

# View Administration

VMware Horizon 7 7.1



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

<https://docs.vmware.com/>

The VMware Web site also provides the latest product updates.

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

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

Copyright © 2014–2017 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

# Contents

View Administration	7
<b>1 Using View Administrator</b>	<b>9</b>
View Administrator and View Connection Server	9
Log In to View Administrator	10
Tips for Using the View Administrator Interface	10
Troubleshooting the Text Display in View Administrator	12
<b>2 Configuring View Connection Server</b>	<b>13</b>
Configuring vCenter Server and View Composer	13
Backing Up View Connection Server	25
Configuring Settings for Client Sessions	25
Disable or Enable View Connection Server	38
Edit the External URLs	38
Join or Withdraw from the Customer Experience Program	39
View LDAP Directory	40
<b>3 Setting Up Smart Card Authentication</b>	<b>43</b>
Logging In with a Smart Card	44
Configure Smart Card Authentication on View Connection Server	44
Configure Smart Card Authentication on Third-Party Solutions	49
Prepare Active Directory for Smart Card Authentication	50
Verify Your Smart Card Authentication Configuration	52
Using Smart Card Certificate Revocation Checking	53
<b>4 Setting Up Other Types of User Authentication</b>	<b>57</b>
Using Two-Factor Authentication	57
Using SAML Authentication	61
Configure Biometric Authentication	65
<b>5 Authenticating Users Without Requiring Credentials</b>	<b>67</b>
Providing Unauthenticated Access for Published Applications	67
Using the Log In as Current User Feature Available with Windows-Based Horizon Client	72
Saving Credentials in Mobile and Mac Horizon Clients	72
Setting Up True SSO	73
<b>6 Configuring Role-Based Delegated Administration</b>	<b>95</b>
Understanding Roles and Privileges	95

	Using Access Groups to Delegate Administration of Pools and Farms	96
	Understanding Permissions	97
	Manage Administrators	98
	Manage and Review Permissions	99
	Manage and Review Access Groups	101
	Manage Custom Roles	103
	Predefined Roles and Privileges	105
	Required Privileges for Common Tasks	109
	Best Practices for Administrator Users and Groups	111
<b>7</b>	<b>Configuring Policies in Horizon Administrator and Active Directory</b>	<b>113</b>
	Setting Policies in View Administrator	113
	Using Horizon 7 Group Policy Administrative Template Files	115
<b>8</b>	<b>Maintaining View Components</b>	<b>123</b>
	Backing Up and Restoring View Configuration Data	123
	Monitor View Components	131
	Monitor Machine Status	131
	Understanding View Services	132
	Change the Product License Key	134
	Monitoring Product License Usage	134
	Update General User Information from Active Directory	135
	Migrate View Composer to Another Machine	136
	Update the Certificates on a View Connection Server Instance, Security Server, or View Composer	141
	Information Collected by the Customer Experience Improvement Program	142
<b>9</b>	<b>Managing View Composer Linked-Clone Desktop Virtual Machines</b>	<b>159</b>
	Reduce Linked-Clone Size with Machine Refresh	159
	Update Linked-Clone Desktops	161
	Rebalance Linked-Clone Virtual Machines	165
	Manage View Composer Persistent Disks	168
<b>10</b>	<b>Managing Desktop Pools, Machines, and Sessions</b>	<b>173</b>
	Managing Instant-Clone Desktop Pools	173
	Managing Desktop Pools	174
	Managing Virtual Machine-Based Desktops	183
	Managing Unmanaged Machines	188
	Manage Published Desktop and Application Sessions	191
	Export View Information to External Files	191
<b>11</b>	<b>Managing Application Pools, Farms, and RDS Hosts</b>	<b>193</b>
	Managing Application Pools	193
	Managing Farms	194
	Managing RDS Hosts	199
	Configuring Load Balancing for RDS Hosts	203
	Configure an Anti-Affinity Rule for an Application Pool	209

<b>12</b>	<b>Managing ThinApp Applications in View Administrator</b>	<b>211</b>
	View Requirements for ThinApp Applications	211
	Capturing and Storing Application Packages	212
	Assigning ThinApp Applications to Machines and Desktop Pools	215
	Maintaining ThinApp Applications in View Administrator	221
	Monitoring and Troubleshooting ThinApp Applications in View Administrator	224
	ThinApp Configuration Example	227
<b>13</b>	<b>Setting Up Clients in Kiosk Mode</b>	<b>229</b>
	Configure Clients in Kiosk Mode	229
<b>14</b>	<b>Troubleshooting View</b>	<b>239</b>
	Monitoring System Health	239
	Monitor Events in View	240
	Collecting Diagnostic Information for View	241
	Update Support Requests	245
	Troubleshooting an Unsuccessful Security Server Pairing with View Connection Server	245
	Troubleshooting View Server Certificate Revocation Checking	246
	Troubleshooting Smart Card Certificate Revocation Checking	247
	Further Troubleshooting Information	247
<b>15</b>	<b>Using the vdmadmin Command</b>	<b>249</b>
	vdmadmin Command Usage	251
	Configuring Logging in Horizon Agent Using the -A Option	253
	Overriding IP Addresses Using the -A Option	254
	Setting the Name of a View Connection Server Group Using the -C Option	255
	Updating Foreign Security Principals Using the -F Option	256
	Listing and Displaying Health Monitors Using the -H Option	257
	Listing and Displaying Reports of View Operation Using the -I Option	258
	Generating View Event Log Messages in Syslog Format Using the -I Option	259
	Assigning Dedicated Machines Using the -L Option	260
	Displaying Information About Machines Using the -M Option	261
	Reclaiming Disk Space on Virtual Machines Using the -M Option	262
	Configuring Domain Filters Using the -N Option	263
	Configuring Domain Filters	265
	Displaying the Machines and Policies of Unentitled Users Using the -O and -P Options	269
	Configuring Clients in Kiosk Mode Using the -Q Option	270
	Displaying the First User of a Machine Using the -R Option	274
	Removing the Entry for a View Connection Server Instance or Security Server Using the -S Option	274
	Providing Secondary Credentials for Administrators Using the -T Option	275
	Displaying Information About Users Using the -U Option	277
	Unlocking or Locking Virtual Machines Using the -V Option	277
	Detecting and Resolving LDAP Entry Collisions Using the -X Option	278
	<b>Index</b>	<b>281</b>



# View Administration

---

*View Administration* describes how to configure and administer VMware Horizon<sup>®</sup> 7, including how to configure View Connection Server, create administrators, set up user authentication, configure policies, and manage VMware ThinApp<sup>®</sup> applications in View Administrator. This document also describes how to maintain and troubleshoot View components.

## Intended Audience

This information is intended for anyone who wants to configure and administer VMware Horizon 7. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.



# Using View Administrator

---

View Administrator is the Web interface through which you configure View Connection Server and manage your remote desktops and applications.

For a comparison of the operations that you can perform with View Administrator, View cmdlets, and vdmadmin, see the *View Integration* document.

---

**NOTE** In Horizon 7, View Administrator is named Horizon Administrator. This document refers to Horizon Administrator as View Administrator.

---

This chapter includes the following topics:

- [“View Administrator and View Connection Server,”](#) on page 9
- [“Log In to View Administrator,”](#) on page 10
- [“Tips for Using the View Administrator Interface,”](#) on page 10
- [“Troubleshooting the Text Display in View Administrator,”](#) on page 12

## View Administrator and View Connection Server

View Administrator provides a Web-based management interface for View.

The View Connection Server can have multiple instances that serve as replica servers or security servers. Depending on your View deployment, you can get a View Administrator interface with each instance of a View Connection Server.

Use the following best practices to use View Administrator with a View Connection Server:

- Use the host name and IP address of the View Connection Server to log in to View Administrator. Use the View Administrator interface to manage the View Connection Server, and any associated security server or replica server.
- In a pod environment, verify that all administrators use the host name and IP address of the same View Connection Server to log in to View Administrator. Do not use the host name and IP address of the load balancer to access a View Administrator web page.

---

**NOTE** If you use Access Point appliances rather than security servers, you must use the Access Point REST API to manage the Access Point appliances. For more information, see *Deploying and Configuring Access Point*.

---

## Log In to View Administrator

To perform initial configuration tasks, you must log in to View Administrator. You access View Administrator by using a secure (SSL) connection.

### Prerequisites

- Verify that View Connection Server is installed on a dedicated computer.
- Verify that you are using a Web browser supported by View Administrator. For View Administrator requirements, see the *View Installation* document.

### Procedure

- 1 Open your Web browser and enter the following URL, where *server* is the host name of the View Connection Server instance.

**https://server/admin**

---

**NOTE** You can use the IP address if you have to access a View Connection Server instance when the host name is not resolvable. However, the host that you contact will not match the SSL certificate that is configured for the View Connection Server instance, resulting in blocked access or access with reduced security.

---

Your access to View Administrator depends on the type of certificate that is configured on the View Connection Server computer.

If you open your Web browser on the View Connection Server host, use **https://127.0.0.1** to connect, not **https://localhost**. This method improves security by avoiding potential DNS attacks on the localhost resolution.

Option	Description
<b>You configured a certificate signed by a CA for View Connection Server.</b>	When you first connect, your Web browser displays View Administrator.
<b>The default, self-signed certificate supplied with View Connection Server is configured.</b>	When you first connect, your Web browser might display a page warning that the security certificate associated with the address is not issued by a trusted certificate authority. Click <b>Ignore</b> to continue using the current SSL certificate.

- 2 Log in as a user with credentials to access the View Administrators account.

You specify the View Administrators account when you install a standalone View Connection Server instance or the first View Connection Server instance in a replicated group. The View Administrators account can be the local Administrators group (BUILTIN\Administrators) on the View Connection Server computer or a domain user or group account.

After you log in to View Administrator, you can use **View Configuration > Administrators** to change the list of users and groups that have the View Administrators role.

## Tips for Using the View Administrator Interface

You can use View Administrator user-interface features to navigate View Pages and to find, filter, and sort View objects.

View Administrator includes many common user interface features. For example, the navigation pane on the left side of each page directs you to other View Administrator pages. The search filters let you select filtering criteria that are related to the objects you are searching for.

Table 1-1 describes a few additional features that can help you to use View Administrator.

**Table 1-1. View Administrator Navigation and Display Features**

View Administrator Feature	Description
Navigating backward and forward in View Administrator pages	<p>Click your browser's <b>Back</b> button to go to the previously displayed View Administrator page. Click the <b>Forward</b> button to return to the current page.</p> <p>If you click the browser's <b>Back</b> button while you are using a View Administrator wizard or dialog box, you return to the main View Administrator page. The information you entered in the wizard or dialog is lost.</p> <p>In View versions that preceded the View 5.1 release, you could not use your browser's <b>Back</b> and <b>Forward</b> buttons to navigate within View Administrator. Separate <b>Back</b> and <b>Forward</b> buttons in the View Administrator window were provided for navigation. These buttons are removed in the View 5.1 release.</p>
Bookmarking View Administrator pages	You can bookmark View Administrator pages in your browser.
Multicolumn sorting	<p>You can sort View objects in a variety of ways by using multicolumn sorting. Click a heading in the top row of a View Administrator table to sort the View objects in alphabetical order based on that heading.</p> <p>For example, in the <b>Resources &gt; Machines</b> page, you can click <b>Desktop Pool</b> to sort desktops by the pools that contain them.</p> <p>The number <b>1</b> appears next to the heading to indicate that it is the primary sorting column. You can click the heading again to reverse the sorting order, indicated by an up or down arrow.</p> <p>To sort the View objects by a secondary item, Ctrl+click another heading.</p> <p>For example, in the Machines table, you can click <b>Users</b> to perform a secondary sort by users to whom the desktops are dedicated. A number <b>2</b> appears next to the secondary heading. In this example, desktops are sorted by pool and by users within each pool.</p> <p>You can continue to Ctrl+click to sort all the columns in a table in descending order of importance.</p> <p>Press Ctrl+Shift and click to deselect a sort item.</p> <p>For example, you might want to display the desktops in a pool that are in a particular state and are stored on a particular datastore. You can select <b>Resources &gt; Machines</b>, click the <b>Datastore</b> heading, and Ctrl+click the <b>Status</b> heading.</p>
Customizing table columns	<p>You can customize the display of View Administrator table columns by hiding selected columns and locking the first column. This feature lets you control the display of large tables such as <b>Catalog &gt; Desktop Pools</b> that contain many columns.</p> <p>Right-click any column header to display a context menu that lets you take the following actions:</p> <ul style="list-style-type: none"> <li>■ Hide the selected column.</li> <li>■ Customize columns. A dialog displays all columns in the table. You can select the columns to display or hide.</li> <li>■ Lock the first column. This option forces the left-hand column to remain displayed as you scroll horizontally across a table with many columns. For example, on the <b>Catalog &gt; Desktop Pools</b> page, the desktop ID remains displayed as you scroll horizontally to see other desktop characteristics.</li> </ul>

