# Using VMware View Client for Linux

December 2011

View Client for Linux



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-000780-00

vmware®

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





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

# Contents

# 1 Using VMware View Client for Linux

This guide, *Using VMware View Client for Linux*, provides information about installing and using VMware View™ software on a Linux 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 View Client for Linux.

This information is intended for administrators who need to set up a VMware View deployment that includes Linux client systems. The information is written for experienced system administrators who are familiar with virtual machine technology and datacenter operations.

---

**NOTE** This document pertains to the View Client for Linux that VMware makes available on Ubuntu. In addition, several VMware partners offer thin client devices for VMware View deployments. The features that are available for each thin client device, and the operating systems supported, are determined by the vendor and model and the configuration that an enterprise chooses to use. For information about the vendors and models for thin client devices, see the *VMware Compatibility Guide*, available on the VMware Web site.

---

# Setup and Installation

Setting up a View deployment for Linux clients involves using certain View Connection Server configuration settings, meeting the system requirements for View servers and Linux clients, and downloading and installing View Client for Linux.



## System Requirements for Linux Clients

You can install View Client for Linux on PCs that use the Ubuntu Linux 10.4 or 10.10 operating system.

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

| | |
|---|---|
| **Model** | Intel-based desktop or laptop computer |
| **Memory** | At least 2GB of RAM |
| **Operating systems** | 32-bit Ubuntu Linux 10.4 or 10.10 |
| **View Connection Server, Security Server, and View Agent** | 4.6 or later<br>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 VMware View** | PCoIP or RDP |
| **Hardware Requirements for PCoIP** | ■ x86-based processor with SSE2 extensions, with a 800MHz or higher processor speed.<br>■ Available RAM above system requirements to support various monitor setups. Use the following formula as a general guide:<br>`20MB + (24 * (# monitors) * (monitor width) * (monitor height))`<br>As a rough guide, you can use the following calculations:<br>`1 monitor: 1600 x 1200: 64MB`<br>`2 monitors: 1600 x 1200: 128MB`<br>`3 monitors: 1600 x 1200: 256MB` |
| **Hardware Requirements for RDP** | ■ x86-based processor with SSE2 extensions, with a 800MHz or higher processor speed. |

- 128MB RAM.

**Software Requirements for RDP**

You must use a remote desktop connection client that is equivalent to RDC 7 or later. In addition, command-line commands use rdesktop to redirect connected client devices to a View desktop.

## 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 VMware View 4.6.x or 5.x installation documentation.

---

IMPORTANT If you use Windows 7 in a virtual machine, the host must be ESX/ESXi 4.0 Update 2 or later, ESX/ESXi 4.1 Update 1 or later, or ESXi 5.0 or later.

---

## 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 and View Security Server 4.6 or later. See the *VMware View Installation* documentation for View 4.6 or later.
- If you plan to use a secure 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 you plan to use is entitled to access this View desktop. See the topics about creating desktop pools in the *VMware View Administration* documentation.

## Install View Client for Linux

End users open View Client to connect to virtual desktops from a physical machine. View Client for Linux runs on Ubuntu 10.4 or 10.10 systems, and you install it by using the Synaptic Package Manager.

### Prerequisites

- Verify that the client system uses a supported operating system. See "System Requirements for Linux Clients," on page 6.
- Verify that you can log in as an administrator on the client system.
- If you plan to use the RDP display protocol to connect to a View desktop, verify that you have the appropriate RDP client installed. See "System Requirements for Linux Clients," on page 6.

### Procedure

1 On your Linux laptop or PC, enable Canonical Partners.

   a From the Ubuntu menu bar, select **System > Administration > Update Manager**.

   b Click the **Settings** button and supply the password for performing administrative tasks.

c In the Software Sources dialog box, click the **Other Software** tab and select the **Canonical Partners** check box to select the archive for software that Canonical packages for their partners.

d Click **Close** and follow the instructions to update the package list.

2 From the Ubuntu menu bar, select **System > Administration > Synaptic Package Manager**.

3 Click **Search** and search for `vmware`.

4 In the list of packages returned, select the check box next to **vmware-view-client** and select **Mark for Installation**.

Do not select the check box for the open client.

5 Click **Apply** in the toolbar.

VMware View Client for Linux is installed.

