identifiers (URIs), you can create a Web page or an email with links that end users click to launch View Client, connect to View Connection Server, and launch a specific desktop with specific configuration options.

You can simplify the process of logging in to a View desktop by creating Web or email links for end users. You create these links by constructing URIs that provide some or all of the following information, so that your end users do not need to supply it:

- View Connection Server address
- Port number for View Connection Server
- Active Directory user name
- RADIUS or RSA SecurID user name, if different from Active Directory user name
- Domain name
- Desktop display name
- Window size
- Desktop actions including reset, log off, and roll back
- Display protocol
- Options for redirecting USB devices

**IMPORTANT** To use this feature you must have View Client 5.1 or later.

To construct a URI, you use the `vmware-view` URI scheme with View Client specific path and query parts.

**NOTE** You can use URIs to launch View Client only if View Client is already installed on end users’ client computers.
Syntax for Creating vmware-view URIs

Syntax includes the vmware-view URI scheme, a path part to specify the desktop, and, optionally, a query to specify desktop actions or configuration options.

VMware View URI Specification

Use the following syntax to create URIs for launching View Client:

`vmware-view://[authority-part] [/path-part] [?query-part]`

The only required element is the URI scheme, vmware-view. For some versions of some client operating systems, the scheme name is case-sensitive. Therefore, use vmware-view.

**IMPORTANT** In all parts, non-ASCII characters must first be encoded according to UTF-8 [STD63], and then each octet of the corresponding UTF-8 sequence must be percent-encoded to be represented as URI characters.

For information about encoding for ASCII characters, see the URL encoding reference at http://www.w3schools.com/tags/ref_urlencode.asp.

**authority-part** Specifies the server address and, optionally, a user name, a non-default port number, or both. Server names must conform to DNS syntax.

To specify a user name, use the following syntax:

```text
user1@server-address
```

Note that you cannot specify a UPN address, which includes the domain. To specify the domain, you can use the `domainName` query part in the URI.

To specify a port number, use the following syntax:

```text
server-address:port-number
```

**path-part** Specifies the desktop. Use the desktop display name. If the display name has a space in it, use the `%20` encoding mechanism to represent the space.

**query-part** Specifies the configuration options to use or the desktop actions to perform. Queries are not case-sensitive. To use multiple queries, use an ampersand (&) between the queries. If queries conflict with each other, the last query in the list is used. Use the following syntax:

```text
query1=value1[&query2=value2...]
```

Supported Queries

This topic lists the queries that are supported for this type of View Client. If you are creating URIs for multiple types of clients, such as desktop clients and mobile clients, see the *Using VMware Horizon View Client* guide for each type of client system.

**action**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>browse</code></td>
<td>Displays a list of available desktops hosted on the specified server. You</td>
</tr>
<tr>
<td></td>
<td>are not required to specify a desktop when using this action.</td>
</tr>
<tr>
<td><code>start-session</code></td>
<td>Launches the specified desktop. If no action query is provided and the</td>
</tr>
<tr>
<td></td>
<td>desktop name is provided, <strong>start-session</strong> is the default action.</td>
</tr>
</tbody>
</table>
Table 3-1. Values That Can Be Used with the action Query (Continued)

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reset</td>
<td>Shuts down and restarts the specified desktop. Unsaved data is lost. Resetting a View desktop is the equivalent of pressing the Reset button on a physical PC.</td>
</tr>
<tr>
<td>logoff</td>
<td>Logs the user out of the guest operating system in the View desktop.</td>
</tr>
<tr>
<td>rollback</td>
<td>Discards changes made to the specified desktop while it was checked out for use in local mode on a Windows PC or laptop.</td>
</tr>
</tbody>
</table>

connectUSBOnInsert  Connects a USB device to the foreground desktop when you plug in the device. This query is implicitly set if you specify the unattended query. To use this query, you must set the action query to start-session or else not have an action query. Valid values are Yes and No. An example of the syntax is connectUSBOnInsert=yes.

connectUSBOnStartup Redirects all USB devices to the desktop that are currently connected to the client system. This query is implicitly set if you specify the unattended query. To use this query, you must set the action query to start-session or else not have an action query. Valid values are Yes and No. An example of the syntax is connectUSBOnStartup=yes.

desktopLayout Sets the size of the window that displays the View desktop. To use this query, you must set the action query to start-session or else not have an action query.

Table 3-2. Valid Values for the desktopLayout Query

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fullscreen</td>
<td>Full screen on one monitor. This is the default.</td>
</tr>
<tr>
<td>multimonitor</td>
<td>Full screen on all monitors.</td>
</tr>
<tr>
<td>windowLarge</td>
<td>Large window.</td>
</tr>
<tr>
<td>windowSmall</td>
<td>Small window.</td>
</tr>
<tr>
<td>WxH</td>
<td>Custom resolution, where you specify the width by height, in pixels. An example of the syntax is desktopLayout=1280x800.</td>
</tr>
</tbody>
</table>

desktopProtocol Valid values are RDP and PCoIP. For example, to specify PCoIP, use the syntax desktopProtocol=PCoIP.

domainName The domain associated with the user who is connecting to the View desktop.

tokenUserName Specifies the RSA or RADIUS user name. Use this query only if the RSA or RADIUS user name is different from the Active Directory user name. If you do not specify this query and RSA or RADIUS authentication is required, the Windows user name is used. The syntax is tokenUserName=name.

unattended Creates a server connection in kiosk mode. If you use this query, do not specify user information.
Examples of vmware-view URIs

You can create hypertext links or buttons with the vmware-view URI scheme and include these links in email or on a Web page. Your end users can click these links to, for example, launch a particular View desktop with the startup options you specify.

URI Syntax Examples

Each URI example is followed by a description of what the end user sees after clicking the URI link.

1  vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session

View Client is launched and connects to the view.mycompany.com server. The login box prompts the user for a user name, domain name, and password. After a successful login, the client connects to the desktop whose display name is displayed as Primary Desktop, and the user is logged in to the guest operating system.

**Note** The default display protocol and window size are used. The default display protocol is PCoIP. The default window size is full screen.

2  vmware-view://view.mycompany.com:7555/Primary%20Desktop

This URI has the same effect as the previous example, except that it uses the nondefault port of 7555 for View Connection Server. (The default port is 443.) Because a desktop identifier is provided, the desktop is launched even though the start-session action is not included in the URI.

3  vmware-view://fred@view.mycompany.com/Finance%20Desktop?desktopProtocol=PCoIP

View Client is launched and connects to the view.mycompany.com server. In the login box, the User name text box is populated with the name fred. The user must supply the domain name and password. After a successful login, the client connects to the desktop whose display name is displayed as Finance Desktop, and the user is logged in to the guest operating system. The connection uses the PCoIP display protocol.

4  vmware-view://fred@view.mycompany.com/Finance%20Desktop?domainName=mycompany

View Client is launched and connects to the view.mycompany.com server. In the login box, the User name text box is populated with the name fred, and the Domain text box is populated with mycompany. The user must supply only a password. After a successful login, the client connects to the desktop whose display name is displayed as Finance Desktop, and the user is logged in to the guest operating system.

5  vmware-view://view.mycompany.com/

View Client is launched, and the user is taken to the login prompt for connecting to the view.mycompany.com server.

6  vmware-view://view.mycompany.com/Primary%20Desktop?action=reset

View Client is launched and connects to the view.mycompany.com server. The login box prompts the user for a user name, domain name, and password. After a successful login, View Client displays a dialog box that prompts the user to confirm the reset operation for Primary Desktop. After the reset occurs, depending on the type of View Client, the user might see a message indicating whether the reset was successful.

**Note** This action is available only if the View administrator has enabled this feature for end users.

7  vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session&connectUSBOnStartup=true

This URI has the same effect as the first example, and all USB devices connected to the client system are redirected to the View desktop.
View Client is launched, and the user is taken to the page for entering the address of a View Connection Server instance.

**HTML Code Examples**

You can use URIs to make hypertext links and buttons to include in emails or on Web pages. The following examples show how to use the URI from the first URI example to code a hypertext link that says, **Test Link**, and a button that says, **TestButton**.

```html
<html>
<body>
  <a href="vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session">Text Link</a><br>
  <form><input type="button" value="TestButton" onClick="window.location.href='vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session'"></form><br>
</body>
</html>
```

**Configuring Certificate Checking for End Users**

Administrators can configure the certificate verification mode so that, for example, full verification is always performed.

Certificate checking occurs for SSL connections between View Connection Server and View Client. Administrators can configure the verification mode to use one of the following strategies:

- End users are allowed to choose the verification mode. The rest of this list describes the three verification modes.
- (No verification) No certificate checks are performed.
- (Warn) End users are warned if a self-signed certificate is being presented by the server. Users can choose whether or not to allow this type of connection.
- (Full security) Full verification is performed and connections that do not pass full verification are rejected.

For details about the types of verification checks performed, see “Certificate Checking Modes for View Client,” on page 30.