**Table 1-1.** View Administrator Navigation and Display Features (Continued)

View Administrator Feature	Description
Selecting View objects and displaying View object details	<p>In View Administrator tables that list View objects, you can select an object or display object details.</p> <ul style="list-style-type: none"> <li>■ To select an object, click anywhere in the object's row in the table. At the top of the page, menus and commands that manage the object become active.</li> <li>■ To display object details, double-click the left cell in the object's row. A new page displays the object's details.</li> </ul> <p>For example, on the <b>Catalog &gt; Desktop Pools</b> page, click anywhere in an individual pool's row to activate commands that affect the pool.</p> <p>Double-click the <b>ID</b> cell in the left column to display a new page that contains details about the pool.</p>
Expanding dialog boxes to view details	<p>You can expand View Administrator dialog boxes to view details such as desktop names and user names in table columns.</p> <p>To expand a dialog box, place your mouse over the dots in the lower right corner of the dialog box and drag the corner.</p>
Displaying context menus for View objects	<p>You can right-click View objects in View Administrator tables to display context menus. A context menu gives you access to the commands that operate on the selected View object.</p> <p>For example, in the <b>Catalog &gt; Desktop Pools</b> page, you can right-click a desktop pool to display commands such as <b>Add</b>, <b>Edit</b>, <b>Delete</b>, <b>Disable (or Enable) Provisioning</b>, and so on.</p>

## Troubleshooting the Text Display in View Administrator

If your Web browser runs on a non-Windows operating system such as Linux, UNIX, or Mac OS, the text in View Administrator does not display properly.

### Problem

The text in the View Administrator interface is garbled. For example, spaces occur in the middle of words.

### Cause

View Administrator requires Microsoft-specific fonts.

### Solution

Install Microsoft-specific fonts on your computer.

Currently, the Microsoft Web site does not distribute Microsoft fonts, but you can download them from independent Web sites.

# Configuring View Connection Server

---

After you install and perform initial configuration of View Connection Server, you can add vCenter Server instances and View Composer services to your View deployment, set up roles to delegate administrator responsibilities, and schedule backups of your configuration data.

This chapter includes the following topics:

- [“Configuring vCenter Server and View Composer,”](#) on page 13
- [“Backing Up View Connection Server,”](#) on page 25
- [“Configuring Settings for Client Sessions,”](#) on page 25
- [“Disable or Enable View Connection Server,”](#) on page 38
- [“Edit the External URLs,”](#) on page 38
- [“Join or Withdraw from the Customer Experience Program,”](#) on page 39
- [“View LDAP Directory,”](#) on page 40

## Configuring vCenter Server and View Composer

To use virtual machines as remote desktops, you must configure View to communicate with vCenter Server. To create and manage linked-clone desktop pools, you must configure View Composer settings in View Administrator.

You can also configure storage settings for View. You can allow ESXi hosts to reclaim disk space on linked-clone virtual machines. To allow ESXi hosts to cache virtual machine data, you must enable View Storage Accelerator for vCenter Server.

## Create a User Account for View Composer AD Operations

If you use View Composer, you must create a user account in Active Directory that allows View Composer to perform certain operations in Active Directory. View Composer requires this account to join linked-clone virtual machines to your Active Directory domain.

To ensure security, you should create a separate user account to use with View Composer. By creating a separate account, you can guarantee that it does not have additional privileges that are defined for another purpose. You can give the account the minimum privileges that it needs to create and remove computer objects in a specified Active Directory container. For example, the View Composer account does not require domain administrator privileges.

### Procedure

- 1 In Active Directory, create a user account in the same domain as your View Connection Server host or in a trusted domain.

- 2 Add the **Create Computer Objects**, **Delete Computer Objects**, and **Write All Properties** permissions to the account in the Active Directory container in which the linked-clone computer accounts are created or to which the linked-clone computer accounts are moved.

The following list shows all the required permissions for the user account, including permissions that are assigned by default:

- List Contents
- Read All Properties
- Write All Properties
- Read Permissions
- Reset Password
- Create Computer Objects
- Delete Computer Objects

---

**NOTE** Fewer permissions are required if you select the **Allow reuse of pre-existing computer accounts** setting for a desktop pool. Make sure that the following permissions are assigned to the user account:

- List Contents
  - Read All Properties
  - Read Permissions
  - Reset Password
- 

- 3 Make sure that the user account's permissions apply to the Active Directory container and to all child objects of the container.

### What to do next

Specify the account in View Administrator when you configure View Composer domains in the Add vCenter Server wizard and when you configure and deploy linked-clone desktop pools.

## Add vCenter Server Instances to View

You must configure View to connect to the vCenter Server instances in your View deployment. vCenter Server creates and manages the virtual machines that View uses in desktop pools.

If you run vCenter Server instances in a Linked Mode group, you must add each vCenter Server instance to View separately.

View connects to the vCenter Server instance using a secure channel (SSL).

### Prerequisites

- Install the View Connection Server product license key.
- Prepare a vCenter Server user with permission to perform the operations in vCenter Server that are necessary to support View. To use View Composer, you must give the user additional privileges.

For details about configuring a vCenter Server user for View, see the *View Installation* document.

- Verify that a TLS/SSL server certificate is installed on the vCenter Server host. In a production environment, install a valid certificate that is signed by a trusted Certificate Authority (CA).

In a testing environment, you can use the default certificate that is installed with vCenter Server, but you must accept the certificate thumbprint when you add vCenter Server to View.

- Verify that all View Connection Server instances in the replicated group trust the root CA certificate for the server certificate that is installed on the vCenter Server host. Check if the root CA certificate is in the **Trusted Root Certification Authorities > Certificates** folder in the Windows local computer certificate stores on the View Connection Server hosts. If it is not, import the root CA certificate into the Windows local computer certificate stores.

See "Import a Root Certificate and Intermediate Certificates into a Windows Certificate Store," in the *View Installation* document.

- Verify that the vCenter Server instance contains ESXi hosts. If no hosts are configured in the vCenter Server instance, you cannot add the instance to View.
- If you upgrade to vSphere 5.5 or a later release, verify that the domain administrator account that you use as the vCenter Server user was explicitly assigned permissions to log in to vCenter Server by a vCenter Server local user.
- If you plan to use View in FIPS mode, verify that you have vCenter Server 6.0 or later and ESXi 6.0 or later hosts.

For more information, see "Installing View in FIPS Mode," in the *View Installation* document.

- Familiarize yourself with the settings that determine the maximum operations limits for vCenter Server and View Composer. See ["Concurrent Operations Limits for vCenter Server and View Composer,"](#) on page 21 and ["Setting a Concurrent Power Operations Rate to Support Remote Desktop Logon Storms,"](#) on page 21.

## Procedure

- 1 In View Administrator, select **View Configuration > Servers**.
- 2 On the **vCenter Servers** tab, click **Add**.
- 3 In the vCenter Server Settings **Server address** text box, type the fully qualified domain name (FQDN) of the vCenter Server instance.

The FQDN includes the host name and domain name. For example, in the FQDN

**myserverhost.companydomain.com**, **myserverhost** is the host name and **companydomain.com** is the domain.

---

**NOTE** If you enter a server by using a DNS name or URL, View does not perform a DNS lookup to verify whether an administrator previously added this server to View by using its IP address. A conflict arises if you add a vCenter Server with both its DNS name and its IP address.

---

- 4 Type the name of the vCenter Server user.  
For example: **domain\user** or **user@domain.com**
- 5 Type the vCenter Server user password.
- 6 (Optional) Type a description for this vCenter Server instance.
- 7 Type the TCP port number.  
The default port is 443.
- 8 Under Advanced Settings, set the concurrent operations limits for vCenter Server and View Composer operations.
- 9 Click **Next** to display the View Composer Settings page.

## What to do next

Configure View Composer settings.

- If the vCenter Server instance is configured with a signed SSL certificate, and View Connection Server trusts the root certificate, the Add vCenter Server wizard displays the View Composer Settings page.

- If the vCenter Server instance is configured with a default certificate, you must first determine whether to accept the thumbprint of the existing certificate. See [“Accept the Thumbprint of a Default SSL Certificate,”](#) on page 22.

If View uses multiple vCenter Server instances, repeat this procedure to add the other vCenter Server instances.

## Configure View Composer Settings

To use View Composer, you must configure settings that allow View to connect to the VMware Horizon View Composer service. View Composer can be installed on its own separate host or on the same host as vCenter Server.

There must be a one-to-one mapping between each VMware Horizon View Composer service and vCenter Server instance. A View Composer service can operate with only one vCenter Server instance. A vCenter Server instance can be associated with only one VMware Horizon View Composer service.

After the initial View deployment, you can migrate the VMware Horizon View Composer service to a new host to support a growing or changing View deployment. You can edit the initial View Composer settings in View Administrator, but you must perform additional steps to ensure that the migration succeeds. See [“Migrate View Composer to Another Machine,”](#) on page 136.

### Prerequisites

- Verify that you created a user in Active Directory with permission to add and remove virtual machines from the Active Directory domain that contains your linked clones. See [“Create a User Account for View Composer AD Operations,”](#) on page 13.
- Verify that you configured View to connect to vCenter Server. To do so, you must complete the vCenter Server Information page in the Add vCenter Server wizard. See [“Add vCenter Server Instances to View,”](#) on page 14.
- Verify that this VMware Horizon View Composer service is not already configured to connect to a different vCenter Server instance.

### Procedure

- 1 In View Administrator, complete the vCenter Server Information page in the Add vCenter Server wizard.
  - a Select **View Configuration > Servers**.
  - b On the **vCenter Servers** tab, click **Add** and provide the vCenter Server settings.
- 2 On the View Composer Settings page, if you are not using View Composer, select **Do not use View Composer**.

If you select **Do not use View Composer**, the other View Composer settings become inactive. When you click **Next**, the Add vCenter Server wizard displays the Storage Settings page. The View Composer Domains page is not displayed.

- 3 If you are using View Composer, select the location of the View Composer host.

Option	Description
<b>View Composer is installed on the same host as vCenter Server.</b>	<ol style="list-style-type: none"> <li>Select <b>View Composer co-installed with the vCenter Server</b>.</li> <li>Make sure that the port number is the same as the port that you specified when you installed the VMware Horizon View Composer service on vCenter Server. The default port number is 18443.</li> </ol>
<b>View Composer is installed on its own separate host.</b>	<ol style="list-style-type: none"> <li>Select <b>Standalone View Composer Server</b>.</li> <li>In the View Composer server address text box, type the fully qualified domain name (FQDN) of the View Composer host.</li> <li>Type the name of the View Composer user.  For example: <b>domain.com\user</b> or <b>user@domain.com</b></li> <li>Type the password of the View Composer user.</li> <li>Make sure that the port number is the same as the port that you specified when you installed the VMware Horizon View Composer service. The default port number is 18443.</li> </ol>

- 4 Click **Next** to display the View Composer Domains page.

### What to do next

Configure View Composer domains.

- If the View Composer instance is configured with a signed SSL certificate, and View Connection Server trusts the root certificate, the Add vCenter Server wizard displays the View Composer Domains page.
- If the View Composer instance is configured with a default certificate, you must first determine whether to accept the thumbprint of the existing certificate. See [“Accept the Thumbprint of a Default SSL Certificate,”](#) on page 22.

## Configure View Composer Domains

You must configure an Active Directory domain in which View Composer deploys linked-clone desktops. You can configure multiple domains for View Composer. After you first add vCenter Server and View Composer settings to View, you can add more View Composer domains by editing the vCenter Server instance in View Administrator.