6 To determine that installation succeeded, verify that the **VMware View** application icon appears in the **Applications > Internet** menu.

### What to do next

Start View Client and verify that you can log in to the correct virtual desktop. See "Log In to a View Desktop for the First Time," on page 9.

## Managing Server Connections and Desktops

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.

- Log In to a View Desktop for the First Time on page 9

  Before you have end users access their virtual desktops, test that you can log in to a virtual desktop from the client system.

- Certificate Checking Modes for View Client on page 10

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

- Configuring Certificate Checking for End Users on page 11

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

- Switch Desktops on page 11

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

- Log Off or Disconnect from a Desktop on page 11

  If you disconnect from a View desktop without logging off, applications remain open.

- Roll Back a Desktop on page 12

  Rolling back discards changes made to a virtual desktop that you checked out for use in local mode on a Windows PC or laptop.

## Log In to a View Desktop for the First Time

Before you have end users access their virtual desktops, test that you can log in to a virtual desktop from the client system.

### Prerequisites

- Obtain the credentials that you need to log in, such as Active Directory user name and password or RSA SecurID user name and passcode.
- Obtain the domain name for logging in.
- Perform the administrative tasks described in "Preparing View Connection Server for View Client," on page 7.
- 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 that the View server presents. See "Certificate Checking Modes for View Client," on page 10.

### Procedure

1. Either open a terminal window and enter `vmware-view` or select **Applications > Internet > VMware View Client** from the Ubuntu menu bar.
2. Enter the server name and a port number if required, and click **Continue**.

   An example using a nondefault port is `view.company.com:1443`.
3. If you are prompted for RSA SecurID credentials, enter the user name and passcode and click **Continue**.
4. Enter your user name and password, select a domain, and click **Continue**.

   You might see a message that you must confirm before the login dialog box appears.
5. (Optional) Select the display protocol and window size to use.

| Option | Description |
|---|---|
| **Display protocol** | The default is **PCoIP**. To use Microsoft RDP instead, click **PCoIP** under the desktop name to toggle and select **Microsoft RDP**. |
| **Window size** | The default is **All Monitors**. To choose another window size, click **Full Screen** under the desktop name and select the size or select to use multiple monitors. |

6. Double-click a View desktop shortcut to connect.

After you are connected, the client window appears. If View Client cannot connect to the 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.
- Verify that the tags set on the View Connection Server instance allow connections from this user. See the *VMware View Administration* document.
- Verify that the user is entitled to access this desktop. See the *VMware 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.

## 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:

- 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 that users can install on their Linux client systems, as well as instructions for importing the certificate, see the Ubuntu documentation.

---

If your administrator has allowed it, you can set the certificate checking mode. Select **File > Preferences** from the VMware View Client menu bar or the View desktop menu bar. You have three choices:

- **Reject the unverifiable connection (Secure)**. If any of the certificate checks fails, the client cannot connect to the server. An error message lists the checks that failed.
- **Warn if the connection may be insecure (Default)**. 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.
- **Allow the unverifiable connection (Not Secure)**. This setting means that View does not perform any certificate checking.

## 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 that 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 10.

Use the `view.sslVerificationMode` property to set the default verification mode:

- **`1`** implements `Full Verification`.
- **`2`** implements `Warn If the Connection May Be Insecure`.
- **`3`** implements `No Verification Performed`.

To configure the mode so that end users cannot change the mode, set the `view.allowSslVerificationMode` property to **`"False"`** in the `/etc/vmware/view-mandatory-config` file on the client system. See "View Client Command Usage and Configuration Settings," on page 15.

## Switch Desktops

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

### Procedure

- Select a View desktop from the same server or a different server.

| Option | Action |
|---|---|
| **Choose a different View desktop on the same server** | Select **Desktop > Disconnect** from the menu bar. |
| **Choose a View desktop on a different server** | Select **File > Choose Another Server** from the menu bar. |

## Log Off or Disconnect from a Desktop

If you disconnect from a View desktop without logging off, applications remain open.

If you are not connected to a View desktop, you can log off without having to connect first. Using this feature has the same result as sending Ctrl+Alt+Del to the desktop and then clicking **Log Off**.

NOTE To use the equivalent of pressing Ctrl+Alt+Delete on a Windows system, select **Desktop > Send Ctrl +Alt+Delete** from the menu bar.