Use the Client Configuration ADM template file to set the verification mode. ADM template files for View components are installed in the `install_directory\VMware\VMware View\Server\Extras\GroupPolicyFiles` directory on your View Connection Server host. For information about using these templates to control GPO settings, see the VMware Horizon View Administration document.

If you do not want to configure this setting as a group policy, you can also enable certificate verification by adding the `CertCheckMode` value name to one of the following registry keys on the client computer:

- For 32-bit Windows: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security`
- For 64-bit Windows: `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security`

Use the following values in the registry key:

- 0 implements Do not verify server identity certificates.
- 1 implements Warn before connecting to untrusted servers.
2 implements Never connect to untrusted servers.

If you configure both the group policy setting and the CertCheckMode setting in the registry key, the group policy setting takes precedence over the registry key value.

Certificate Checking Modes for View Client

Administrators and sometimes end users can configure whether client connections are rejected if any or some server certificate checks fail.

Certificate checking occurs for SSL connections between View Connection Server and View Client. Certificate verification includes the following checks:

- Has the certificate been revoked?
- Is the certificate intended for a purpose other than verifying the identity of the sender and encrypting server communications? That is, is it the correct type of certificate?
- Has the certificate expired, or is it valid only in the future? That is, is the certificate valid according to the computer clock?
- Does the common name on the certificate match the host name of the server that sends it? A mismatch can occur if a load balancer redirects View Client to a server with a certificate that does not match the host name entered in View Client. Another reason a mismatch can occur is if you enter an IP address rather than a host name in the client.
- Is the certificate signed by an unknown or untrusted certificate authority (CA)? Self-signed certificates are one type of untrusted CA.

To pass this check, the certificate's chain of trust must be rooted in the device's local certificate store.

**NOTE**  For instructions on distributing a self-signed root certificate to all Windows client systems in a domain, see the topic called “Add the Root Certificate to Trusted Root Certification Authorities” in the *VMware Horizon View Installation* document.

When you use View Client to log in to a desktop, if your administrator has allowed it, you can click **Configure SSL** to set the certificate checking mode. You have three choices:

- **Never connect to untrusted servers.** If any of the certificate checks fails, the client cannot connect to the server. An error message lists the checks that failed.

- **Warn before connecting to untrusted servers.** If a certificate check fails because the server uses a self-signed certificate, you can click **Continue** to ignore the warning. For self-signed certificates, the certificate name is not required to match the View Connection Server name you entered in View Client.

  You can also receive a warning if the certificate has expired.

- **Do not verify server identity certificates.** This setting means that View does not perform any certificate checking.

If the certificate checking mode is set to **Warn**, you can still connect to a View Connection Server instance that uses a self-signed certificate.

If an administrator later installs a security certificate from a trusted certificate authority, so that all certificate checks pass when you connect, this trusted connection is remembered for that specific server. In the future, if that server ever presents a self-signed certificate again, the connection fails. After a particular server presents a fully verifiable certificate, it must always do so.

**IMPORTANT**  When you use a checked-out View desktop on your local system, if you are connected to the corporate network, certificate checking occurs as described when you log in to your View desktop. If you are not connected to the corporate network, no certificate checking can be done. The View desktop runs just as if certificate checking succeeded.
Running View Client from the Command Line

You can run View Client for Windows from the command line or from scripts. You might want to do this if you are implementing a kiosk-based application that grants end users access to desktop applications.

You use the `wswc` command to run the View Client for Windows from the command line. The command includes options that you can specify to change the behavior of View Client.

**View Client Command Usage**

The syntax of the `wswc` command controls the operation of View Client.

Use the following form of the `wswc` command from a Windows command prompt.

```
wswc [command_line_option [argument]] ...
```

By default, the path to the `wswc` command executable file is `C:\Program Files\VMware\VMware View\Client\bin`. For your convenience, add this path to your `PATH` environment variable.

Table 3-3 shows the command-line options that you can use with the `wswc` command.

### Table 3-3. View Client Command-Line Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/?</td>
<td>Displays the list of command options.</td>
</tr>
<tr>
<td>--checkin</td>
<td>(Local Desktop only) Checks in the specified desktop and unlocks the online equivalent. This option requires that you also specify the <code>--desktopName</code> option.</td>
</tr>
<tr>
<td>--checkout</td>
<td>(Local Desktop only) Checks out the specified desktop, and locks the online equivalent. This option requires that you also specify the <code>--desktopName</code> option.</td>
</tr>
<tr>
<td>--confirmRollback</td>
<td>(Local Desktop only) Suppresses the confirmation dialog box that appears when you use the <code>--rollback</code> option. To perform rollback in non-interactive mode, also specify the <code>--nonInteractive</code> option.</td>
</tr>
<tr>
<td>--connectUSBOnStartup</td>
<td>When set to <code>true</code>, redirects all USB devices to the desktop that are currently connected to the host. This option is implicitly set if you specify the <code>--unattended</code> option. The default is <code>false</code>.</td>
</tr>
<tr>
<td>--connectUSBOnInsert</td>
<td>When set to <code>true</code>, connects a USB device to the foreground desktop when you plug in the device. This option is implicitly set if you specify the <code>--unattended</code> option. The default is <code>false</code>.</td>
</tr>
<tr>
<td>--desktopLayout window_size</td>
<td>Specifies how to display the window for the desktop:</td>
</tr>
<tr>
<td></td>
<td><code>fullscreen</code> Full screen display</td>
</tr>
<tr>
<td></td>
<td><code>multimonitor</code> Multiple-monitor display</td>
</tr>
<tr>
<td></td>
<td><code>windowLarge</code> Large window</td>
</tr>
<tr>
<td></td>
<td><code>windowSmall</code> Small window</td>
</tr>
<tr>
<td>--desktopName desktop_name</td>
<td>Specifies the name of the desktop as it would appear in the Select Desktop dialog box. This is the name as you see it in the select desktop dialog.</td>
</tr>
<tr>
<td>--desktopProtocol protocol</td>
<td>Specifies the desktop protocol to use as it would appear in the Select Desktop dialog box. The protocol can be PCOIP or RDP.</td>
</tr>
<tr>
<td>--domainName domain_name</td>
<td>Specifies the domain that the end user uses to log in to View Client.</td>
</tr>
<tr>
<td>--file file_path</td>
<td>Specifies the path of a configuration file that contains additional command options and arguments. See &quot;View Client Configuration File,&quot; on page 33.</td>
</tr>
</tbody>
</table>
Table 3-3. View Client Command-Line Options (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-languageId Locale_ID</td>
<td>Provides localization support for different languages in View Client. If a resource library is available, specify the Locale ID (LCID) to use. For US English, enter the value 0x409.</td>
</tr>
<tr>
<td>-localDirectory directory_path</td>
<td>(Local Desktop only) Specifies which directory on the local system to use for downloading the local desktop. The downloaded local files are stored directly in the specified directory. By contrast, if the local directory is selected in View Client, a subfolder with the desktop name is created under the selected directory and local files are stored in that subfolder. This option requires that you also specify the -desktopName option.</td>
</tr>
<tr>
<td>-logInAsCurrentUser</td>
<td>When set to true, uses the credential information that the end user provides when logging in to the client system to log in to the View Connection Server instance and ultimately to the View desktop. The default is false.</td>
</tr>
<tr>
<td>-nonInteractive</td>
<td>Suppresses error message boxes when starting View Client from a script. This option is implicitly set if you specify the -unattended option.</td>
</tr>
<tr>
<td>-password password</td>
<td>Specifies the password that the end user uses to log in to View Client. You do not need to specify this option for clients in kiosk mode if you generate the password automatically.</td>
</tr>
<tr>
<td>-printEnvironmentInfo</td>
<td>Displays the IP address, MAC address, and machine name of the client device.</td>
</tr>
<tr>
<td>-rollback</td>
<td>(Local Desktop only) Unlocks the online version of a checked out desktop and discards the local session. This option requires that you also specify the -desktopName option. To perform rollback in non-interactive mode, also specify the -nonInteractive option and the -confirmRollback option.</td>
</tr>
<tr>
<td>-serverURL connection_server</td>
<td>Specifies the URL, IP address, or FQDN of the View Connection Server instance.</td>
</tr>
<tr>
<td>-smartCardPIN PIN</td>
<td>Specifies the PIN when an end user inserts a smart card to login.</td>
</tr>
<tr>
<td>-standalone</td>
<td>Launches a second instance of the View Client that can connect to the same or a different View Connection Server over PCoIP. For multiple desktop connections to the same server, using the secure tunnel is not supported. For multiple desktop connections to different servers, the secure tunnel is supported. Note: The second desktop connection might not have access to local hardware, such as USB devices, smart cards, printers, and multiple monitors.</td>
</tr>
<tr>
<td>-unattended</td>
<td>Runs View Client in a noninteractive mode that is suitable for clients in kiosk mode. You must also specify:</td>
</tr>
<tr>
<td></td>
<td>■ The account name of the client, if you did not generate the account name from the MAC address of the client device. The name must begin with the string “custom-” or an alternate prefix that you have configured in ADAM.</td>
</tr>
<tr>
<td></td>
<td>■ The password of the client, if you did not generate a password automatically when you set up the account for the client.</td>
</tr>
<tr>
<td></td>
<td>The -unattended option implicitly sets the -nonInteractive, -connectUSBOnStartup, and -connectUSBOnInsert options.</td>
</tr>
<tr>
<td>-userName user_name</td>
<td>Specifies the account name that the end user uses to log in to View Client. You do not need to specify this option for clients in kiosk mode if you generate the account name from the MAC address of the client device.</td>
</tr>
</tbody>
</table>

Options that you specify on the command line or in the configuration file take precedence over any global system policies that you have defined, which in turn override user policies.