### Prerequisites

- Your Active Directory administrator must create a View Composer user for AD operations. This domain user must have permission to add and remove virtual machines from the Active Directory domain that contains your linked clones. For information about the required permissions for this user, see [“Create a User Account for View Composer AD Operations,”](#) on page 13.
- In View Administrator, verify that you completed the vCenter Server Information and View Composer Settings pages in the Add vCenter Server wizard.

### Procedure

- On the View Composer Domains page, click **Add** to add the View Composer user for AD operations account information.
- Type the domain name of the Active Directory domain.  
For example: **domain.com**
- Type the domain user name, including the domain name, of the View Composer user.  
For example: **domain.com\admin**
- Type the account password.

- 5 Click **OK**.
- 6 To add domain user accounts with privileges in other Active Directory domains in which you deploy linked-clone pools, repeat the preceding steps.
- 7 Click **Next** to display the Storage Settings page.

### What to do next

Enable virtual machine disk space reclamation and configure View Storage Accelerator for View.

## Allow vSphere to Reclaim Disk Space in Linked-Clone Virtual Machines

In vSphere 5.1 and later, you can enable the disk space reclamation feature for View. Starting in vSphere 5.1, View creates linked-clone virtual machines in an efficient disk format that allows ESXi hosts to reclaim unused disk space in the linked clones, reducing the total storage space required for linked clones.

As users interact with linked-clone desktops, the clones' OS disks grow and can eventually use almost as much disk space as full-clone desktops. Disk space reclamation reduces the size of the OS disks without requiring you to refresh or recompose the linked clones. Space can be reclaimed while the virtual machines are powered on and users are interacting with their remote desktops.

Disk space reclamation is especially useful for deployments that cannot take advantage of storage-saving strategies such as refresh on logoff. For example, knowledge workers who install user applications on dedicated remote desktops might lose their personal applications if the remote desktops were refreshed or recomposed. With disk space reclamation, View can maintain linked clones at close to the reduced size they start out with when they are first provisioned.

This feature has two components: space-efficient disk format and space reclamation operations.

In a vSphere 5.1 or later environment, when a parent virtual machine is virtual hardware version 9 or later, View creates linked clones with space-efficient OS disks, whether or not space reclamation operations are enabled.

To enable space reclamation operations, you must use View Administrator to enable space reclamation for vCenter Server and reclaim VM disk space for individual desktop pools. The space reclamation setting for vCenter Server gives you the option to disable this feature on all desktop pools that are managed by the vCenter Server instance. Disabling the feature for vCenter Server overrides the setting at the desktop pool level.

The following guidelines apply to the space reclamation feature:

- It operates only on space-efficient OS disks in linked clones.
- It does not affect View Composer persistent disks.
- It works only with vSphere 5.1 or later and only on virtual machines that are virtual hardware version 9 or later.
- It does not operate on full-clone desktops.
- It operates on virtual machines with SCSI controllers. IDE controllers are not supported.

Native NFS snapshot technology (VAAI) is not supported in pools that contain virtual machines with space-efficient disks.

### Prerequisites

- Verify that your vCenter Server and ESXi hosts, including all ESXi hosts in a cluster, are version 5.1 with ESXi 5.1 download patch ESXi510-201212001 or later.

### Procedure

- 1 In View Administrator, complete the Add vCenter Server wizard pages that precede the Storage Settings page.
  - a Select **View Configuration > Servers**.
  - b On the **vCenter Servers** tab, click **Add**.
  - c Complete the vCenter Server Information, View Composer Settings, and View Composer Domains pages.
- 2 On the Storage Settings page, make sure that **Enable space reclamation** is selected.  
 Space reclamation is selected by default if you are performing a fresh installation of View 5.2 or later. You must select **Enable space reclamation** if you are upgrading to View 5.2 or later from View 5.1 or an earlier release.

### What to do next

On the Storage Settings page, configure View Storage Accelerator.

To finish configuring disk space reclamation in View, set up space reclamation for desktop pools.

## Configure View Storage Accelerator for vCenter Server

In vSphere 5.0 and later, you can configure ESXi hosts to cache virtual machine disk data. This feature, called View Storage Accelerator, uses the Content Based Read Cache (CBRC) feature in ESXi hosts. View Storage Accelerator improves Horizon 7 performance during I/O storms, which can take place when many virtual machines start up or run anti-virus scans at once. The feature is also beneficial when administrators or users load applications or data frequently. Instead of reading the entire OS or application from the storage system over and over, a host can read common data blocks from cache.

By reducing the number of IOPS during boot storms, View Storage Accelerator lowers the demand on the storage array, which lets you use less storage I/O bandwidth to support your Horizon 7 deployment.

You enable caching on your ESXi hosts by selecting the View Storage Accelerator setting in the vCenter Server wizard in Horizon Administrator, as described in this procedure.

Make sure that View Storage Accelerator is also configured for individual desktop pools. To operate on a desktop pool, View Storage Accelerator must be enabled for vCenter Server and for the individual desktop pool.

View Storage Accelerator is enabled for desktop pools by default. The feature can be disabled or enabled when you create or edit a pool. The best approach is to enable this feature when you first create a desktop pool. If you enable the feature by editing an existing pool, you must ensure that a new replica and its digest disks are created before linked clones are provisioned. You can create a new replica by recomposing the pool to a new snapshot or rebalancing the pool to a new datastore. Digest files can only be configured for the virtual machines in a desktop pool when they are powered off.

You can enable View Storage Accelerator on desktop pools that contain linked clones and pools that contain full virtual machines.

Native NFS snapshot technology (VAAI) is not supported in pools that are enabled for View Storage Accelerator.

View Storage Accelerator is now qualified to work in configurations that use Horizon 7 replica tiering, in which replicas are stored on a separate datastore than linked clones. Although the performance benefits of using View Storage Accelerator with Horizon 7 replica tiering are not materially significant, certain capacity-related benefits might be realized by storing the replicas on a separate datastore. Hence, this combination is tested and supported.

---

**IMPORTANT** If you plan to use this feature and you are using multiple View pods that share some ESXi hosts, you must enable the View Storage Accelerator feature for all pools that are on the shared ESXi hosts. Having inconsistent settings in multiple pods can cause instability of the virtual machines on the shared ESXi hosts.

---

### Prerequisites

- Verify that your vCenter Server and ESXi hosts are version 5.0 or later.  
In an ESXi cluster, verify that all the hosts are version 5.0 or later.
- Verify that the vCenter Server user was assigned the **Host > Configuration > Advanced settings** privilege in vCenter Server.  
See the topics in the *View Installation* document that describe Horizon 7 and View Composer privileges required for the vCenter Server user.

### Procedure

- 1 In Horizon Administrator, complete the Add vCenter Server wizard pages that precede the Storage Settings page.
  - a Select **View Configuration > Servers**.
  - b On the **vCenter Servers** tab, click **Add**.
  - c Complete the vCenter Server Information, View Composer Settings, and View Composer Domains pages.
- 2 On the Storage Settings page, make sure that the **Enable View Storage Accelerator** check box is selected.  
This check box is selected by default.
- 3 Specify a default host cache size.  
The default cache size applies to all ESXi hosts that are managed by this vCenter Server instance.  
The default value is 1,024MB. The cache size must be between 100MB and 2,048MB.
- 4 To specify a different cache size for an individual ESXi host, select an ESXi host and click **Edit cache size**.
  - a In the Host cache dialog box, check **Override default host cache size**.
  - b Type a **Host cache size** value between 100MB and 2,048MB and click **OK**.
- 5 On the Storage Settings page, click **Next**.
- 6 Click **Finish** to add vCenter Server, View Composer, and Storage Settings to Horizon 7.

### What to do next

Configure settings for client sessions and connections. See [“Configuring Settings for Client Sessions,”](#) on page 25.

To complete View Storage Accelerator settings in Horizon 7, configure View Storage Accelerator for desktop pools. See "Configure View Storage Accelerator for Desktop Pools" in the *Setting Up Virtual Desktops in Horizon 7* document.

## Concurrent Operations Limits for vCenter Server and View Composer

When you add vCenter Server to View or edit the vCenter Server settings, you can configure several options that set the maximum number of concurrent operations that are performed by vCenter Server and View Composer.

You configure these options in the Advanced Settings panel on the vCenter Server Information page.

**Table 2-1.** Concurrent Operations Limits for vCenter Server and View Composer

Setting	Description
<b>Max concurrent vCenter provisioning operations</b>	Determines the maximum number of concurrent requests that View Connection Server can make to provision and delete full virtual machines in this vCenter Server instance. The default value is 20. This setting applies to full virtual machines only.
<b>Max concurrent power operations</b>	Determines the maximum number of concurrent power operations (startup, shutdown, suspend, and so on) that can take place on virtual machines managed by View Connection Server in this vCenter Server instance. The default value is 50. For guidelines for calculating a value for this setting, see <a href="#">“Setting a Concurrent Power Operations Rate to Support Remote Desktop Logon Storms,”</a> on page 21. This setting applies to full virtual machines and linked clones.
<b>Max concurrent View Composer maintenance operations</b>	Determines the maximum number of concurrent View Composer refresh, recompose, and rebalance operations that can take place on linked clones managed by this View Composer instance. The default value is 12. Remote desktops that have active sessions must be logged off before a maintenance operation can begin. If you force users to log off as soon as a maintenance operation begins, the maximum number of concurrent operations on remote desktops that require logoffs is half the configured value. For example, if you configure this setting as 24 and force users to log off, the maximum number of concurrent operations on remote desktops that require logoffs is 12. This setting applies to linked clones only.
<b>Max concurrent View Composer provisioning operations</b>	Determines the maximum number of concurrent creation and deletion operations that can take place on linked clones managed by this View Composer instance. The default value is 8. This setting applies to linked clones only.

## Setting a Concurrent Power Operations Rate to Support Remote Desktop Logon Storms

The **Max concurrent power operations** setting governs the maximum number of concurrent power operations that can occur on remote desktop virtual machines in a vCenter Server instance. This limit is set to 50 by default. You can change this value to support peak power-on rates when many users log on to their desktops at the same time.

As a best practice, you can conduct a pilot phase to determine the correct value for this setting. For planning guidelines, see “Architecture Design Elements and Planning Guidelines” in the *View Architecture Planning* document.

The required number of concurrent power operations is based on the peak rate at which desktops are powered on and the amount of time it takes for the desktop to power on, boot, and become available for connection. In general, the recommended power operations limit is the total time it takes for the desktop to start multiplied by the peak power-on rate.

For example, the average desktop takes two to three minutes to start. Therefore, the concurrent power operations limit should be 3 times the peak power-on rate. The default setting of 50 is expected to support a peak power-on rate of 16 desktops per minute.

The system waits a maximum of five minutes for a desktop to start. If the start time takes longer, other errors are likely to occur. To be conservative, you can set a concurrent power operations limit of 5 times the peak power-on rate. With a conservative approach, the default setting of 50 supports a peak power-on rate of 10 desktops per minute.

Logons, and therefore desktop power on operations, typically occur in a normally distributed manner over a certain time window. You can approximate the peak power-on rate by assuming that it occurs in the middle of the time window, during which about 40% of the power-on operations occur in 1/6th of the time window. For example, if users log on between 8:00 AM and 9:00 AM, the time window is one hour, and 40% of the logons occur in the 10 minutes between 8:25 AM and 8:35 AM. If there are 2,000 users, 20% of whom have their desktops powered off, then 40% of the 400 desktop power-on operations occur in those 10 minutes. The peak power-on rate is 16 desktops per minute.

## Accept the Thumbprint of a Default SSL Certificate

When you add vCenter Server and View Composer instances to View, you must ensure that the SSL certificates that are used for the vCenter Server and View Composer instances are valid and trusted by View Connection Server. If the default certificates that are installed with vCenter Server and View Composer are still in place, you must determine whether to accept these certificates' thumbprints.

If a vCenter Server or View Composer instance is configured with a certificate that is signed by a CA, and the root certificate is trusted by View Connection Server, you do not have to accept the certificate thumbprint. No action is required.