Alternatively, you can press Ctrl+Alt+Insert.

### Procedure

- Disconnect without logging off.

| Option | Action |
|---|---|
| **Also quit View Client** | Click the **Close** button in the corner of the window or select **File > Quit** from the menu bar. |
| **Choose a different View desktop on the same server** | Select **Desktop > Disconnect** from the menu bar. |
| **Choose a View desktop on a different server** | Select **File > Choose Another Server** from the menu bar. |

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.

| Option | Action |
|---|---|
| **From within the desktop OS** | Use the Windows **Start** menu to log off. |
| **From the menu bar** | Select **Desktop > Disconnect and Log Off**.<br>If you use this procedure, files that are open on the View desktop will be closed without being saved first. |

- Log off when you are not connected to a View desktop.

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

| Option | Action |
|---|---|
| **From Home screen with server shortcuts** | a Double-click the server shortcut and supply credentials.<br>These might include RSA SecurID credentials and credentials for logging in to the desktop.<br>b Select the desktop and select **Desktop > Disconnect and Log Off** from the menu bar. |
| **From Home screen with desktop shortcuts** | Select the desktop and select **Desktop > Disconnect and Log Off** from the menu bar. |

## Roll Back a Desktop

Rolling back discards changes made to a virtual desktop that you checked out for use in local mode on a Windows PC or laptop.

You can roll back a View desktop only if your View administrator has enabled this feature and only if you checked out the desktop.

CAUTION If changes were made to the local mode desktop and those changes were not replicated back to the View server before rolling back, the changes are lost.

### Prerequisites

- Obtain the credentials that you need to log in, such as Active Directory user name and password or RSA SecurID user name and passcode.
- Back up the desktop to the server to preserve data or files.

  You can use View Administrator to replicate data to the server, or, if the policy is set to allow it, you can use View Client with Local Mode on the Windows client where the desktop is currently checked out.

### Procedure

1 If the View Client Home screen displays the **View Connection Server** prompt, supply the server name and click **Continue.**

   a If you are prompted for RSA SecurID credentials, enter the user name and passcode and click **Continue**.

   b Enter your user name and password in the login dialog box.

2 On the View Client Home screen that displays View desktop shortcuts, select the desktop and select **Desktop > Rollback Desktop** from the menu bar.

After the View desktop is rolled back, you can log in to it from the Linux client.

# Using a Microsoft Windows Desktop on a Linux System

View Client for Linux supports some of the features included in View Client for Windows.

## Feature Support Matrix

View Client for Linux supports a subset of the features available on other clients, such as the View Client for Windows desktops and laptops.

**Table 1-1.** Features Supported on Windows Desktops for Linux Clients

| Feature | Windows 7 View Desktop | Windows Vista View Desktop | Windows XP View Desktop |
|---|---|---|---|
| RSA SecurID | X | X | X |
| Single sign-on | X | X | X |
| RDP display protocol | X | X | X |
| PCoIP display protocol | X | X | X |
| USB access | | | |
| Wyse MMR | | | |
| Virtual printing | | | |
| Location-based printing | X | X | X |
| Smart cards | | | |
| Multiple monitors | X | X | X |
| Local mode | | | |

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

**NOTE** This feature support matrix applies to the View Client for Linux that VMware makes available on Ubuntu. In addition, several VMware partners offer thin client devices for VMware View deployments. The features that are available for each thin client device are determined by the vendor and model and the configuration that an enterprise chooses to use. For information about the vendors and models for thin client devices, see the *VMware Compatibility Guide*, available on the VMware Web site.

### Internationalization

For this Tech Preview release, the user interface and the documentation for View Client are available only in English.

# Troubleshooting View Client

You can solve most problems with View Client by resetting the desktop or by reinstalling the VMware View Client.

## Reset a Desktop

Resetting shuts down and restarts the desktop. Unsaved data is lost.

You might need to reset a desktop if the desktop operating system stops responding.

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 **Desktop Reset** command.

| Option | Action |
|---|---|
| **From within the desktop OS** | Select **Desktop > Desktop Reset** from the menu bar. |
| **From Home screen with server shortcuts** | a Double-click the server shortcut and supply credentials.<br>These might include RSA SecurID credentials and credentials for logging in to the desktop.<br>b Select the desktop and select **Desktop > Desktop Reset** from the menu bar. |
| **From Home screen with desktop shortcuts** | Select the desktop and select **Desktop > Desktop Reset** from the menu bar. |

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 View Client application.