You can specify all options by Active Directory group policies except for -checkin, -checkout, -file, -languageId, -localDirectory, -printEnvironmentInfo, -rollback, -smartCardPIN, and -unattended.
View Client Configuration File

You can read command-line options for View Client from a configuration file.

You can specify the path of the configuration file as an argument to the `-f` option of the `wswc` command. The file must be a Unicode (UTF-16) or ASCII text file.

**Example: Example of a Configuration File for a Noninteractive Application**

The following example shows the contents of a configuration file for a noninteractive application.

```
-`serverURL https://view.yourcompany.com
-`userName autouser
-`password auto123
-`domainName companydomain
-`desktopName autodesktop
-`nonInteractive
```

**Example: Example of a Configuration File for a Client in Kiosk Mode**

The following example shows a client in kiosk mode whose account name is based on its MAC address. The client has an automatically generated password.

```
-`serverURL 145.124.24.100
-`unattended
```

View Client Registry Settings

You can define default settings for the View Client in the Windows registry instead of specifying these settings on the command line.

Table 3-4 shows the registry settings for View Client. All the settings are located under `HKLM\Software\VMware, Inc.\VMware VDM\Client\` in the registry.

Policy entries take precedence over registry settings, and command-line settings take precedence over policy entries.

<table>
<thead>
<tr>
<th>Registry Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainName</td>
<td>Specifies the default domain name.</td>
</tr>
<tr>
<td>EnableShade</td>
<td>Specifies whether the menu bar (shade) at the top of the View Client window is enabled. The menu bar is enabled by default except for clients in kiosk mode. A value of false disables the menu bar.</td>
</tr>
<tr>
<td>Password</td>
<td>Specifies the default password.</td>
</tr>
<tr>
<td>ServerURL</td>
<td>Specifies the default View Connection Server instance by its URL, IP address, or FQDN.</td>
</tr>
<tr>
<td>UserName</td>
<td>Specifies the default user name.</td>
</tr>
</tbody>
</table>

View Client Exit Codes

The command-line interface for View Client can return exit codes to indicate the nature of any error that View Client encounters.

Table 3-5 shows the exit codes that the `wswc` command can return.
### Table 3-5. View Client Exit Codes

<table>
<thead>
<tr>
<th>Exit Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>Fatal error in kiosk mode.</td>
</tr>
<tr>
<td>0</td>
<td>Success.</td>
</tr>
<tr>
<td>1</td>
<td>Connection failed.</td>
</tr>
<tr>
<td>2</td>
<td>Login failed.</td>
</tr>
<tr>
<td>3</td>
<td>Desktop failed to start.</td>
</tr>
<tr>
<td>4</td>
<td>RDP failed to start.</td>
</tr>
<tr>
<td>5</td>
<td>RDP operation failed.</td>
</tr>
<tr>
<td>6</td>
<td>Tunnel connection lost.</td>
</tr>
<tr>
<td>7</td>
<td>Local desktop transfer failure.</td>
</tr>
<tr>
<td>8</td>
<td>Local desktop check-in failure.</td>
</tr>
<tr>
<td>9</td>
<td>Local desktop check-out failure.</td>
</tr>
<tr>
<td>10</td>
<td>Local desktop rollback failure.</td>
</tr>
<tr>
<td>11</td>
<td>Unknown result received during authentication.</td>
</tr>
<tr>
<td>12</td>
<td>Authentication error.</td>
</tr>
<tr>
<td>13</td>
<td>Received request to use an unknown authentication method.</td>
</tr>
<tr>
<td>14</td>
<td>Invalid server response.</td>
</tr>
<tr>
<td>15</td>
<td>Desktop was disconnected.</td>
</tr>
<tr>
<td>16</td>
<td>Tunnel was disconnected.</td>
</tr>
<tr>
<td>17</td>
<td>Reserved for future development.</td>
</tr>
<tr>
<td>18</td>
<td>Reserved for future development.</td>
</tr>
<tr>
<td>19</td>
<td>Unsupported kiosk operation.</td>
</tr>
<tr>
<td>20</td>
<td>Remote mouse, keyboard, or screen (RMKS) connection error.</td>
</tr>
<tr>
<td>21</td>
<td>PIN error.</td>
</tr>
<tr>
<td>22</td>
<td>PIN mismatch.</td>
</tr>
<tr>
<td>23</td>
<td>Password mismatch.</td>
</tr>
<tr>
<td>24</td>
<td>View Connection Server error.</td>
</tr>
<tr>
<td>25</td>
<td>Desktop was not available.</td>
</tr>
</tbody>
</table>
Use View Client to connect to View Connection Server or a security server and log in to or off of a View desktop. For troubleshooting purposes, you can also reset a View desktop assigned to you and roll back a desktop you checked out.

Depending on how the administrator configures policies for View desktops, end users might be able to perform many operations on their desktops.

This chapter includes the following topics:
- “Log In to a View Desktop,” on page 35
- “Switch Desktops,” on page 37
- “Log Off or Disconnect from a Desktop,” on page 38

Log In to a View Desktop

Before you have end users access their virtual desktops, test that you can log in to a virtual desktop from a client device. You can start View Client from the Start menu or a desktop shortcut on the client system.

In environments where a network connection is available, the user session is authenticated by View Connection Server.

Prerequisites

- Obtain the credentials you need to log in, such as a user name and password, RSA SecurID user name and passcode, RADIUS authentication user name and passcode, or smart card personal identification number (PIN).
- Obtain the domain name for logging in.
- Perform the administrative tasks described in “Preparing View Connection Server for View Client,” on page 13.
- If you are outside the corporate network and are not using a security server to access the virtual desktop, verify that your client device is set up to use a VPN connection and turn that connection on.

**IMPORTANT** VMware recommends using a security server rather than a VPN.

- Verify that you have the fully qualified domain name (FQDN) of the server that provides access to the virtual desktop. You also need the port number if the port is not 443.
- If you plan to use the RDP display protocol to connect to a View desktop, verify that the AllowDirectRDP View Agent group policy setting is enabled.
- If your administrator has allowed it, you can configure the certificate checking mode for the SSL certificate presented by View Connection Server.
To determine which mode to use, see “Certificate Checking Modes for View Client,” on page 30.

**Procedure**

1. Double-click the VMware Horizon View Client desktop shortcut or click **Start > Programs > VMware > VMware Horizon View Client**.

2. In the **Connection Server** drop-down menu, enter the host name of View Connection Server or a security server.

3. Verify that the other optional settings in the dialog box appear as you configured them.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log in as current user</strong></td>
<td>This check box is displayed or hidden according to the global setting in View Administrator. Do not select this check box if you plan to check out the View desktop for use in local mode.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>If you leave this field blank, the default port 443 is used. <strong>Autoconnect</strong> If you select this check box, the next time you start View Client, the <strong>Connection Server</strong> field is disabled and you are connected to the server specified when you selected the <strong>Autoconnect</strong> check box. To deselect this check box, cancel the next dialog box that appears and click <strong>Options</strong> to display and change this setting.</td>
</tr>
<tr>
<td><strong>Configure SSL</strong></td>
<td>If your View administrator has allowed it, you can set the certificate checking mode by clicking this link, as mentioned in the prerequisites to this procedure.</td>
</tr>
</tbody>
</table>

4. Click **Connect**.

   You might see a message that you must confirm before the login dialog box appears.

5. If you are prompted for RSA SecurID credentials or RADIUS authentication credentials, enter the user name and passcode and click **Continue**.

6. Enter the credentials of a user who is entitled to use at least one desktop pool, select the domain, and click **Login**.

   If you type the user name using the format `user@domain`, the name is treated as a user principal name (UPN) because of the @ sign, and the domain drop-down menu is disabled.

   For information about creating desktop pools and entitling users to pools, see *VMware Horizon View Administration* document.

7. In the list of desktops that appears, select a desktop.

   a. (Optional) In the **Display** drop-down menu, select the window size for displaying the View desktop. The display setting is retained as the default the next time you open the desktop.

   b. (Optional) To select a display protocol, click the down-arrow next to a desktop in the list, click **Display Protocol**, and select the protocol.