If you replace a default certificate with a certificate that is signed by a CA, but View Connection Server does not trust the root certificate, you must determine whether to accept the certificate thumbprint. A thumbprint is a cryptographic hash of a certificate. The thumbprint is used to quickly determine if a presented certificate is the same as another certificate, such as the certificate that was accepted previously.

---

**NOTE** If you install vCenter Server and View Composer on the same Windows Server host, they can use the same SSL certificate, but you must configure the certificate separately for each component.

---

For details about configuring SSL certificates, see "Configuring SSL Certificates for View Servers" in the *View Installation* document.

You first add vCenter Server and View Composer in View Administrator by using the Add vCenter Server wizard. If a certificate is untrusted and you do not accept the thumbprint, you cannot add vCenter Server and View Composer.

After these servers are added, you can reconfigure them in the Edit vCenter Server dialog box.

---

**NOTE** You also must accept a certificate thumbprint when you upgrade from an earlier release and a vCenter Server or View Composer certificate is untrusted, or if you replace a trusted certificate with an untrusted certificate.

---

On the View Administrator dashboard, the vCenter Server or View Composer icon turns red and an Invalid Certificate Detected dialog box appears. You must click **Verify** and follow the procedure shown here.

---

Similarly, in View Administrator you can configure a SAML authenticator for use by a View Connection Server instance. If the SAML server certificate is not trusted by View Connection Server, you must determine whether to accept the certificate thumbprint. If you do not accept the thumbprint, you cannot configure the SAML authenticator in View. After a SAML authenticator is configured, you can reconfigure it in the Edit View Connection Server dialog box.

**Procedure**

- 1 When View Administrator displays an Invalid Certificate Detected dialog box, click **View Certificate**.
- 2 Examine the certificate thumbprint in the Certificate Information window.
- 3 Examine the certificate thumbprint that was configured for the vCenter Server or View Composer instance.
  - a On the vCenter Server or View Composer host, start the MMC snap-in and open the Windows Certificate Store.
  - b Navigate to the vCenter Server or View Composer certificate.
  - c Click the Certificate Details tab to display the certificate thumbprint.

Similarly, examine the certificate thumbprint for a SAML authenticator. If appropriate, take the preceding steps on the SAML authenticator host.
- 4 Verify that the thumbprint in the Certificate Information window matches the thumbprint for the vCenter Server or View Composer instance.
 

Similarly, verify that the thumbprints match for a SAML authenticator.
- 5 Determine whether to accept the certificate thumbprint.

Option	Description
<b>The thumbprints match.</b>	Click <b>Accept</b> to use the default certificate.
<b>The thumbprints do not match.</b>	Click <b>Reject</b> . Troubleshoot the mismatched certificates. For example, you might have provided an incorrect IP address for vCenter Server or View Composer.

**Remove a vCenter Server Instance from View**

You can remove the connection between View and a vCenter Server instance. When you do so, View no longer manages the virtual machines created in that vCenter Server instance.

**Prerequisites**

Delete all the virtual machines that are associated with the vCenter Server instance. See [“Delete a Desktop Pool,”](#) on page 181.

**Procedure**

- 1 Click **View Configuration > Servers**.
- 2 On the **vCenter Servers** tab, select the vCenter Server instance.
- 3 Click **Remove**.
 

A dialog warns you that View will no longer have access to the virtual machines that are managed by this vCenter Server instance.
- 4 Click **OK**.

View can no longer access the virtual machines created in the vCenter Server instance.

## Remove View Composer from View

You can remove the connection between View and the VMware Horizon View Composer service that is associated with a vCenter Server instance.

Before you disable the connection to View Composer, you must remove from View all the linked-clone virtual machines that were created by View Composer. View prevents you from removing View Composer if any associated linked clones still exist. After the connection to View Composer is disabled, View cannot provision or manage new linked clones.

### Procedure

- 1 Remove the linked-clone desktop pools that were created by View Composer.
  - a In View Administrator, select **Catalog > Desktop Pools**.
  - b Select a linked-clone desktop pool and click **Delete**.  
 A dialog box warns that you will permanently delete the linked-clone desktop pool from View. If the linked-clone virtual machines are configured with persistent disks, you can detach or delete the persistent disks.
  - c Click **OK**.  
 The virtual machines are deleted from vCenter Server. In addition, the associated View Composer database entries and the replicas that were created by View Composer are removed.
  - d Repeat these steps for each linked-clone desktop pool that was created by View Composer.
- 2 Select **View Configuration > Servers**.
- 3 On the **vCenter Servers** tab, select the vCenter Server instance with which View Composer is associated.
- 4 Click **Edit**.
- 5 Under View Composer Server Settings, click **Edit**, select **Do not use View Composer**, and click **OK**.

You can no longer create linked-clone desktop pools in this vCenter Server instance, but you can continue to create and manage full virtual-machine desktop pools in the vCenter Server instance.

### What to do next

If you intend to install View Composer on another host and reconfigure View to connect to the new VMware Horizon View Composer service, you must perform certain additional steps. See [“Migrate View Composer Without Linked-Clone Virtual Machines,”](#) on page 139.

## Conflicting vCenter Server Unique IDs

If you have multiple vCenter Server instances configured in your environment, an attempt to add a new instance might fail because of conflicting unique IDs.

### Problem

You try to add a vCenter Server instance to View, but the unique ID of the new vCenter Server instance conflicts with an existing instance.

### Cause

Two vCenter Server instances cannot use the same unique ID. By default, a vCenter Server unique ID is randomly generated, but you can edit it.

**Solution**

- 1 In vSphere Client, click **Administration > vCenter Server Settings > Runtime Settings**.
- 2 Type a new unique ID and click **OK**.

For details about editing vCenter Server unique ID values, see the vSphere documentation.

## Backing Up View Connection Server

After you complete the initial configuration of View Connection Server, you should schedule regular backups of your View and View Composer configuration data.

For information about backing up and restoring your View configuration, see [“Backing Up and Restoring View Configuration Data,”](#) on page 123.

## Configuring Settings for Client Sessions

You can configure global settings that affect the client sessions and connections that are managed by a View Connection Server instance or replicated group. You can set the session timeout length, display prelogin and warning messages, and set security-related client connection options.

### Set Options for Client Sessions and Connections

You configure global settings to determine the way client sessions and connections work.

The global settings are not specific to a single View Connection Server instance. They affect all client sessions that are managed by a standalone View Connection Server instance or a group of replicated instances.

You can also configure View Connection Server instances to use direct, nontunneled connections between Horizon clients and remote desktops. See [“Configure the Secure Tunnel and PCoIP Secure Gateway,”](#) on page 33 for information about configuring direct connections.

**Prerequisites**

Familiarize yourself with the global settings. See [“Global Settings for Client Sessions,”](#) on page 26 and [“Global Security Settings for Client Sessions and Connections,”](#) on page 29.

**Procedure**

- 1 In View Administrator, select **View Configuration > Global Settings**.
- 2 Choose whether to configure general settings or security settings.

Option	Description
<b>General global settings</b>	In the General pane, click <b>Edit</b> .
<b>Global security settings</b>	In the Security pane, click <b>Edit</b> .

- 3 Configure the global settings.
- 4 Click **OK**.

**What to do next**

You can change the data recovery password that was provided during installation. See [“Change the Data Recovery Password,”](#) on page 26.

## Change the Data Recovery Password

You provide a data recovery password when you install View Connection Server version 5.1 or later. After installation, you can change this password in View Administrator. The password is required when you restore the View LDAP configuration from a backup.

When you back up View Connection Server, the View LDAP configuration is exported as encrypted LDIF data. To restore the encrypted backup View configuration, you must provide the data recovery password.

The password must contain between 1 and 128 characters. Follow your organization's best practices for generating secure passwords.

### Procedure

- 1 In View Administrator, select **View Configuration > Global Settings**.
- 2 In the Security pane, click **Change data recovery password**.
- 3 Type and retype the new password.
- 4 (Optional) Type a password reminder.

---

**NOTE** You can also change the data recovery password when you schedule your View configuration data to be backed up. See [“Schedule View Configuration Backups,”](#) on page 124.

---

### What to do next

When you use the `vdimport` utility to restore a backup View configuration, provide the new password.

## Global Settings for Client Sessions

General global settings determine session timeout lengths, SSO enablement and timeout limits, status updates in View Administrator, whether prelogin and warning messages are displayed, whether View Administrator treats Windows Server as a supported operating system for remote desktops, and other settings.

Changes to any of the settings in the following table take effect immediately. You do not need to restart View Connection Server or Horizon Client.

**Table 2-2.** General Global Settings for Client Sessions

Setting	Description
<b>View Administrator session timeout</b>	<p>Determines how long an idle View Administrator session continues before the session times out.</p> <p><b>IMPORTANT</b> Setting the View Administrator session timeout to a high number of minutes increases the risk of unauthorized use of View Administrator. Use caution when you allow an idle session to persist a long time.</p> <p>By default, the View Administrator session timeout is 30 minutes. You can set a session timeout from 1 to 4320 minutes (72 hours).</p>
<b>Forcibly disconnect users</b>	<p>Disconnects all desktops and applications after the specified number of minutes has passed since the user logged in to View. All desktops and applications will be disconnected at the same time regardless of when the user opened them.</p> <p>For clients that do not support application remoting, a maximum timeout value of 1200 minutes applies if the value of this setting is <b>Never</b> or greater than 1200 minutes.</p> <p>The default is <b>After 600 minutes</b>.</p>

**Table 2-2.** General Global Settings for Client Sessions (Continued)

Setting	Description
<b>Single sign-on (SSO)</b>	<p>If SSO is enabled, View caches a user's credentials so that the user can launch remote desktops or applications without having to provide credentials to log in to the remote Windows session. The default is <b>Enabled</b>.</p> <p>If you plan to use the True SSO feature, introduced in Horizon 7 or later, SSO must be enabled. With True SSO, if a user logs in using some other form of authentication than Active Directory credentials, the True SSO feature generates short-term certificates to use, rather than cached credentials, after users log in to VMware Identity Manager.</p> <p><b>NOTE</b> If a desktop is launched from Horizon Client, and the desktop is locked, either by the user or by Windows based on a security policy, and if the desktop is running View Agent 6.0 or later or Horizon Agent 7.0 or later, View Connection Server discards the user's SSO credentials. The user must provide login credentials to launch a new desktop or a new application, or reconnect to any disconnected desktop or application. To enable SSO again, the user must disconnect from View Connection Server or exit Horizon Client, and reconnect to View Connection Server. However, if the desktop is launched from Workspace Portal or VMware Identity Manager and the desktop is locked, SSO credentials are not discarded.</p>
<b>For clients that support applications.</b> <b>If the user stops using the keyboard and mouse, disconnect their applications and discard SSO credentials:</b>	<p>Protects application sessions when there is no keyboard or mouse activity on the client device. If set to <b>After ... minutes</b>, View disconnects all applications and discards SSO credentials after the specified number of minutes without user activity. Desktop sessions are not disconnected. Users must log in again to reconnect to the applications that were disconnected or launch a new desktop or application.</p> <p>This setting also applies to the True SSO feature. After SSO credentials are discarded, users are prompted for Active Directory credentials. If users logged in to VMware Identity Manager without using AD credentials and do not know what AD credentials to enter, users can log out and log in to VMware Identity Manager again to access their remote desktops and applications.</p> <p><b>IMPORTANT</b> Users must be aware that when they have both applications and desktops open, and their applications are disconnected because of this timeout, their desktops remain connected. Users must not rely on this timeout to protect their desktops.</p> <p>If set to <b>Never</b>, View never disconnects applications or discards SSO credentials due to user inactivity.</p> <p>The default is <b>Never</b>.</p>
<b>Other clients.</b> <b>Discard SSO credentials:</b>	<p>Discards SSO credentials after the specified number of minutes. This setting is for clients that do not support application remoting. If set to <b>After ... minutes</b>, users must log in again to connect to a desktop after the specified number of minutes has passed since the user logged in to View, regardless of any user activity on the client device.</p> <p>If set to <b>Never</b>, View stores SSO credentials until the user closes Horizon Client, or the <b>Forcibly disconnect users</b> timeout is reached, whichever comes first.</p> <p>The default is <b>After 15 minutes</b>.</p>
<b>Enable automatic status updates</b>	<p>Determines if status updates appear in the global status pane in the upper-left corner of View Administrator every few minutes. The dashboard page of View Administrator is also updated every few minutes.</p> <p>By default, this setting is not enabled.</p>
<b>Display a pre-login message</b>	<p>Displays a disclaimer or another message to Horizon Client users when they log in.</p> <p>Type your information or instructions in the text box in the Global Settings dialog box.</p> <p>To display no message, leave the check box unselected.</p>