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

For example, select **Applications > Ubuntu Software Center**, and in the **Installed Software** section, select **vmware-view-client** and click **Remove.**

After uninstalling is complete, you can reinstall the application.

See "Install View Client for Linux," on page 7.

# View Client Command Usage and Configuration Settings

You can configure View Client using command-line options or equivalent properties in a configuration file.

You can use the `vmware-view` command-line interface or set properties in configuration files to define default values your users see in View Client or to suppress some dialog boxes from prompting users for information. You can also specify settings that you do not want users to change.

## Processing Order for Configuration Settings

When View Client starts up, configuration settings are processed from various locations in the following order:

1 `/etc/vmware/view-default-config`

2 `~/.vmware/view-preferences`

3 Command-line arguments

4 `/etc/vmware/view-mandatory-config`

If a setting is defined in multiple locations, the value that is used is the value from the last file read. For example, to specify settings that override users' preferences, set properties in the `/etc/vmware/view-mandatory-config` file.

To set default values that users can change, use the `/etc/vmware/view-default-config` file. After users change a setting, when they exit View Client, any changed settings are saved in the `~/.vmware/view-preferences` file.

## Properties That Prevent Users from Changing Defaults

For each property, you can set a corresponding `view.allow` property that controls whether users are allowed to change the setting. For example, if you set the `view.allowDefaultBroker` property to "FALSE" in the `/etc/vmware/view-mandatory-config` file, users will not be able to change the name in the **Server Name** field when they use View Client.

## Syntax for Using the Command-Line Interface

Use the following form of the `vmware-view` command from a terminal window.

`vmware-view [`*`command_line_option`* `[`*`argument`*`]] ...`

By default, the `vmware-view` command is located in the `/usr/bin` directory.

You can use either the short form or the long form of the option name. For example, to specify the domain you can use either `-d` (short form) or `--domainName=` (long form). You might choose to use the long form to make a script more human-readable.

You can use the `--help` option to get a list of command-line options and usage information.

## View Client Configuration Settings

For your convenience, almost all configuration settings have both a *key=value* property and a corresponding command-line option name. For a few settings, there is a command-line option but no corresponding property you can set in a configuration file. For a few other settings, you must set a property because no command-line option is available.

**Table 1-2.** View Client Command-Line Options and Configuration File Keys

| Configuration Key | Command-Line Option | Description |
|---|---|---|
| `view.autoConnectBroker` | None | Automatically connects to the last View server used unless the `view.defaultBroker` configuration property is set or unless the `--serverURL=` command-line option is used.<br>Specify **`"TRUE"`** or **`"FALSE"`**. Default is "FALSE". |
| `view.autoConnectDesktop` | None | Automatically connects to the last View desktop used unless the `view.defaultDesktop` configuration property is set or unless the `--desktopName=` command-line option is used.<br>Specify **`"TRUE"`** or **`"FALSE"`**. Default is "FALSE". |
| `view.defaultBroker` | `-s, --serverURL=`<br>Examples:<br>`--serverURL=https://view.company.com`<br>`-s view.company.com`<br>`--serverURL=view.company.com:1443` | Adds the fully qualified domain name that you specify to the **Server Name** field in View Client. You can also specify a port number if you do not use the default 443.<br>Default is the most recently used value. |
| `view.defaultDesktop` | `-n, --desktopName=` | Specifies which desktop to use when `autoConnectDedsktop` is set to "TRUE" and the user has access to multiple desktops.<br>This is the name you would see in the Select Desktop dialog box. The name is usually the pool name. |
| `view.defaultDesktopHeight` | None | Specifies the default height of the window for the View desktop, in pixels. |
| `view.defaultDesktopSize` | `--desktopSize=`<br>Examples:<br>`--desktopSize="1280x800"`<br>`--desktopSize="1"` | Sets the default size of the window for the View desktop.<br>Specify **`"1"`** to use all monitors, **`"2"`** to use full screen mode on one monitor, **`"3"`** for a large window, **`"4"`** for a small window, or **`"`*`widthxheight`*`"`** to specify the width by height, in pixels. |
| `view.defaultDesktopWidth` | None | Specifies the default width of the window for the View desktop, in pixels. |
| `view.defaultDomain` | `-d, --domainName=` | Adds the domain name that you specify to the **Domain Name** field in View Client authentication dialog box. |
| `view.defaultPassword` | `-p "-", --password="-"` | Always specify **`"-"`** to read the password from `stdin`.<br>Adds the password to the **Password** field in View Client authentication dialog box if View Connection Server accepts password authentication. |
| `view.defaultProtocol` | `--protocol=` | Specifies which display protocol to use. Specify **`"PCOIP"`** or **`"RDP"`**. Default is "PCOIP". |
| `view.defaultUser` | `-u, --userName=` | Adds the user name that you specify to the **User Name** field in View Client authentication dialog box. |