      This choice is available only if your View administrator has enabled it. PCoIP provides an optimized PC experience for the delivery of images, audio, and video content on the LAN or across the WAN.

      **Note**: If you are using smart card credentials to log in and you want to switch protocols, you must log off and log on again.

      The protocol setting is retained as the default the next time you open the desktop.

8. Click **Connect**.

   You are connected to the desktop.
After you are connected, the client window appears.

If authentication to View Connection Server fails or if View Client cannot connect to a desktop, perform the following tasks:

- Determine whether View Connection Server is configured not to use SSL. View Client requires SSL connections. Check whether the global setting in View Administrator for the **Use SSL for client connections** check box is deselected. If so, you must either select the check box, so that SSL is used, or set up your environment so that clients can connect to an HTTPS enabled load balancer or other intermediate device that is configured to make an HTTP connection to View Connection Server.

- Verify that the security certificate for View Connection Server is working properly. If it is not, in View Administrator, you might also see that the View Agent on desktops is unreachable and the Transfer Server status shows that it is not ready. These are symptoms of additional connection problems caused by certificate problems.

- Verify that the tags set on the View Connection Server instance allow connections from this user. See the VMware Horizon View Administration document.

- Verify that the user is entitled to access this desktop. See the VMware Horizon View Administration document.

- If you are using the RDP display protocol to connect to a View desktop, verify that the client computer allows remote desktop connections.

**What to do next**

- Configure startup options.

  If you do not want to require end users to provide the host name of View Connection Server, or if you want to configure other startup options, use the View Client command-line options to create a desktop shortcut.

  See “**Running View Client from the Command Line**,” on page 31.

- Check out a desktop that can be used in local mode.

  End users can determine if a desktop is eligible for checkout by clicking the down-arrow next to the desktop in the list provided by View Client with Local Mode. If the desktop can be used in local mode, the **Check out** option appears in the context menu. Only the user who checks out the desktop can access it, even if a group is entitled to access the desktop.

**Switch Desktops**

If you are connected to a desktop, you can switch to another desktop.

**Procedure**

- From the View desktop menu bar, select **Options > Switch Desktop** and select a desktop to view.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose a View desktop on the same server</td>
<td>If the desktop name is not listed, select <strong>Other Desktop</strong> to choose another desktop from the desktop selection list.</td>
</tr>
<tr>
<td>Choose a View desktop on a different server</td>
<td>If the desktop you want is not on the same server, exit View Client and restart to connect to a different server.</td>
</tr>
</tbody>
</table>
Log Off or Disconnect from a Desktop

If you disconnect from a View desktop without logging off, applications remain open. Even if you do not have a View desktop open, you can log off of the View desktop operating system. Using this feature has the same result as sending Ctrl+Alt+Del to the desktop and then clicking Log Off.

**Note** The Windows key combination Ctrl+Alt+Del is not supported in View desktops. To use the equivalent of pressing Ctrl+Alt+Del, select Desktop > Send Ctrl+Alt+Del from the menu bar. Alternatively, you can press Ctrl+Alt+Insert.

If you are using a View desktop in local mode, you can instead suspend or shut down the desktop, as described in “Shut Down or Suspend a Local Desktop,” on page 48.

**Procedure**

- Disconnect without logging off.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Also quit View Client</td>
<td>Click the Close button in the corner of the window or select Options &gt; Disconnect from the menu bar.</td>
</tr>
<tr>
<td>Choose a different View desktop on the same server</td>
<td>Select Options &gt; Switch Desktop from the menu bar.</td>
</tr>
<tr>
<td>Choose a View desktop on a different server</td>
<td>Exit View Client and restart to connect to a different server.</td>
</tr>
</tbody>
</table>

**Note** Your View administrator can configure your desktop to automatically log off when disconnected. In that case, any open programs in your desktop are stopped.

- Log off and disconnect from a desktop.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>From within the desktop OS</td>
<td>Use the Windows Start menu to log off.</td>
</tr>
<tr>
<td>From the menu bar</td>
<td>Select Options &gt; Disconnect and Log Off. If you use this procedure, files that are open on the View desktop will be closed without being saved first.</td>
</tr>
</tbody>
</table>

- Log off when you do not have a View desktop open.

If you use this procedure, files that are open on the View desktop will be closed without being saved first.

  a. Start View Client, connect to the View Connection Server that provides access to the View desktop, and supply your authentication credentials.

  b. When the desktop selection list appears, click the down-arrow next to the desktop and select Log Off.
Horizon View provides the familiar, personalized desktop environment that end users expect. End users can access USB and other devices connected to their local computer, send documents to any printer that their local computer can detect, authenticate with smart cards, and use multiple display monitors.

This chapter includes the following topics:
- “Feature Support Matrix,” on page 39
- “Internationalization,” on page 41
- “Connect USB Devices,” on page 41
- “Configure Clients to Reconnect When USB Devices Restart,” on page 42
- “Copying and Pasting Text and Images,” on page 43
- “Printing from a View Desktop,” on page 44
- “Control Adobe Flash Display,” on page 45
- “Using the Relative Mouse Feature for CAD and 3D Applications,” on page 46

**Feature Support Matrix**

Many features, such as RSA SecurID authentication, location-based printing, and PCoIP protocol, are supported on most client operating systems. You must also take into consideration whether the feature is supported on the View desktop operating system.

When planning which display protocol and features to make available to your end users, use the following information to determine which client operating systems and agent (View desktop) operating systems support the feature.

The types and editions of the supported guest operating system depend on the Windows version.

<table>
<thead>
<tr>
<th>Guest Operating System</th>
<th>Version</th>
<th>Edition</th>
<th>Service Pack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 8</td>
<td>64-bit and 32-bit</td>
<td>Enterprise and Professional</td>
<td>N/A</td>
</tr>
<tr>
<td>Windows 7</td>
<td>64-bit and 32-bit</td>
<td>Enterprise and Professional</td>
<td>None and SP1</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>32-bit</td>
<td>Business and Enterprise</td>
<td>SP1 and SP2</td>
</tr>
<tr>
<td>Windows XP</td>
<td>32-bit</td>
<td>Professional</td>
<td>SP3</td>
</tr>
<tr>
<td>Guest Operating System</td>
<td>Version</td>
<td>Edition</td>
<td>Service Pack</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------</td>
<td>---------</td>
<td>--------------</td>
</tr>
<tr>
<td>Windows 2008 R2 Terminal Server</td>
<td>64-bit</td>
<td>Standard</td>
<td>SP1</td>
</tr>
<tr>
<td>Windows 2008 Terminal Server</td>
<td>64-bit</td>
<td>Standard</td>
<td>SP2</td>
</tr>
</tbody>
</table>

**Table 5-2. Features Supported on Operating Systems for View Desktops (Where View Agent Is Installed)**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows XP</th>
<th>Windows Vista</th>
<th>Windows 7</th>
<th>Windows 2008</th>
<th>Windows 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB access</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>RDP display protocol</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>PCoIP display protocol</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Persona Management</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Wyse MMR</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location-based printing</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Virtual printing</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Smart cards</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>RSA SecurID or RADIUS</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>N/A</td>
<td>X</td>
</tr>
<tr>
<td>Single sign-on</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Multiple monitors</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>With RDP 7</td>
<td>X</td>
</tr>
<tr>
<td>Local Mode</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

**Table 5-3. Features Supported on Windows-Based View Clients**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows XP</th>
<th>Windows Vista</th>
<th>Windows 7</th>
<th>Windows 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB access</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>RDP display protocol</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>PCoIP display protocol</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Persona Management</td>
<td>X (not with local mode)</td>
<td>X (not with local mode)</td>
<td>X (not with local mode)</td>
<td>X (not with local mode)</td>
</tr>
<tr>
<td>Wyse MMR</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location-based printing</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Virtual printing</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Smart cards</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>RSA SecurID or RADIUS</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Single sign-on</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Multiple monitors</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Local Mode</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

For information about which editions of each client operating system are supported, or which service packs, see the system requirements topics.

For descriptions of these features and their limitations, see the *VMware Horizon View Architecture Planning* document.
Internationalization

The user interface and documentation are available in English, Japanese, French, German, Simplified Chinese, Traditional Chinese, and Korean.

Connect USB Devices

You can use locally attached USB devices, such as thumb flash drives, cameras, and printers, from a View desktop. This feature is called USB redirection.

When you use this feature, most USB devices that are attached to the local client system become available from a menu in View Client. You use the menu to connect and disconnect the devices.

Using USB devices with View desktops has the following limitations:

- When you access a USB device from a menu in View Client and use the device in a View desktop, you cannot access the device on the local computer.

  **IMPORTANT** For this reason, do not redirect devices such as USB Ethernet devices and touch screen devices. For example, if you redirect a USB Ethernet device, your client system will lose network connectivity. If you redirect a touch screen device, the View desktop will receive touch input but not keyboard input.