**Table 2-2.** General Global Settings for Client Sessions (Continued)

Setting	Description
<b>Display warning before forced logoff</b>	<p>Displays a warning message when users are forced to log off because a scheduled or immediate update such as a desktop-refresh operation is about to start. This setting also determines how long to wait after the warning is shown before the user is logged off.</p> <p>Check the box to display a warning message.</p> <p>Type the number of minutes to wait after the warning is displayed and before logging off the user. The default is 5 minutes.</p> <p>Type your warning message. You can use the default message:  Your desktop is scheduled for an important update and  will be shut down in 5 minutes. Please  save any unsaved work now.</p>
<b>Enable Windows Server desktops</b>	<p>Determines whether you can select available Windows Server 2008 R2 and Windows Server 2012 R2 machines for use as desktops. When this setting is enabled, View Administrator displays all available Windows Server machines, including machines on which View server components are installed.</p> <p><b>NOTE</b> The Horizon Agent software cannot coexist on the same virtual or physical machine with any other View server software component, including a security server, View Connection Server, or View Composer.</p>
<b>Clean up credential when tab closed for HTML Access</b>	<p>Removes a user's credentials from cache when a user closes a tab that connects to a remote desktop or application, or closes a tab that connects to the desktop and application selection page, in the HTML Access client.</p> <p>When this setting is enabled, View also removes the credentials from cache in the following HTML Access client scenarios:</p> <ul style="list-style-type: none"> <li>■ A user refreshes the desktop and application selection page or the remote session page.</li> <li>■ The server presents a self-signed certificate, a user launches a remote desktop or application, and the user accepts the certificate when the security warning appears.</li> <li>■ A user runs a URI command in the tab that contains the remote session.</li> </ul> <p>When this setting is disabled, the credentials remain in cache. This feature is disabled by default.</p> <p><b>NOTE</b> This feature is available in Horizon 7 version 7.0.2 and later.</p>
<b>Mirage Server configuration</b>	<p>Allows you to specify the URL of a Mirage server, using the format <b>mirage://server-name:port</b> or <b>mirages://server-name:port</b>. Here <i>server-name</i> is the fully qualified domain name. If you do not specify the port number, the default port number 8000 is used.</p> <p><b>NOTE</b> You can override this global setting by specifying a Mirage server in the desktop pool settings.</p> <p>Specifying the Mirage server in View Administrator is an alternative to specifying the Mirage server when installing the Mirage client. To find out which versions of Mirage support having the server specified in View Administrator, see the Mirage documentation, at <a href="https://www.vmware.com/support/pubs/mirage_pubs.html">https://www.vmware.com/support/pubs/mirage_pubs.html</a>.</p>

**Table 2-2.** General Global Settings for Client Sessions (Continued)

Setting	Description
<b>Hide server information in client user interface</b>	Enable this security setting to hide server URL information in Horizon Client 4.4 or later.
<b>Hide domain list in client user interface</b>	<p>Enable this security setting to hide the Domain drop-down menu in Horizon Client 4.4 or later.</p> <p>When users log in to a Connection Server instance for which the <b>Hide domain list in client user interface</b> global setting is enabled, the Domain drop-down menu is hidden in Horizon Client and users provide domain information in the Horizon Client <b>User name</b> text box. For example, users must enter their user name in the format <code>domain\username</code> or <code>username@domain</code>.</p> <p><b>IMPORTANT</b> If you enable the <b>Hide server information in client user interface</b> and <b>Hide domain list in client user interface</b> settings and select two-factor authentication (RSA SecureID or RADIUS) for the Connection Server instance, do not enforce Windows user name matching. Enforcing Windows user name matching will prevent users from being able to enter domain information in the user name text box and login will always fail. For more information, see the topics about two-factor authentication in the <i>View Administration</i> document.</p>

## Global Security Settings for Client Sessions and Connections

Global security settings determine whether clients are reauthenticated after interruptions, message security mode is enabled, and IPSec is used for security server connections.

SSL is required for all Horizon Client connections and View Administrator connections to View. If your View deployment uses load balancers or other client-facing, intermediate servers, you can off-load SSL to them and then configure non-SSL connections on individual View Connection Server instances and security servers. See [“Off-load SSL Connections to Intermediate Servers,”](#) on page 35.

**Table 2-3.** Global Security Settings for Client Sessions and Connections

Setting	Description
<b>Reauthenticate secure tunnel connections after network interruption</b>	<p>Determines if user credentials must be reauthenticated after a network interruption when Horizon clients use secure tunnel connections to remote desktops.</p> <p>When you select this setting, if a secure tunnel connection is interrupted, Horizon Client requires the user to reauthenticate before reconnecting.</p> <p>This setting offers increased security. For example, if a laptop is stolen and moved to a different network, the user cannot automatically gain access to the remote desktop without entering credentials.</p> <p>When this setting is not selected, the client reconnects to the remote desktop without requiring the user to reauthenticate.</p> <p>This setting has no effect when the secure tunnel is not used.</p>
<b>Message security mode</b>	<p>Determines the security mechanism used for sending JMS messages between components</p> <ul style="list-style-type: none"> <li>■ When the mode is set to <b>Enabled</b>, signing and verification of the JMS messages passed between View components takes place.</li> <li>■ When the mode is set to <b>Enhanced</b>, security is provided by mutually authenticated SSL JMS connections and access control on JMS topics.</li> </ul> <p>For details, see <a href="#">“Message Security Mode for View Components,”</a> on page 30.</p> <p>For new installations, by default, message security mode is set to <b>Enhanced</b>. If you upgrade from a previous version, the setting used in the previous version is retained.</p>

**Table 2-3.** Global Security Settings for Client Sessions and Connections (Continued)

Setting	Description
<b>Enhanced Security Status</b> (Read-only)	<p>Read-only field that appears when <b>Message security mode</b> is changed from <b>Enabled</b> to <b>Enhanced</b>. Because the change is made in phases, this field shows the progress through the phases:</p> <ul style="list-style-type: none"> <li>■ <b>Waiting for Message Bus restart</b> is the first phase. This state is displayed until you manually restart either all Connection Server instances in the pod or the VMware Horizon View Message Bus Component service on all Connection Server hosts in the pod.</li> <li>■ <b>Pending Enhanced</b> is the next state. After all View Message Bus Component services have been restarted, the system begins changing the message security mode to <b>Enhanced</b> for all desktops and security servers.</li> <li>■ <b>Enhanced</b> is the final state, indicating that all components are now using <b>Enhanced</b> message security mode.</li> </ul> <p>You can also use the <code>vdmutil</code> command-line utility to monitor progress. See <a href="#">“Using the vdmutil Utility to Configure the JMS Message Security Mode,”</a> on page 31.</p>
<b>Use IPSec for Security Server connections</b>	<p>Determines whether to use Internet Protocol Security (IPSec) for connections between security servers and View Connection Server instances.</p> <p>By default, secure connections (using IPSec) for security server connections is enabled.</p>

**NOTE** If you upgrade to View 5.1 or later from an earlier View release, the global setting **Require SSL for client connections** is displayed in View Administrator, but only if the setting was disabled in your View configuration before you upgraded. Because SSL is required for all Horizon Client connections and View Administrator connections to View, this setting is not displayed in fresh installations of View 5.1 or later versions and is not displayed after an upgrade if the setting was already enabled in the previous View configuration.

After an upgrade, if you do not enable the **Require SSL for client connections** setting, HTTPS connections from Horizon clients will fail, unless they connect to an intermediate device that is configured to make onward connections using HTTP. See [“Off-load SSL Connections to Intermediate Servers,”](#) on page 35.

## Message Security Mode for View Components

You can set the message security mode to specify the security mechanism used when JMS messages pass among View components.

[Table 2-4](#) shows the options you can select to configure the message security mode. To set an option, select it from the **Message security mode** list in the Global Settings dialog window.

**Table 2-4.** Message Security Mode Options

Option	Description
<b>Disabled</b>	Message security mode is disabled.
<b>Mixed</b>	<p>Message security mode is enabled but not enforced.</p> <p>You can use this mode to detect components in your View environment that predate View 3.0. The log files generated by View Connection Server contain references to these components. This setting is not recommended. Use this setting only to discover components that need to be upgraded.</p>

**Table 2-4.** Message Security Mode Options (Continued)

Option	Description
<b>Enabled</b>	<p>Message security mode is enabled, using a combination of message signing and encryption. JMS messages are rejected if the signature is missing or invalid, or if a message was modified after it was signed.</p> <p>Some JMS messages are encrypted because they carry sensitive information such as user credentials. If you use the <b>Enabled</b> setting, you can also use IPSec to encrypt all JMS messages between View Connection Server instances, and between View Connection Server instances and security servers.</p> <p><b>NOTE</b> View components that predate View 3.0 are not allowed to communicate with other View components.</p>
<b>Enhanced</b>	<p>SSL is used for all JMS connections. JMS access control is also enabled so that desktops, security servers, and View Connection Server instances can only send and receive JMS messages on certain topics.</p> <p>View components that predate Horizon 6 version 6.1 cannot communicate with a View Connection Server 6.1 instance.</p> <p><b>NOTE</b> Using this mode requires opening TCP port 4002 between DMZ-based security servers and their paired View Connection Server instances.</p>

When you first install View on a system, the message security mode is set to **Enhanced**. If you upgrade View from a previous release, the message security mode remains unchanged from its existing setting.

**IMPORTANT** If you plan to change an upgraded View environment from **Enabled** to **Enhanced**, you must first upgrade all View Connection Server instances, security servers, and View desktops to Horizon 6 version 6.1 or a later release. After you change the setting to **Enhanced**, the new setting takes place in stages.

- 1 You must manually restart the VMware Horizon View Message Bus Component service on all View Connection Server hosts in the pod, or restart the View Connection Server instances.
- 2 After the services are restarted, the View Connection Server instances reconfigure the message security mode on all desktops and security servers, changing the mode to **Enhanced**.
- 3 To monitor the progress in View Administrator, go to **View Configuration > Global Settings**.

On the **Security** tab, the **Enhanced Security Status** item will show **Enhanced** when all components have made the transition to Enhanced mode.

Alternatively, you can use the `vdmutil` command-line utility to monitor progress. See [“Using the vdmutil Utility to Configure the JMS Message Security Mode,”](#) on page 31.

View components that predate Horizon 6 version 6.1 cannot communicate with a View Connection Server 6.1 instance that uses Enhanced mode

If you plan to change an active View environment from **Disabled** to **Enabled**, or from **Enabled** to **Disabled**, change to **Mixed** mode for a short time before you make the final change. For example, if your current mode is **Disabled**, change to **Mixed** mode for one day, then change to **Enabled**. In **Mixed** mode, signatures are attached to messages but not verified, which allows the change of message mode to propagate through the environment.

## Using the vdmutil Utility to Configure the JMS Message Security Mode

You can use the `vdmutil` command-line interface to configure and manage the security mechanism used when JMS messages are passed between View components.

### Syntax and Location of the Utility

The `vdmutil` command can perform the same operations as the `lmvutil` command that was included with earlier versions of View. In addition, the `vdmutil` command has options for determining the message security mode being used and monitoring the progress of changing all View components to Enhanced mode. Use the following form of the `vdmutil` command from a Windows command prompt.

```
vdmutil command_option [additional_option argument] ...
```

The additional options that you can use depend on the command option. This topic focuses on the options for message security mode. For the other options, which relate to Cloud Pod Architecture, see the *Administering Cloud Pod Architecture in Horizon 7* document.

By default, the path to the `vdmutl` command executable file is `C:\Program Files\VMware\VMware View\Server\tools\bin`. To avoid entering the path on the command line, add the path to your `PATH` environment variable.

## Authentication

You must run the command as a user who has the Administrators role. You can use View Administrator to assign the Administrators role to a user. See [Chapter 6, “Configuring Role-Based Delegated Administration,”](#) on page 95.