**Table 1-2.** View Client Command-Line Options and Configuration File Keys (Continued)

| Configuration Key | Command-Line Option | Description |
|---|---|---|
| `view.fullScreen` | `--fullscreen=` | Hides the host operating system and opens the View Client user interface in full screen mode. This option does not affect the screen mode of the desktop session.<br>Specify **`"TRUE"`** or **`"FALSE"`**. Default is "FALSE". |
| `view.kbdLayout` | `-k, --kbdLayout=`<br>Examples:<br>`--kbdLayout="en-us"`<br>`-k "fr"` | Specifies which locale to use for the keyboard layout, by language code. |
| `view.noninteractive` | `-q, --nonInteractive=`<br>Example:<br>`--serverURL="https://view.company.com"`<br>`--userName="user1" --password="-"`<br>`--domainName="xyz"`<br>`--desktopName="Windows 7"`<br>`--nonInteractive="TRUE"` | Hides unnecessary steps from end users by skipping the screens that are specified in the command line or configuration properties.<br>Specify **`"TRUE"`** or **`"FALSE"`**. Default is "FALSE". |
| `view.rdesktopOptions` | `--rdesktopOptions=`<br>Example:<br>`--rdesktopOptions="-f -k en-us -m"` | (Available if you use the Microsoft RDP display protocol) Specifies command-line options to forward to the rdesktop application. For information about rdesktop options, see the rdesktop documentation. |
| | `-r, --redirect=`<br>Example:<br>`--redirect="lspci"`<br>`--redirect="sound:off"` | (Available if you use the Microsoft RDP display protocol) Specifies a local device that you want rdesktop to redirect to the View desktop.<br>Specify the device information that you want to pass to the `-r` option of rdesktop. You can set multiple device options in a single command. |
| `view.sslVerificationMode` | | Sets the server certificate verification mode.<br>Specify **`"1"`** to reject connections when the certificate fails any of the verification checks, **`"2"`** to warn but allow connections that use a self-signed certificate, or **`"3"`** to allow unverifiable connections. If you specify **`"3"`** no verification checks are performed. Default is "1". |
| | `--printEnvironmentInfo` | Displays information about the environment of a client device, including its IP address, MAC address, machine name, and domain name. |
| | `--version` | Displays version information about View Client. |

## 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 1-3 shows the exit codes that the `vmware-view` command can return. Some codes pertain only to View Client for Windows.

**Table 1-3.** View Client Exit Codes

| Exit Code | Description |
|---|---|
| -1 | Fatal error in kiosk mode. |
| 0 | Success. |
| 1 | Connection failed. |
| 2 | Login failed. |
| 3 | Desktop failed to start. |
| 4 | RDP failed to start. |
| 5 | RDP operation failed. |
| 6 | Tunnel connection lost. |
| 7 | Local desktop transfer failure. |
| 8 | Local desktop check-in failure. |
| 9 | Local desktop check-out failure. |
| 10 | Local desktop rollback failure. |
| 11 | Unknown result received during authentication. |
| 12 | Authentication error. |
| 13 | Received request to use an unknown authentication method. |
| 14 | Invalid server response. |
| 15 | Desktop was disconnected. |
| 16 | Tunnel was disconnected. |
| 17 | Reserved for future development. |
| 18 | Reserved for future development. |
| 19 | Unsupported kiosk operation. |
| 20 | Remote mouse, keyboard, or screen (RMKS) connection error. |
| 21 | PIN error. |
| 22 | PIN mismatch. |
| 23 | Password mismatch. |
| 24 | View Connection Server error. |
| 25 | Desktop was not available. |

# Index