- USB devices that do not appear in the menu, but are available in a View desktop, include human interface devices such as keyboards and pointing devices. The View desktop and the local computer use these devices at the same time. Interaction with these devices can sometimes be slow because of network latency.

- Large USB disk drives can take several minutes to appear in the desktop.

- Some USB devices require specific drivers. If a required driver is not already installed on a View desktop, you might be prompted to install it when you connect the USB device to the View desktop.

- If you plan to attach USB devices that use MTP drivers, such as Android-based Samsung smart phones and tablets, you must set View Client to automatically connect USB devices to your View desktop. Otherwise, if you try to manually redirect the USB device by using a menu item, the device will not be redirected unless you unplug the device and then plug it in again.

- Webcams are not supported for USB redirection.

- The redirection of USB audio devices depends on the state of the network and is not reliable. Some devices require a high data throughput even when they are idle.

You can connect USB devices to a View desktop either manually or automatically.

**NOTE** Do not redirect USB devices such as USB Ethernet devices and touch screen devices to the virtual desktop. If you redirect a USB Ethernet device, your client system will lose network connectivity. If you redirect a touch screen device, the View desktop will receive touch input but not keyboard input. If you have set your virtual desktop to autoconnect USB devices, you can configure a policy to exclude specific devices. See the topic “Configuring Filter Policy Settings for USB Devices” in the *VMware Horizon View Administration* document.

**IMPORTANT** This procedure tells how to use a VMware Horizon View Client menu item to configure autoconnecting USB devices to a View desktop. You can also configure autoconnecting by using the View Client command-line interface or by creating a group policy.

For more information about the command-line interface, see “Running View Client from the Command Line,” on page 31. For more information about creating group policies, see the *VMware Horizon View Administration* document.
Prerequisites

- To use USB devices with a View desktop, the View administrator must have enabled the USB feature for the View desktop.

This task includes installing the USB Redirection component of View Agent. For instructions, see the chapter about creating and preparing virtual machines, in the VMware Horizon View Administration document.

This task can also include setting group policies to allow USB redirection. For more information, see the sections “USB Settings for the View Agent,” “USB Settings for the View Client,” “Configuring Device Splitting Policy Settings for Composite USB Devices,” and “Configuring Filter Policy Settings for USB Devices” in the VMware Horizon View Administration document.

- When View Client was installed, the USB Redirection component must have been installed. If you did not include this component in the installation, run the installer again to modify the components and include the USB Redirection component.

Procedure

- Manually connect the USB device to a View desktop.
  - a. Connect the USB device to your local client system.
  - b. From the VMware Horizon View Client menu bar, click Connect USB Device.
  - c. Select the USB device.

The device is manually redirected from the local system to the View desktop.

- Configure View Client to connect USB devices automatically to the View desktop when you plug them in to the local system.

  If you plan to connect devices that use MTP drivers, such as Android-based Samsung smart phones and tablets, be sure to use this autoconnect feature.

  - a. Before you plug in the USB device, start View Client and connect to a View desktop.
  - b. From the VMware Horizon View Client menu bar, select Connect USB Device > Autoconnect USB Devices.
  - c. Plug in the USB device.

The USB device appears in the desktop. This might take up to 20 seconds. The first time you connect the device to the desktop you might be prompted to install drivers.

If the USB device does not appear in the desktop after several minutes, disconnect and reconnect the device to the client computer.

What to do next

If you have problems with USB redirection, see the topic about troubleshooting USB redirection problems in the VMware Horizon View Administration document.

Configure Clients to Reconnect When USB Devices Restart

If you do not configure View Client to automatically connect USB devices to your View desktop, you can still configure View Client to reconnect to specific devices that occasionally restart. Otherwise, when a device restarts during an upgrade, the device will connect to the local system rather than to the View desktop.

If you plan to attach a USB device such as a smart phone or tablet, which is automatically restarted during operating system upgrades, you can set View Client to reconnect that specific device to the View desktop. To perform this task, you edit a configuration file on the client.
If you use the Autoconnect USB Devices option in View Client, all devices that you plug in to the client system get redirected to the View desktop. If you do not want all devices to be connected, use the following procedure to configure View Client so that only certain USB devices get automatically reconnected.

**Prerequisites**

Determine the hexadecimal format of the vendor ID (VID) and product ID (PID) of the device. For instructions see the VMware KB article at http://kb.vmware.com/kb/1011600.

**Procedure**

1. Use a text editor to open the config.ini file on the client.

<table>
<thead>
<tr>
<th>OS Version</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7</td>
<td>C:\ProgramData\VMware\VMware USB Arbitration Service\config.ini</td>
</tr>
<tr>
<td>Windows XP</td>
<td>C:\Documents and Settings\All Users\Application Data\VMware\VMware USB Arbitration Service\config.ini</td>
</tr>
</tbody>
</table>

2. Set the slow-reconnect property for the specific device or devices.

   `usb.quirks.device0 = "vid:pid slow-reconnect"`

   Here, `vid:pid` represent the vendor ID and product ID, in hexadecimal format, for the device. For example, the following lines set this property for two USB devices:

   `usb.quirks.device0 = "0x0529:0x0001 slow-reconnect"`
   `usb.quirks.device1 = "0x0601:0x0009 slow-reconnect"

   Specify the `usb.quirks.deviceN` device properties in order, starting from 0. For example, if the line `usb.quirks.device0` is followed by a line with `usb.quirks.device2` rather than `usb.quirks.device1`, only the first line is read.

When devices such as smart phones and tablets undergo a firmware or operating system upgrade, the upgrade will succeed because the device will restart and connect to the View desktop that manages it.

**Copying and Pasting Text and Images**

If your administrator enables the feature, you can copy and paste formatted text and images between a remote View desktop and your client system or between two View desktops. Some restrictions apply.

If you use the PCoIP display protocol and you are using a View 5.x or later View desktop, your View administrator can set this feature so that copy and paste operations are allowed only from your client system to a View desktop, or only from a View desktop to your client system, or both, or neither.

Administrators configure the ability to copy and paste by using group policy objects (GPOs) that pertain to View Agent in View desktops. For more information, see the topic about View PCoIP general session variables in the VMware Horizon View Administration document, in the chapter about configuring policies.

Supported file formats include text, images, and RTF (Rich Text Format). The clipboard can accommodate 1MB of data for copy and paste operations. If you are copying formatted text, some of the data is text and some of the data is formatting information. For example, an 800KB document might use more than 1MB of data when it is copied because more than 200KB of RTF data might get put in the clipboard.

If you copy a large amount of formatted text or text and an image, when you attempt to paste the text and image, you might see some or all of the plain text but no formatting or image. The reason is that the three types of data are sometimes stored separately. For example, depending on the type of document you are copying from, images might be stored as images or as RTF data.
If the text and RTF data together use less than 1MB, the formatted text is pasted. Often the RTF data cannot be truncated, so that if the text and formatting use more than 1MB, the RTF data is discarded, and plain text is pasted.

If you are unable to paste all of the formatted text and images you selected in one operation, you might need to copy and paste smaller amounts in each operation.

You cannot copy and paste files between a View desktop and the file system on your client computer.

**Printing from a View Desktop**

From a View desktop, you can print to a virtual printer or to a USB printer that is attached to your client computer. Virtual printing and USB printing work together without conflict.

**Set Printing Preferences for the Virtual Printer Feature on Windows Clients**

The virtual printing feature lets end users use local or network printers from a View desktop without requiring that additional print drivers be installed in the View desktop. For each printer available through this feature, you can set preferences for data compression, print quality, double-sided printing, color, and so on.

After a printer is added on the local Windows computer, View adds that printer to the list of available printers on the View desktop. No further configuration is required. Users who have administrator privileges can still install printer drivers on the View desktop without creating a conflict with the virtual printer component.

**IMPORTANT** This feature is not available for the following types of printers:

- USB printers that are using the USB redirection feature to connect to a virtual USB port in the View desktop
  
  You must disconnect the USB printer from the View desktop in order to use the virtual printing feature with it.

- The Windows feature for printing to a file
  
  Selecting the **Print to file** check box in a Print dialog box does not work. Using a printer driver that creates a file does work. For example, you can use a PDF writer to print to a PDF file.

**Prerequisites**

Verify that the Virtual Printing component of View Agent is installed on the View desktop. In the View desktop file system, the drivers are located in `C:\Program Files\Common Files\VMware\Drivers\Virtual Printer`.

Installing View Agent is one of the tasks required for preparing a virtual machine to be used as a View desktop. For more information, see the [VMware Horizon View Administration](#) document.

**Procedure**

1. In the View desktop, click **Start > Settings > Printers and Faxes**.
2. In the Printers and Faxes window, right-click any of the locally available printers and select **Properties**.
   
   On Windows 7 and 8 desktops, you might see only the default printer, even though other printers are available. To see the other printers, right-click the default printer and point to **Printer properties**.