The `vdmutl` command includes options to specify the user name, domain, and password to use for authentication.

**Table 2-5.** `vdmutl` Command Authentication Options

Option	Description
<code>--authAs</code>	Name of a View administrator user. Do not use <i>domain\username</i> or user principal name (UPN) format.
<code>--authDomain</code>	Fully qualified domain name for the View administrator user specified in the <code>--authAs</code> option.
<code>--authPassword</code>	Password for the View administrator user specified in the <code>--authAs</code> option. Entering "*" instead of a password causes the <code>vdmutl</code> command to prompt for the password and does not leave sensitive passwords in the command history on the command line.

You must use the authentication options with all `vdmutl` command options except for `--help` and `--verbose`.

## Options Specific to JMS Message Security Mode

The following table lists only the `vdmutl` command-line options that pertain to viewing, setting, or monitoring the JMS message security mode. For a list of the arguments you can use with a specific option, use the `--help` command-line option.

The `vdmutl` command returns 0 when an operation succeeds and a failure-specific non-zero code when an operation fails. The `vdmutl` command writes error messages to standard error. When an operation produces output, or when verbose logging is enabled by using the `--verbose` option, the `vdmutl` command writes output to standard output, in US English.

**Table 2-6.** `vdmutl` Command Options

Option	Description
<code>--activatePendingConnectionServerCertificate</code>	Activates a pending security certificate for a View Connection Server instance in the local pod.
<code>--countPendingMsgSecStatus</code>	Counts the number of machines preventing a transition to or from Enhanced mode.
<code>--createPendingConnectionServerCertificate</code>	Creates a new pending security certificate for a View Connection Server instance in the local pod.
<code>--getMsgSecLevel</code>	Gets the enhanced message security status for the local pod. This status pertains to the process of changing the JMS message security mode from <b>Enabled</b> to <b>Enhanced</b> for all the components in a View environment.
<code>--getMsgSecMode</code>	Gets the message security mode for the local pod.
<code>--help</code>	Lists the <code>vdmutl</code> command options. You can also use <code>--help</code> on a particular command, such as <code>--setMsgSecMode --help</code> .

**Table 2-6.** vdmutil Command Options (Continued)

Option	Description
--listMsgBusSecStatus	Lists the message bus security status for all connection servers in the local pod.
--listPendingMsgSecStatus	List machines preventing a transition to or from Enhanced mode. Limited to 25 entries by default.
--setMsgSecMode	Sets the message security mode for the local pod.
--verbose	Enables verbose logging. You can add this option to any other option to obtain detailed command output. The vdmutil command writes to standard output.

## Configure the Secure Tunnel and PCoIP Secure Gateway

When the secure tunnel is enabled, Horizon Client makes a second HTTPS connection to the View Connection Server or security server host when users connect to a remote desktop.

When the PCoIP Secure Gateway is enabled, Horizon Client makes a further secure connection to the View Connection Server or security server host when users connect to a remote desktop with the PCoIP display protocol.

**NOTE** With Horizon 6 version 6.2 and later releases, you can use Access Point appliances, rather than security servers, for secure external access to Horizon 6 servers and desktops. If you use Access Point appliances, you must disable the secure gateways on View Connection Server instances and enable these gateways on the Access Point appliances. For more information, see *Deploying and Configuring Access Point*.

When the secure tunnel or PCoIP Secure Gateway is not enabled, a session is established directly between the client system and the remote desktop virtual machine, bypassing the View Connection Server or security server host. This type of connection is called a direct connection.

**IMPORTANT** A typical network configuration that provides secure connections for external clients includes a security server. To use View Administrator to enable or disable the secure tunnel and PCoIP Secure Gateway on a security server, you must edit the View Connection Server instance that is paired with the security server.

In a network configuration in which external clients connect directly to a View Connection Server host, you enable or disable the secure tunnel and PCoIP Secure Gateway by editing that View Connection Server instance in View Administrator.

### Prerequisites

- If you intend to enable the PCoIP Secure Gateway, verify that the View Connection Server instance and paired security server are View 4.6 or later.
- If you pair a security server to a View Connection Server instance on which you already enabled the PCoIP Secure Gateway, verify that the security server is View 4.6 or later.

### Procedure

- 1 In View Administrator, select **View Configuration > Servers**.
- 2 On the **Connection Servers** tab, select a View Connection Server instance and click **Edit**.

- 3 Configure use of the secure tunnel.

Option	Description
<b>Enable the secure tunnel</b>	Select <b>Use Secure Tunnel connection to machine</b> .
<b>Disable the secure tunnel</b>	Deselect <b>Use Secure Tunnel connection to machine</b> .

The secure tunnel is enabled by default.

- 4 Configure use of the PCoIP Secure Gateway.

Option	Description
<b>Enable the PCoIP Secure Gateway</b>	Select <b>Use PCoIP Secure Gateway for PCoIP connections to machine</b>
<b>Disable the PCoIP secure Gateway</b>	Deselect <b>Use PCoIP Secure Gateway for PCoIP connections to machine</b>

The PCoIP Secure Gateway is disabled by default.

- 5 Click **OK** to save your changes.

## Configure the Blast Secure Gateway

In Horizon Administrator, you can configure the use of the Blast Secure Gateway to provide secure access to remote desktops and applications, either through HTML Access or through client connections that use the VMware Blast display protocol.

The Blast Secure Gateway includes Blast Extreme Adaptive Transport (BEAT) networking, which dynamically adjusts to network conditions such as varying speeds and packet loss.

- Horizon Clients can use BEAT networking with an excellent network condition while connecting to the Connection Server, security server, or Access Point appliance.
- Horizon Clients that use a typical network condition must connect to a Connection Server (BSG disabled), security server (BSG disabled), or versions later than 2.8 of an Access Point appliance. If Horizon Client uses a typical network condition to connect to a Connection Server (BSG enabled), security server (BSG enabled), or versions earlier than 2.8 of an Access Point appliance, the client automatically senses the network condition and falls back to TCP networking.
- Horizon Clients that use a poor network condition must connect to version 2.9 or later of an Access Point appliance (with UDP Tunnel Server Enabled). If Horizon Client uses a poor network condition to connect to the Connection Server (BSG enabled), security server (BSG enabled), or versions earlier than 2.8 of an Access Point appliance, the client automatically senses the network condition and falls back to TCP networking.
- Horizon Clients that use a poor network condition to connect to Connection Server (BSG disabled), security server (BSG disabled), or version 2.9 or later of Access Point appliance (without UDP Tunnel Server Enabled), or version 2.8 of Access Point appliance, the client automatically senses the network condition and falls back to the typical network condition.

For more information, see the Horizon Client documentation at [https://www.vmware.com/support/viewclients/doc/viewclients\\_pubs.html](https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html).

**NOTE** You can also use Access Point appliances, rather than security servers, for secure external access to Horizon 7 servers and desktops. If you use Access Point appliances, you must disable the secure gateways on Connection Server instances and enable these gateways on the Access Point appliances. For more information, see *Deploying and Configuring Access Point*.

When the Blast Secure Gateway is not enabled, client devices and client Web browsers use the VMware Blast Extreme protocol to establish direct connections to remote desktop virtual machines and applications, bypassing the Blast Secure Gateway.

---

**IMPORTANT** A typical network configuration that provides secure connections for external users includes a security server. To enable or disable the Blast Secure Gateway on a security server, you must edit the Connection Server instance that is paired with the security server. If external users connect directly to a Connection Server host, you enable or disable the Blast Secure Gateway by editing that Connection Server instance.

---

### Prerequisites

If users select remote desktops by using VMware Identity Manager, verify that VMware Identity Manager is installed and configured for use with Connection Server and that Connection Server is paired with a SAML 2.0 Authentication server.

### Procedure

- 1 In Horizon Administrator, select **View Configuration > Servers**.
- 2 On the **Connection Servers** tab, select a Connection Server instance and click **Edit**.
- 3 Configure use of the Blast Secure Gateway.

Option	Description
<b>Enable the Blast Secure Gateway</b>	Select <b>Use Blast Secure Gateway for Blast connections to machine</b>
<b>Disable the Blast secure Gateway</b>	Deselect <b>Use Blast Secure Gateway for Blast connections to machine</b>

The Blast Secure Gateway is enabled by default.

- 4 Click **OK** to save your changes.

## Off-load SSL Connections to Intermediate Servers

Horizon Client must use HTTPS to connect to View. If your Horizon clients connect to load balancers or other intermediate servers that pass on the connections to View Connection Server instances or security servers, you can off-load SSL to the intermediate servers.

### Import SSL Off-loading Servers' Certificates to View Servers

If you off-load SSL connections to an intermediate server, you must import the intermediate server's certificate onto the View Connection Server instances or security servers that connect to the intermediate server. The same SSL server certificate must reside on both the off-loading intermediate server and each off-loaded View server that connects to the intermediate server.

If you deploy security servers, the intermediate server and the security servers that connect to it must have the same SSL certificate. You do not have to install the same SSL certificate on View Connection Server instances that are paired to the security servers and do not connect directly to the intermediate server.

If you do not deploy security servers, or if you have a mixed network environment with some security servers and some external-facing View Connection Server instances, the intermediate server and any View Connection Server instances that connect to it must have the same SSL certificate.

If the intermediate server's certificate is not installed on the View Connection Server instance or security server, clients cannot validate their connections to View. In this situation, the certificate thumbprint sent by the View server does not match the certificate on the intermediate server to which Horizon Client connects.

Do not confuse load balancing with SSL off-loading. The preceding requirement applies to any device that is configured to provide SSL off-loading, including some types of load balancers. However, pure load balancing does not require copying of certificates between devices.

For information about importing certificates to View servers, see "Import a Signed Server Certificate into a Windows Certificate Store" in the *View Installation* document.

## Set View Server External URLs to Point Clients to SSL Off-loading Servers

If SSL is off-loaded to an intermediate server and Horizon Client devices use the secure tunnel to connect to View, you must set the secure tunnel external URL to an address that clients can use to access the intermediate server.

You configure the external URL settings on the View Connection Server instance or security server that connects to the intermediate server.

If you deploy security servers, external URLs are required for the security servers but not for the View Connection Server instances that are paired with the security servers.

If you do not deploy security servers, or if you have a mixed network environment with some security servers and some external-facing View Connection Server instances, External URLs are required for any View Connection Server instances that connect to the intermediate server.

---

**NOTE** You cannot off-load SSL connections from a PCoIP Secure Gateway (PSG) or Blast Secure Gateway. The PCoIP external URL and Blast Secure Gateway external URL must allow clients to connect to the computer that hosts the PSG and Blast Secure Gateway. Do not reset the PCoIP external URL and Blast external URL to point to the intermediate server unless you plan to require SSL connections between the intermediate server and the View server.

---

For information about configuring External URLs, see "Configuring External URLs for PCoIP Secure Gateway and Tunnel Connections" in the *View Installation* document.

## Allow HTTP Connections From Intermediate Servers

When SSL is off-loaded to an intermediate server, you can configure View Connection Server instances or security servers to allow HTTP connections from the client-facing, intermediate devices. The intermediate devices must accept HTTPS for Horizon Client connections.

To allow HTTP connections between View servers and intermediate devices, you must configure the `locked.properties` file on each View Connection Server instance and security server on which HTTP connections are allowed.

Even when HTTP connections between View servers and intermediate devices are allowed, you cannot disable SSL in View. View servers continue to accept HTTPS connections as well as HTTP connections.

---

**NOTE** If your Horizon clients use smart card authentication, the clients must make HTTPS connections directly to View Connection Server or security server. SSL off-loading is not supported with smart card authentication.

---

### Procedure

- 1 Create or edit the `locked.properties` file in the SSL gateway configuration folder on the View Connection Server or security server host.

For example: `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`

- 2 To configure the View server's protocol, add the `serverProtocol` property and set it to `http`.

The value `http` must be typed in lower case.

- 3 (Optional) Add properties to configure a non-default HTTP listening port and a network interface on the View server.
  - To change the HTTP listening port from 80, set `serverPortNonSSL` to another port number to which the intermediate device is configured to connect.
  - If the View server has more than one network interface, and you intend the server to listen for HTTP connections on only one interface, set `serverHostNonSSL` to the IP address of that network interface.
- 4 Save the `locked.properties` file.
- 5 Restart the View Connection Server service or security server service to make your changes take effect.