   In the View desktop, virtual printers appear as `<printer_name>#:<number>`.

3. In the Print Properties window, click the **ThinPrint Device Setup** tab and specify which settings to use.
4. On the **General** tab, click **Printing Preferences** and edit the page and color settings.
5. On the **Advanced** tab, set preferences for double-sided printing and portrait (long edge) or landscape (short edge) printing.
To preview each printout on the host, enable **Preview on client before printing.** From this preview, you can use any printer with all its available properties.

On the **Adjustment** tab, review the settings for automatic print adjustment. VMware recommends that you retain the default settings.

Click **OK.**

### Using USB Printers

In a View environment, virtual printers and redirected USB printers can work together without conflict.

A USB printer is a printer that is attached to a USB port on the local client system. To send print jobs to a USB printer, you can either use the USB redirection feature or use the virtual printing feature. USB printing can sometimes be faster than virtual printing, depending on network conditions.

- You can use the USB redirection feature to attach a USB printer to a virtual USB port in the View desktop as long as the required drivers are also installed on the View desktop.

  If you use this redirection feature the printer is no longer attached to the physical USB port on the client and this is why the USB printer does not appear in the list of local printers that the virtual printing feature displays. This also means that you can print to the USB printer from the View desktop but not from the local client machine.

  In the View desktop, USB printers appear as `<printer_name>`. For information about how to connect a USB printer, see “Connect USB Devices,” on page 41.

- On Windows clients, you can alternatively use the virtual printing feature to send print jobs to a USB printer. If you use the virtual printing feature you can print to the USB printer from both the View desktop and the local client, and you do not need to install print drivers on the View desktop.

### Control Adobe Flash Display

The View administrator can set Adobe Flash content to display in your View desktop at a level designed to conserve computing resources. In some cases, these settings can result in low playback quality. By using the mouse pointer in the desktop, you can override the Adobe Flash settings that your View administrator specifies.

Adobe Flash display control is available for Internet Explorer sessions on Windows only, and for Adobe Flash versions 9 and 10 only. To control Adobe Flash display quality, Adobe Flash must not be running in full screen mode.

**Procedure**

1. From Internet Explorer in the View desktop, browse to the relevant Adobe Flash content and start it if necessary.

   Depending on how your View administrator configured Adobe Flash settings, you might notice dropped frames or low playback quality.

2. Move the mouse pointer into the Adobe Flash content while it is playing.

   Display quality is improved as long as the cursor remains in the Adobe Flash content.

3. To retain the improvement in quality, double-click inside the Adobe Flash content.
Using the Relative Mouse Feature for CAD and 3D Applications

If you use the PCoIP display protocol when using CAD or 3D applications in a Horizon View 5.2 desktop, mouse performance improves when you enable the relative mouse feature.

In most circumstances, if you are using applications that do not require 3D rendering, View Client transmits information about mouse pointer movements by using absolute coordinates. Using absolute coordinates, the client renders the mouse movements locally, which improves performance, especially if you are outside the corporate network.

For work that requires using graphics-intensive applications, such as AutoCAD, or for playing video games, you can improve mouse performance by enabling the relative mouse feature, which uses relative, rather than absolute, coordinates. To use this feature, select Options > Enable Relative Mouse from the View Client menu bar.

**NOTE** If you use View Client in windowed mode, rather than full screen mode, and the relative mouse feature is enabled, you might not be able to move the mouse pointer to the View Client menu options or move the pointer outside of the View Client window. To resolve this situation, press Ctrl+Alt.

When the relative mouse feature is enabled, performance might be slow if you are outside the corporate network, on a WAN.

**IMPORTANT** This feature requires a Horizon View 5.2 desktop, and you must turn on 3D rendering for the desktop pool. For more information about pool settings and the options available for 3D rendering, see the VMware Horizon View Administration document.
View desktops in local mode behave in the same way as their remote desktop equivalents, yet can take advantage of local resources and do not require a network connection.

When you check out a View desktop, the desktop is downloaded to your client computer so you can run it locally. You can back up a View desktop to the server while it is checked out, to save the changes that you made to the local desktop.

When you are not using a local desktop, you can shut it down or suspend it. When you are done using a local desktop, you can check it back in to the server. Alternatively, you can roll back the desktop to discard the changes that you made.

For more information about the benefits of View Client with Local Mode, see the VMware Horizon View Architecture Planning document.

This chapter includes the following topics:

- “Checking Out a Local Mode Desktop for the First Time,” on page 47
- “Shut Down or Suspend a Local Desktop,” on page 48
- “Back Up a Desktop,” on page 48
- “Check In a Desktop,” on page 49
- “Roll Back a Desktop,” on page 49
- “Configuring Endpoint Resource Usage,” on page 50

## Checking Out a Local Mode Desktop for the First Time

The first time an end user checks out a View desktop to use in local mode, the check-out and download process involves several phases and takes more time than for subsequent check-out operations.

After an end user logs in with View Client and is provided with a list of one or more desktops, the user can either connect to the desktop and then check it out or else check out the desktop without connecting remotely first.

**IMPORTANT** You cannot check out a desktop if when you logged in, you used the Log in as current user feature. You must close View Client, start it again, and clear the Log in as current user check box.

If the end user connects to the desktop and then checks it out, the user is logged off of the remote desktop, the virtual machine in the datacenter is locked, and a copy of the virtual machine is downloaded to the end user.

After the download is complete, the first time the end user powers on the local desktop, a number of drivers are installed in the local desktop. Which drivers are installed depends on the View desktop operating system and the local computer’s hardware and operating system. During installation of the drivers, performance of the View desktop is affected, especially if the View desktop runs a Windows XP operating system.
After the drivers are installed, the end user is prompted to reboot the local desktop.

**NOTE** Occasionally, if you click inside a View desktop window when the guest operating system is starting up or shutting down, your pointer remains inside the window. After startup is complete and VMware Tools is running, the pointer is released. If your pointer is grabbed inside the desktop window, you can release it by pressing Ctrl+Alt.

The amount of RAM and the number of CPUs that the local View desktop uses depends on the capabilities of the local computer. The View desktop uses NAT so that it shares the IP and MAC addresses of the local computer. For more information, see “Configuring Endpoint Resource Usage,” on page 50.

## Shut Down or Suspend a Local Desktop

When you are not using a local desktop, you can close it. A local desktop can be shut down or suspended.

**Prerequisites**

If files are open in the desktop, save and close them.

**Procedure**

- From the **Options** menu in the View desktop, select how to close the desktop.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspend</td>
<td>Closes View Client and leaves any open programs in their current state. When you reconnect to the desktop, programs resume in the same state that you left them in. <strong>Note</strong> Suspending the desktop takes longer than shutting down the desktop.</td>
</tr>
<tr>
<td>Shut Down Guest</td>
<td>Closes View Client and stops all open programs. Any unsaved data is lost. This option has the same result as sending Ctrl+Alt+Del to the desktop and then clicking <strong>Shut Down</strong>.</td>
</tr>
</tbody>
</table>

If you click the **Close** button in the title bar, the desktop is either suspended or shut down, depending on how your View administrator has configured your desktop.

## Back Up a Desktop

You can back up a desktop to the server to save changes that you make in the local desktop.

You can back up a desktop only if your View administrator has enabled this feature.

**Prerequisites**

- The desktop must be checked out.
- You must have a network connection.

**Procedure**

- Back up the desktop.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>From the View desktop</td>
<td>Double-click the <strong>VMware View</strong> icon in the System tray to open the backup dialog box, and click <strong>Request Backup</strong>.</td>
</tr>
<tr>
<td>From the desktop selection list</td>
<td>Click the down-arrow next to the desktop to back up and select <strong>Backup</strong>.</td>
</tr>
</tbody>
</table>

To pause a backup in progress, click **Defer Backup**. You can pause a backup only if your View administrator has enabled this feature.
To resume a paused backup, click **Resume Deferred Backup**.
To disable toast notifications that display backup status, right-click the **VMware Horizon View** tray icon and select **Disable Backup Notifications**.

### Check In a Desktop

When you are done using a local desktop, you can check it back in to the server.

You can check in a View desktop only if your View administrator has enabled the feature.

You cannot access the desktop during check-in.

**Prerequisites**

- The desktop must be checked out.
- You must have a network connection.

**Procedure**

- **Check in the desktop.**

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>From the View desktop</td>
<td>In the title bar, select Options &gt; Check In.</td>
</tr>
<tr>
<td>From the desktop selection list</td>
<td>Click the down-arrow next to the desktop to check in and select Check In.</td>
</tr>
</tbody>
</table>

To pause a check-in while it is in progress, select **Pause Check In**. To resume a paused check-in, select **Resume Check In**. To cancel a check-in while it is in progress, select **Cancel Check In**.

The desktop is checked back in to the server and becomes available for check-out by other authorized users.

Checking in a desktop does not remove the local desktop files from your client computer's disk drive.