#### Example: `locked.properties` file

This file allows non-SSL HTTP connections to a View server. The IP address of the View server's client-facing network interface is 10.20.30.40. The server uses the default port 80 to listen for HTTP connections. The value `http` must be lower case.

```
serverProtocol=http
serverHostNonSSL=10.20.30.40
```

## Configure the Gateway Location for a Horizon Connection Server or Security Server Host

By default, Horizon Connection Server instances set the gateway location to `Internal` and security servers set the gateway location to `External`. You can change the default gateway location by setting the `gatewayLocation` property in the `locked.properties` file.

The gateway location determines the value of the `ViewClient_Broker_GatewayLocation` registry key in a remote desktop. You can use this value with Smart Policies to create a policy that takes effect only if a user connects to a remote desktop from inside or outside your corporate network. For more information, see "Using Smart Policies" in the *Configuring Remote Desktop Features in Horizon 7* document.

### Procedure

- 1 Create or edit the `locked.properties` file in the SSL gateway configuration folder on the Horizon Connection Server or security server host.  
 For example: `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`  
 The properties in the `locked.properties` file are case sensitive.
- 2 Add the following line to the `locked.properties` file:  

```
gatewayLocation=value
```

*value* can be either `External` or `Internal`. `External` indicates that the gateway is available for users outside the corporate network. `Internal` indicates that the gateway is available only for users inside the corporate network.

For example: `gatewayLocation=External`
- 3 Save the `locked.properties` file.
- 4 Restart the VMware Horizon Connection Server service or the VMware Horizon Security Server service to make your changes take effect.

## Disable or Enable View Connection Server

You can disable a View Connection Server instance to prevent users from logging in to their remote desktops and applications. After you disable an instance, you can enable it again.

When you disable a View Connection Server instance, users who are currently logged in to remote desktops and applications are not affected.

Your View deployment determines how users are affected by disabling an instance.

- If this is a single, standalone View Connection Server instance, users cannot log in to their remote desktops or applications. They cannot connect to View Connection Server.
- If this is a replicated View Connection Server instance, your network topology determines whether users can be routed to another replicated instance. If users can access another instance, they can log in to their remote desktops and applications.

### Procedure

- 1 In View Administrator, select **View Configuration > Servers**.
- 2 On the **Connection Servers** tab, select the View Connection Server instance.
- 3 Click **Disable**.

You can enable the instance again by clicking **Enable**.

## Edit the External URLs

You can use View Administrator to edit external URLs for View Connection Server instances and security servers.

By default, a View Connection Server or security server host can be contacted only by tunnel clients that reside within the same network. Tunnel clients that run outside of your network must use a client-resolvable URL to connect to a View Connection Server or security server host.

When users connect to remote desktops with the PCoIP display protocol, Horizon Client can make a further connection to the PCoIP Secure Gateway on the View Connection Server or security server host. To use the PCoIP Secure Gateway, a client system must have access to an IP address that allows the client to reach the View Connection Server or security server host. You specify this IP address in the PCoIP external URL.

A third URL allows users to make secure connections through the Blast Secure Gateway.

The secure tunnel external URL, PCoIP external URL, and Blast external URL must be the addresses that client systems use to reach this host.

---

**NOTE** You cannot edit the external URLs for a security server that has not been upgraded to View Connection Server 4.5 or later.

---

### Procedure

- 1 In View Administrator, select **View Configuration > Servers**.

Option	Action
<b>View Connection Server instance</b>	Select the View Connection Server instance on the <b>Connection Servers</b> tab and click <b>Edit</b> .
<b>Security server</b>	Select the security server on the <b>Security Servers</b> tab and click <b>Edit</b> .

- 2 Type the secure tunnel external URL in the **External URL** text box.

The URL must contain the protocol, client-resolvable host name and port number.

For example: `https://view.example.com:443`

---

**NOTE** You can use the IP address if you have to access a View Connection Server instance or security server when the host name is not resolvable. However, the host that you contact will not match the SSL certificate that is configured for the View Connection Server instance or security server, resulting in blocked access or access with reduced security.

---

- 3 Type the PCoIP Secure Gateway external URL in the **PCoIP External URL** text box.

Specify the PCoIP external URL as an IP address with the port number 4172. Do not include a protocol name.

For example: `10.20.30.40:4172`

The URL must contain the IP address and port number that a client system can use to reach this security server or View Connection Server instance.

- 4 Type the Blast Secure Gateway external URL in the **Blast External URL** text box.

The URL must contain the HTTPS protocol, client-resolvable host name, and port number.

For example: `https://myserver.example.com:8443`

By default, the URL includes the FQDN of the secure tunnel external URL and the default port number, 8443. The URL must contain the FQDN and port number that a client system can use to reach this host.

- 5 Verify that all addresses in this dialog allow client systems to reach this host.

- 6 Click **OK** to save your changes.

The external URLs are updated immediately. You do not need to restart the View Connection Server service or the security server service for the changes to take effect.

## Join or Withdraw from the Customer Experience Program

When you install View Connection Server with a new configuration, you can choose to participate in a customer experience improvement program. If you change your mind about participating after the installation, you can join or withdraw from the program by using View Administrator.

If you participate in the program, VMware collects anonymous data about your deployment in order to improve VMware's response to user requirements. No data that identifies your organization is collected.

To review the list of fields from which data is collected, including the fields that are made anonymous, see ["Information Collected by the Customer Experience Improvement Program,"](#) on page 142.

### Procedure

- 1 In View Administrator, select **View Configuration > Product Licensing and Usage**.
- 2 In the Customer Experience Program pane, click **Edit Settings**.
- 3 Decide whether to participate in or withdraw from the program by selecting or deselecting the **Send anonymous data to VMware** checkbox.
- 4 (Optional) If you participate, you can select the geographic location, type of business, and number of employees in your organization.
- 5 Click **OK**.

## View LDAP Directory

View LDAP is the data repository for all View configuration information. View LDAP is an embedded Lightweight Directory Access Protocol (LDAP) directory that is provided with the View Connection Server installation.

View LDAP contains standard LDAP directory components that are used by View.

- View schema definitions
- Directory information tree (DIT) definitions
- Access control lists (ACLs)

View LDAP contains directory entries that represent View objects.

- Remote desktop entries that represent each accessible desktop. Each entry contains references to the Foreign Security Principal (FSP) entries of Windows users and groups in Active Directory who are authorized to use the desktop.
- Remote desktop pool entries that represent multiple desktops managed together
- Virtual machine entries that represent the vCenter Server virtual machine for each remote desktop
- View component entries that store configuration settings

View LDAP also contains a set of View plug-in DLLs that provide automation and notification services for other View components.

---

**NOTE** Security server instances do not contain a View LDAP directory.

---

## LDAP Replication

When you install a replicated instance of View Connection Server, View copies the View LDAP configuration data from the existing View Connection Server instance. Identical View LDAP configuration data is maintained on all View Connection Server instances in the replicated group. When a change is made on one instance, the updated information is copied to the other instances.

If a replicated instance fails, the other instances in the group continue to operate. When the failed instance resumes activity, its configuration is updated with the changes that took place during the outage. With Horizon 7 and later releases, a replication status check is performed every 15 minutes to determine whether each instance can communicate with the other servers in the replicated group and whether each instance can fetch LDAP updates from the other servers in the group.

You can use the dashboard in View Administrator to check the replication status. If any View Connection Server instances have a red icon in the dashboard, click the icon to see the replication status. Replication might be impaired for any of the following reasons:

- A firewall might be blocking communication
- The VMware VDMDS service might be stopped on a View Connection Server instance
- The VMware VDMDS DSA options might be blocking the replications
- A network problem has occurred

By default, the replication check occurs every 15 minutes. You can use ADSI Edit on a View Connection Server instance to change the interval. To set the number of minutes, connect to **DC=vdi,DC=vmware,DC=int** and edit the **pae-ReplicationStatusDataExpiryInMins** attribute on the **CN=Common,OU=Global,OU=Properties** object.

The **pae-ReplicationStatusDataExpiryInMins** attribute value should be between 10 minutes and 1440 minutes (one day). If the attribute value is less than 10 minutes, View treats it as 10 minutes. If the attribute value is greater than 1440, View treats it as 1440 minutes.



## Setting Up Smart Card Authentication

---

For added security, you can configure a View Connection Server instance or security server so that users and administrators can authenticate by using smart cards.

A smart card is a small plastic card that contains a computer chip. The chip, which is like a miniature computer, includes secure storage for data, including private keys and public key certificates. One type of smart card used by the United States Department of Defense is called a Common Access Card (CAC).

With smart card authentication, a user or administrator inserts a smart card into a smart card reader attached to the client computer and enters a PIN. Smart card authentication provides two-factor authentication by verifying both what the person has (the smart card) and what the person knows (the PIN).

See the *View Installation* document for information about hardware and software requirements for implementing smart card authentication. The Microsoft TechNet Web site includes detailed information on planning and implementing smart card authentication for Windows systems.

To use smart cards, client machines must have smart card middleware and a smart card reader. To install certificates on smart cards, you must set up a computer to act as an enrollment station. For information about whether a particular type of Horizon Client supports smart cards, see the Horizon Client documentation at [https://www.vmware.com/support/viewclients/doc/viewclients\\_pubs.html](https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html).

This chapter includes the following topics:

- “Logging In with a Smart Card,” on page 44
- “Configure Smart Card Authentication on View Connection Server,” on page 44
- “Configure Smart Card Authentication on Third-Party Solutions,” on page 49
- “Prepare Active Directory for Smart Card Authentication,” on page 50
- “Verify Your Smart Card Authentication Configuration,” on page 52
- “Using Smart Card Certificate Revocation Checking,” on page 53

## Logging In with a Smart Card

When a user or administrator inserts a smart card into a smart card reader, the user certificates on the smart card are copied to the local certificate store on the client system if the client operating system is Windows. The certificates in the local certificate store are available to all of the applications running on the client computer, including Horizon Client.

When a user or administrator initiates a connection to a View Connection Server instance or security server that is configured for smart card authentication, the View Connection Server instance or security server sends a list of trusted certificate authorities (CAs) to the client system. The client system checks the list of trusted CAs against the available user certificates, selects a suitable certificate, and then prompts the user or administrator to enter a smart card PIN. If there are multiple valid user certificates, the client system prompts the user or administrator to select a certificate.

The client system sends the user certificate to the View Connection Server instance or security server, which verifies the certificate by checking the certificate trust and validity period. Typically, users and administrators can successfully authenticate if their user certificate is signed and valid. If certificate revocation checking is configured, users or administrators who have revoked user certificates are prevented from authenticating.

In some environments, a user's smart card certificate can map to multiple Active Directory domain user accounts. A user might have multiple accounts with administrator privileges and needs to specify which account to use in the Username hint field during smart card login. To make the Username hint field appear on the Horizon Client login dialog box, the administrator must enable the smart card user name hints feature for the Connection Server instance in View Administrator. The smart card user can then enter a user name or UPN in the Username hint field during smart card login.

If your environment uses an Access Point appliance for secure external access, you must configure the Access Point appliance to support the smart card user name hints feature. The smart card user name hints feature is supported only with Access Point 2.7.2 and later. For information about enabling the smart card user name hints feature in Access Point, see the *Deploying and Configuring Access Point* document.

Display protocol switching is not supported with smart card authentication in Horizon Client. To change display protocols after authenticating with a smart card in Horizon Client, a user must log off and log on again.

## Configure Smart Card Authentication on View Connection Server

To configure smart card authentication, you must obtain a root certificate and add it to a server truststore file, modify View Connection Server configuration properties, and configure smart card authentication settings. Depending on your particular environment, you might need to perform additional steps.

### Procedure

- 1 [Obtain the Certificate Authority Certificates](#) on page 45

You must obtain all applicable CA (certificate authority) certificates for all trusted user certificates on the smart cards presented by your users and administrators. These certificates include root certificates and can include intermediate certificates if the user's smart card certificate was issued by an intermediate certificate authority.