### Roll Back a Desktop

Rolling back a local desktop discards changes that you made to the desktop. All data that was updated after the last check-out or backup to the server is lost.

You can roll back a desktop only if your View administrator has enabled this feature.

You cannot access the desktop during rollback.

**Prerequisites**

- The desktop must be checked out.
- You must have a network connection.

**Procedure**

- **Roll back the desktop.**

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>From the View desktop</td>
<td>In the title bar, select Options &gt; Rollback.</td>
</tr>
<tr>
<td>From the desktop selection list</td>
<td>Click the down-arrow next to the desktop to roll back and select Rollback.</td>
</tr>
</tbody>
</table>

The desktop is no longer running locally.

Rolling back a desktop does not remove the local desktop files from your client computer's disk drive.
Configuring Endpoint Resource Usage

By default, a View desktop that is checked out for use on a local system takes advantage of the memory and CPU capabilities of that host. The virtual NICs on the desktop use NAT to share the IP and MAC addresses of the host. You can change this default behavior.

Override Local Usage of Memory and CPU Resources

After a local desktop is checked out, it takes advantage of the memory and CPU capabilities of the local system, regardless of the memory and CPU settings specified for the virtual machine in vCenter Server. You can override this default behavior.

By default, the amount of RAM allocated to a View desktop that is checked out for use in local mode is automatically adjusted to be a certain amount of the RAM that is available on the client host.

The formula takes into consideration how much memory is available to split between the host and guest View desktop. A Windows XP operating system requires a minimum of 512MB RAM. A 32-bit Windows 8, Windows 7, or Windows Vista operating system requires a minimum of 1GB RAM. The amount of memory available to split is the total amount of RAM on the host minus the minimum RAM required for the host and guest operating systems.

### Table 6-2. Memory Allotted to Local View Desktops

<table>
<thead>
<tr>
<th>Memory Allocation</th>
<th>Windows XP Guests</th>
<th>Windows 8, Windows 7, and Vista Guests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum</td>
<td>512MB</td>
<td>1GB</td>
</tr>
<tr>
<td>Best effort</td>
<td>512MB + (Available/2)</td>
<td>1GB + (Available/2)</td>
</tr>
<tr>
<td>Maximum</td>
<td>2GB</td>
<td>4GB</td>
</tr>
</tbody>
</table>

For example, if a Windows 7 host has a total of 2GB of RAM, to run a Windows 7 View desktop locally would require 2GB of RAM, with 1GB of RAM allocated to the host and 1GB of RAM allocated to the local View desktop. If the host had 3GB of RAM, 1.5GB of RAM would be allocated to the host and 1.5GB of RAM would be allocated to the local View desktop.

**Note** The automatic adjustment of memory allocation never sets the memory of the local desktop to a lower value than what is configured in vCenter Server.

Similarly, the local View desktop can use up to two CPUs available on the client host if the View desktop is running a Windows Vista or later operating system.

You can change the defaults and specify the scope of the setting. The setting can apply to all local desktops on the client or, depending on the setting, it can apply to a specific desktop or to all desktops from a specific View Connection Server instance that a specific user is entitled to use on the client.

To change these defaults, you must configure Windows registry settings. You can then use standard Windows tools such as Group Policy Objects (GPOs) to deploy these registry settings.

**Prerequisites**

- If you plan to set a specific number of CPUs that the local desktop can use, power off the local desktop.
Because in many cases you can specify the scope of the setting, determine the IDs you will need to specify.

### Table 6-1. Identifiers Used in Registry Settings for Local Mode Resource Usage

<table>
<thead>
<tr>
<th>Scope</th>
<th>Variable Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server specific</td>
<td>broker_guid</td>
<td>Globally unique identifier for the View Connection Server instance or group. Use the <code>vdmadmin -C</code> command to determine the GUID.</td>
</tr>
<tr>
<td>Server and user specific</td>
<td>remote_user_sid</td>
<td>The security ID of the end user. Use the ADSI Edit utility on a View Connection Server host and find the value of the <code>pae-SIDString</code> field of <code>CN=machine_CN,OU=Servers,DC=vdi,DC=vmware,DC=int</code>.</td>
</tr>
<tr>
<td>Server, user, and desktop specific</td>
<td>desktop_ID</td>
<td>The ID of the View desktop. Use the ADSI Edit utility on a View Connection Server. The ID is listed in <code>OU=Applications of DC=vdi,DC=vmware,DC=int</code>. The desktop ID is the distinguished name that uses the display name of the desktop pool: <code>CN=pool_display_name,OU=Applications,DC=vdi,DC=vmware,DC=int</code>.</td>
</tr>
</tbody>
</table>

You can also find the broker GUID in the `mvdi.lst` file on the client computer. On Windows XP, the file is located in the `C:\Documents and Settings\user_name\Local Settings\Application Data\VMware\VDM` folder. Open the file and search for `brokerGUID`. The remote user security ID is also listed in this file. Open the file and search for `user-sid`.

### Procedure

- To override the default behavior so that the local desktop uses only the amount of memory configured in vCenter Server, create and deploy a GPO to add one of the following registry keys and set the key to 1.

<table>
<thead>
<tr>
<th>Scope of Setting</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client-wide</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\disableOfflineDesktopMemoryScaleup</td>
</tr>
<tr>
<td>Server and user specific</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\remote_user_sid\disableOfflineDesktopMemoryScaleup</td>
</tr>
</tbody>
</table>

The value 1 indicates that `disableOfflineDesktopMemoryScaleup` is on, and the value 0 indicates that it is off.

- To set a specific amount of memory that the View desktop can use when running locally, create and deploy a GPO to add one of the following registry keys that specify the number in megabytes, up to 32GB.

<table>
<thead>
<tr>
<th>Scope of Setting</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client-wide</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\offlineDesktopDefaultMemoryScaleupValue</td>
</tr>
<tr>
<td>Server specific</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\offlineDesktopDefaultMemoryScaleupValue</td>
</tr>
<tr>
<td>Server and user specific</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\remote_user_sid\offlineDesktopDefaultMemoryScaleupValue</td>
</tr>
<tr>
<td>Server, user, and desktop specific</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\remote_user_sid\desktop_ID\offlineDesktopDefaultMemoryScaleupValue</td>
</tr>
</tbody>
</table>

If you set the value to a number that is too large, the local desktop does not power on, and an error message appears.
To check out a desktop that was configured to require more memory than is available on the client host, create and deploy a GPO to add the following registry key that specifies the number of megabytes that you want the local client to report that it has available.

HKCU\Software\VMware, Inc.\VMware VDM\Client\offlineDesktopReportedHostMemoryValue

Setting this value to one that is greater than or equal to the memory required by the View desktop allows you to check out and run the View desktop if the client has enough spare memory to run the virtual machine.

<table>
<thead>
<tr>
<th>Scope of Setting</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client-wide</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\offlineDesktopReportedHostMemoryValue</td>
</tr>
<tr>
<td>Server specific</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\offlineDesktopReportedHostMemoryValue</td>
</tr>
<tr>
<td>Server and user specific</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\remote_user_sid\offlineDesktopReportedHostMemoryValue</td>
</tr>
<tr>
<td>Server, user, and desktop specific</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\remote_user_sid\desktop_ID\offlineDesktopReportedHostMemoryValue</td>
</tr>
</tbody>
</table>

If the client does not have enough spare memory, you can use the offlineDesktopDefaultMemoryScaleupValue setting in conjunction with the offlineDesktopReportedHostMemoryValue setting.

For example, if your client system has 2GB of memory and the View desktop is configured to require 2GB of memory, you will not be able to check out the View desktop because some memory is also required for client hosted virtualization. You can, however, use the registry setting offlineDesktopReportedHostMemoryValue = 2048, so that you can check out the desktop, and use the registry setting offlineDesktopDefaultMemoryScaleupValue = 1024 so that the View desktop uses only 1GB of memory when it runs locally.

To override the default behavior so that the local desktop uses only the number of CPUs configured in vCenter Server, create and deploy a GPO to add one of the following registry keys and set the key to 1.

<table>
<thead>
<tr>
<th>Scope of Setting</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client-wide</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\disableOfflineDesktopCPUScaleup</td>
</tr>
<tr>
<td>Server and user specific</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\remote_user_sid\disableOfflineDesktopCPUScaleup</td>
</tr>
</tbody>
</table>

The value 1 indicates that disableOfflineDesktopCPUScaleup is on, and the value 0 indicates that it is off.

To set a specific number of CPUs that the View desktop can use when running locally, create and deploy a GPO to add one of the following registry keys that specify the number of CPUs, up to 2.

<table>
<thead>
<tr>
<th>Scope of Setting</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client-wide</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\offlineDesktopDefaultCPUScaleupValue</td>
</tr>
<tr>
<td>Server specific</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\offlineDesktopDefaultCPUScaleupValue</td>
</tr>
</tbody>
</table>
Change the Network Type from NAT to Bridged

By default, the virtual network type of a View desktop changes to NAT (network address translation) when the desktop is checked out for use on a local system. You can override this behavior to use bridged networking so that the View desktop has its own identity on the network.

With bridged networking, the virtual network adapter in the View desktop connects to the physical network adapter in the host computer. Bridged networking makes the View desktop visible to other computers on the network and requires the desktop to have its own IP address.

NAT configures a virtual machine to share the IP and MAC addresses of the host. The View desktop and the client host share a single network identity on the network.

To change these defaults for all local desktops or for specific local desktops on a client host, you must configure Windows registry settings. You can then use standard Windows tools such as Group Policy Objects (GPOs) to deploy these registry settings.

Prerequisites

Because in many cases you can specify the scope of the setting, determine the IDs you will need to specify.

### Table 6-3. Identifiers Used in Registry Settings for Local Mode Resource Usage

<table>
<thead>
<tr>
<th>Scope</th>
<th>Variable Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server specific</td>
<td>broker_guid</td>
<td>Globally unique identifier for the View Connection Server instance or group. Use the vdmadmin –C command to determine the GUID.</td>
</tr>
<tr>
<td>Server and user specific</td>
<td>remote_user_sid</td>
<td>The security ID of the end user. Use the ADSI Edit utility on a View Connection Server host and find the value of the pae-SIDString field of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN=machine_CN,OU=Servers,DC=vdí,DC=vmware,DC=int.</td>
</tr>
<tr>
<td>Server, user, and desktop specific</td>
<td>desktop_ID</td>
<td>The ID of the View desktop. Use the ADSI Edit utility on a View Connection Server. The ID is listed in OU=Applications of DC=vdí,DC=vmware,DC=int. The desktop ID is the distinguished name that uses the display name of the desktop pool: CN=pool_display_name,OU=Applications,DC=vdí,DC=vmware,DC=int.</td>
</tr>
</tbody>
</table>

You can also find the broker GUID in the vdi.lst file on the client computer. On Windows XP, the file is located in the C:\Documents and Settings\user_name\Local Settings\Application Data\VMware\VDM folder. Open the file and search for brokerGUID. The remote user security ID is also listed in this file. Open the file and search for user-sid.
Procedure

To override the default behavior so that the local desktop uses bridged networking, create and deploy a GPO to add one of the following registry keys and set the key to 1.

<table>
<thead>
<tr>
<th>Scope of Setting</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client-wide</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\offlineDesktopUseBridgedNetworking</td>
</tr>
<tr>
<td>Server and user specific</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\remote_user_sid\offlineDesktopUseBridgedNetworking</td>
</tr>
<tr>
<td>Server, user, and desktop-specific</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\remote_user_sid\desktop_ID\offlineDesktopUseBridgedNetworking</td>
</tr>
</tbody>
</table>

A value of 1 sets the desktop to use bridged networking. A value of 0 sets it to use NAT, which is the default.

The setting takes effect when the end user powers on the local desktop.
You can solve most problems with View Client by resetting the desktop or by reinstalling the VMware Horizon View Client application.

This chapter includes the following topics:

- “What to Do If View Client Exits Unexpectedly,” on page 55
- “Reset a Desktop,” on page 55
- “Uninstalling View Client,” on page 56

What to Do If View Client Exits Unexpectedly

View Client might exit even if you do not close it.

Problem

View Client might exit unexpectedly. Depending on your View Connection Server configuration, you might see a message such as There is no secure connection to the View Connection Server. In some cases, no message is displayed.

Cause

This problem occurs when the connection to View Connection Server is lost.

Solution

- Restart View Client. You can connect successfully as soon as View Connection Server is running again. If you continue to have connection problems, contact your View administrator.

Reset a Desktop

You might need to reset a desktop if the desktop operating system stops responding. Resetting shuts down and restarts the desktop. Unsaved data is lost.

Resetting a View desktop is the equivalent of pressing the Reset button on a physical PC to force the PC to restart. Any files that are open on the View desktop will be closed without being saved first.

You can reset the desktop only if your View administrator has enabled this feature.
Procedure

◆ Use the **Reset Desktop** command.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>From within the desktop OS</td>
<td>Select Options &gt; Reset Desktop from the menu bar.</td>
</tr>
</tbody>
</table>
| From the desktop selection list | a  Start View Client, connect to the View Connection Server that provides access to the View desktop, and supply your authentication credentials.  
   b  When the desktop selection list appears, click the down-arrow next to the desktop and select **Reset Desktop**. |

The operating system in the View desktop is rebooted. View Client disconnects from the desktop.

**What to do next**

Wait an appropriate amount of time for system startup before attempting to connect to the View desktop.

**Uninstalling View Client**

You can sometimes resolve problems with View Client by uninstalling and reinstalling the VMware Horizon View Client application.

You uninstall View Client using the same method you usually use for uninstalling any other application.

For example, use the **Add or Remove Programs** applet available in your Windows operating system to remove the VMware Horizon View Client application.

After uninstalling is complete, you can reinstall the application.

Index

**Numerics**

3D applications 46

**A**

Adobe Flash video, control 45
autoconnect USB devices 41

**B**

back up a desktop 48
bridged networking for local desktops 53
browser requirements 12

**C**

CAD applications 46
certificates, ignoring problems 29, 30
check in a View desktop 49
client software requirements 7
connect, USB devices 41, 42
control, Adobe Flash video display 45
copying text and images 43
CPU requirements, local mode desktops 9
Ctrl+Alt for ungrabbing the mouse pointer 47
Ctrl+Alt+Delete 38
customer experience program, desktop pool 13

data

**D**

defer desktop backup 48
desktop
back up 48
local 47
log off from 38
reset 55
shut down 48
suspend 48
switch 37
devices, connecting USB 41, 42
disconnecting from a View desktop 38
display protocols
Microsoft RDP 39
View PCoIP 39
display requirements, local mode desktops 9
drivers, installed on client systems for local desktops 47

**E**

default resource usage, configuring 50

**F**

feature support matrix 39
Firefox, supported versions 12

**H**

hardware requirements
for Windows systems 7
local mode desktops 9
smart card authentication 12

**I**

images, copying 43
Internet Explorer, supported versions 12

**L**

local CPU usage, overriding 50
local desktop 47
local desktop configuration
changing the network type to bridged 53
hardware requirements 9
local desktop use, checking out 47
local memory usage, overriding 50
Log in as current user feature 35
log off 38

**M**

media file formats, supported 10
memory requirements, local mode desktops 9
Microsoft Lync support 11
Microsoft RDP 39
Microsoft Windows Installer
command-line options for silent installation 22
properties for View Client 21
mouse grabbed inside desktop window 47
multimedia redirection (MMR) 10

**N**

NAT on local desktops 53
NICs 53

**O**

operating systems, supported on View Agent 11
Using VMware Horizon View Client for Windows

P
pasting text and images 43
pause desktop backup 48
PCoIP 39
pointer grabbed inside desktop window 47
prerequisites for client devices 13
print from a desktop 44
printers, setting up 44

R
registry
  settings for View Client 33
  settings for wswc command 33
relative mouse 46
remote desktops, logging off 47
reset desktop 55
resume desktop backup 48
roll back a View desktop 49

S
security servers 13
Send Ctrl+Alt+Del menu command 38
server certificate verification 29
server connections 35
shut down a desktop 48
silent installation
  group policies to allow installation 19
  View Client 19, 20
  View Client with Local Mode 20
smart card authentication, requirements 12
SSL certificates, verifying 29
streaming multimedia 10
suspend a desktop 48
switch desktops 37
system requirements, for Windows 7

T
text, copying 43
thin client support 39
ThinPrint setup 44

U
Unified Communications 11
uninstalling View Client 56
UPNs
  View Client 35
  View Client with Local Mode 35
URI examples 28
URI syntax for View Clients 26
URIs (uniform resource identifiers) 25
USB devices, using with View desktops 39
USB printers 44, 45

V
verification modes for certificate checking 29
View Agent, installation requirements 11
View Client
  command syntax 31
  configuration file 33
  configuring 25
  disconnect from a desktop 38
  exits unexpectedly 55
  installation overview 15
  installing on a Windows PC or laptop 15
  installing silently on a Windows PC or laptop 19, 20
  registry settings 33
  running from the command line 31
  silent installation properties 21
  starting 15, 35
  system requirements for Windows 7
  troubleshooting 55
  using View Portal to download 18
  using View Portal to install 16
  View Client with Local Mode, group policies for silent installation 19
  View components, command-line options for silent installation 22
  View Connection Server 13
View desktop
  check in 49
  roll back 49
View Portal, browser requirements 12
virtual printers 44
virtual printing feature 39, 44
virtual profiles 39
VoIP (voice over IP) 11

W
Web browser requirements 12
Windows, installing View Client on 7
Windows 7 and 8 requirements, local mode desktops 9
Windows computers, installing View Client 15
wswc command
  configuration file 33
  exit codes 33
  syntax 31
Wyse MMR 10, 39