- 2 [Obtain the CA Certificate from Windows](#) on page 45

If you have a CA-signed user certificate or a smart card that contains one, and Windows trusts the root certificate, you can export the root certificate from Windows. If the issuer of the user certificate is an intermediate certificate authority, you can export that certificate.

- 3 [Add the CA Certificate to a Server Truststore File](#) on page 46  
You must add root certificates, intermediate certificates, or both to a server truststore file for all users and administrators that you trust. View Connection Server instances and security servers use this information to authenticate smart card users and administrators.
- 4 [Modify View Connection Server Configuration Properties](#) on page 47  
To enable smart card authentication, you must modify View Connection Server configuration properties on your View Connection Server or security server host.
- 5 [Configure Smart Card Settings in View Administrator](#) on page 47  
You can use View Administrator to specify settings to accommodate different smart card authentication scenarios.

## Obtain the Certificate Authority Certificates

You must obtain all applicable CA (certificate authority) certificates for all trusted user certificates on the smart cards presented by your users and administrators. These certificates include root certificates and can include intermediate certificates if the user's smart card certificate was issued by an intermediate certificate authority.

If you do not have the root or intermediate certificate of the CA that signed the certificates on the smart cards presented by your users and administrators, you can export the certificates from a CA-signed user certificate or a smart card that contains one. See [“Obtain the CA Certificate from Windows,”](#) on page 45.

### Procedure

- ◆ Obtain the CA certificates from one of the following sources.
  - A Microsoft IIS server running Microsoft Certificate Services. See the Microsoft TechNet Web site for information on installing Microsoft IIS, issuing certificates, and distributing certificates in your organization.
  - The public root certificate of a trusted CA. This is the most common source of a root certificate in environments that already have a smart card infrastructure and a standardized approach to smart card distribution and authentication.

### What to do next

Add the root certificate, intermediate certificate, or both to a server truststore file.

## Obtain the CA Certificate from Windows

If you have a CA-signed user certificate or a smart card that contains one, and Windows trusts the root certificate, you can export the root certificate from Windows. If the issuer of the user certificate is an intermediate certificate authority, you can export that certificate.

### Procedure

- 1 If the user certificate is on a smart card, insert the smart card into the reader to add the user certificate to your personal store.  
If the user certificate does not appear in your personal store, use the reader software to export the user certificate to a file. This file is used in Step 4 of this procedure.
- 2 In Internet Explorer, select **Tools > Internet Options**.
- 3 On the **Content** tab, click **Certificates**.
- 4 On the **Personal** tab, select the certificate you want to use and click **View**.  
If the user certificate does not appear on the list, click **Import** to manually import it from a file. After the certificate is imported, you can select it from the list.

- 5 On the **Certification Path** tab, select the certificate at the top of the tree and click **View Certificate**.  
If the user certificate is signed as part of a trust hierarchy, the signing certificate might be signed by another higher-level certificate. Select the parent certificate (the one that actually signed the user certificate) as your root certificate. In some cases, the issuer might be an intermediate CA.
- 6 On the **Details** tab, click **Copy to File**.  
The Certificate Export Wizard appears.
- 7 Click **Next > Next** and type a name and location for the file that you want to export.
- 8 Click **Next** to save the file as a root certificate in the specified location.

### What to do next

Add the CA certificate to a server truststore file.

## Add the CA Certificate to a Server Truststore File

You must add root certificates, intermediate certificates, or both to a server truststore file for all users and administrators that you trust. View Connection Server instances and security servers use this information to authenticate smart card users and administrators.

### Prerequisites

- Obtain the root or intermediate certificates that were used to sign the certificates on the smart cards presented by your users or administrators. See [“Obtain the Certificate Authority Certificates,”](#) on page 45 and [“Obtain the CA Certificate from Windows,”](#) on page 45.

---

**IMPORTANT** These certificates can include intermediate certificates if the user's smart card certificate was issued by an intermediate certificate authority.

---

- Verify that the `keytool` utility is added to the system path on your View Connection Server or security server host. See the *View Installation* document for more information.

### Procedure

- 1 On your View Connection Server or security server host, use the `keytool` utility to import the root certificate, intermediate certificate, or both into the server truststore file.

For example: `keytool -import -alias alias -file root_certificate -keystore truststorefile.key`

In this command, *alias* is a unique case-sensitive name for a new entry in the truststore file, *root\_certificate* is the root or intermediate certificate that you obtained or exported, and *truststorefile.key* is the name of the truststore file that you are adding the root certificate to. If the file does not exist, it is created in the current directory.

---

**NOTE** The `keytool` utility might prompt you to create a password for the truststore file. You will be asked to provide this password if you need to add additional certificates to the truststore file at a later time.

---

- 2 Copy the truststore file to the SSL gateway configuration folder on the View Connection Server or security server host.

For example: `install_directory\VMware\VMware View\Server\sslgateway\conf\truststorefile.key`

### What to do next

Modify View Connection Server configuration properties to enable smart card authentication.

## Modify View Connection Server Configuration Properties

To enable smart card authentication, you must modify View Connection Server configuration properties on your View Connection Server or security server host.

### Prerequisites

Add the CA (certificate authority) certificates for all trusted user certificates to a server truststore file. These certificates include root certificates and can include intermediate certificates if the user's smart card certificate was issued by an intermediate certificate authority.

### Procedure

- 1 Create or edit the `locked.properties` file in SSL gateway configuration folder on the View Connection Server or security server host.

For example: `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`

- 2 Add the `trustKeyfile`, `trustStoretype`, and `useCertAuth` properties to the `locked.properties` file.
  - a Set `trustKeyfile` to the name of your truststore file.
  - b Set `trustStoretype` to `jks`.
  - c Set `useCertAuth` to `true` to enable certificate authentication.
- 3 Restart the View Connection Server service or security server service to make your changes take effect.

### Example: locked.properties File

The file shown specifies that the root certificate for all trusted users is located in the file `lonqa.key`, sets the trust store type to `jks`, and enables certificate authentication.

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
```

### What to do next

If you configured smart card authentication for a View Connection Server instance, configure smart card authentication settings in View Administrator. You do not need to configure smart card authentication settings for a security server. Settings that are configured on a View Connection Server instance are also applied to a paired security server.

## Configure Smart Card Settings in View Administrator

You can use View Administrator to specify settings to accommodate different smart card authentication scenarios.

When you configure these settings on a View Connection Server instance, the settings are also applied to paired security servers.

### Prerequisites

- Modify View Connection Server configuration properties on your View Connection Server host.
- Verify that Horizon clients make HTTPS connections directly to your View Connection Server or security server host. Smart card authentication is not supported if you off-load SSL to an intermediate device.

### Procedure

- 1 In View Administrator, select **View Configuration > Servers**.

- 2 On the **Connection Servers** tab, select the View Connection Server instance and click **Edit**.
- 3 To configure smart card authentication for remote desktop and application users, perform these steps.
  - a On the **Authentication** tab, select a configuration option from the **Smart card authentication for users** drop-down menu in the View Authentication section.

Option	Action
<b>Not allowed</b>	Smart card authentication is disabled on the View Connection Server instance.
<b>Optional</b>	Users can use smart card authentication or password authentication to connect to the View Connection Server instance. If smart card authentication fails, the user must provide a password.
<b>Required</b>	<p>Users are required to use smart card authentication when connecting to the View Connection Server instance.</p> <p>When smart card authentication is required, authentication fails for users who select the <b>Log in as current user</b> check box when they connect to the View Connection Server instance. These users must reauthenticate with their smart card and PIN when they log in to View Connection Server.</p> <p><b>NOTE</b> Smart card authentication replaces Windows password authentication only. If SecurID is enabled, users are required to authenticate by using both SecurID and smart card authentication.</p>

- b Configure the smart card removal policy.

You cannot configure the smart card removal policy when smart card authentication is set to **Not Allowed**.

Option	Action
<b>Disconnect users from View Connection Server when they remove their smart cards.</b>	Select the <b>Disconnect user sessions on smart card removal</b> check box.
<b>Keep users connected to View Connection Server when they remove their smart cards and let them start new desktop or application sessions without reauthenticating.</b>	Deselect the <b>Disconnect user sessions on smart card removal</b> check box.

The smart card removal policy does not apply to users who connect to the View Connection Server instance with the **Log in as current user** check box selected, even if they log in to their client system with a smart card.

- c Configure the smart card user name hints feature.

You cannot configure the smart card user name hints feature when smart card authentication is set to **Not Allowed**.

Option	Action
<b>Enable users to use a single smart card certificate to authenticate to multiple user accounts.</b>	Select the <b>Allow smart card user name hints</b> check box.
<b>Disable users from using a single smart card certificate to authenticate to multiple user accounts.</b>	Deselect the <b>Allow smart card user name hints</b> check box.

- 4 To configure smart card authentication for administrators logging in to View Administrator, click the **Authentication** tab and select a configuration option from the **Smart card authentication for administrators** drop-down menu in the View Administration Authentication section.

Option	Action
<b>Not allowed</b>	Smart card authentication is disabled on the View Connection Server instance.
<b>Optional</b>	Administrators can use smart card authentication or password authentication to log in to the View Administrator. If smart card authentication fails, the administrator must provide a password.
<b>Required</b>	Administrators are required to use smart card authentication when they log in to View Administrator.

- 5 Click **OK**.
- 6 Restart the View Connection Server service.

You must restart the View Connection Server service for changes to smart card settings to take effect, with one exception. You can change smart card authentication settings between **Optional** and **Required** without having to restart the View Connection Server service.

Currently logged in user and administrators are not affected by changes to smart card settings.

#### What to do next

Prepare Active Directory for smart card authentication, if required. See [“Prepare Active Directory for Smart Card Authentication,”](#) on page 50.

Verify your smart card authentication configuration. See [“Verify Your Smart Card Authentication Configuration,”](#) on page 52.

## Configure Smart Card Authentication on Third-Party Solutions

Third-party solutions such as load balancers and gateways can perform smart card authentication by passing a SAML assertion that contains the smart card's X.590 certificate and encrypted PIN.

This topic outlines the tasks involved in setting up third-party solutions to provide the relevant X.590 certificate to View Connection Server after the certificate has been validated by the partner device. Because this feature uses SAML authentication, one of the tasks is to create a SAML authenticator in View Administrator.

For information about configuring smart card authentication on Access Point, see *Deploying and Configuring Access Point*.

#### Procedure

- 1 Create a SAML authenticator for the third-party gateway or load balancer.  
See [“Configure a SAML Authenticator in View Administrator,”](#) on page 62.
- 2 Extend the expiration period of the View Connection Server metadata so that remote sessions are not terminated after only 24 hours.  
See [“Change the Expiration Period for Service Provider Metadata on View Connection Server,”](#) on page 64.
- 3 If necessary, configure the third-party device to use service provider metadata from View Connection Server.  
See the product documentation for the third-party device.

- 4 Configure smart card settings on the third-party device.
- See the product documentation for the third-party device.

## Prepare Active Directory for Smart Card Authentication

You might need to perform certain tasks in Active Directory when you implement smart card authentication.

- [Add UPNs for Smart Card Users](#) on page 50  
Because smart card logins rely on user principal names (UPNs), the Active Directory accounts of users and administrators that use smart cards to authenticate in View must have a valid UPN.
- [Add the Root Certificate to the Enterprise NTAAuth Store](#) on page 51  
If you use a CA to issue smart card login or domain controller certificates, you must add the root certificate to the Enterprise NTAAuth store in Active Directory. You do not need to perform this procedure if the Windows domain controller acts as the root CA.
- [Add the Root Certificate to Trusted Root Certification Authorities](#) on page 51  
If you use a certification authority (CA) to issue smart card login or domain controller certificates, you must add the root certificate to the Trusted Root Certification Authorities group policy in Active Directory. You do not need to perform this procedure if the Windows domain controller acts as the root CA.
- [Add an Intermediate Certificate to Intermediate Certification Authorities](#) on page 52  
If you use an intermediate certification authority (CA) to issue smart card login or domain controller certificates, you must add the intermediate certificate to the Intermediate Certification Authorities group policy in Active Directory.

## Add UPNs for Smart Card Users

Because smart card logins rely on user principal names (UPNs), the Active Directory accounts of users and administrators that use smart cards to authenticate in View must have a valid UPN.

If the domain a smart card user resides in is different from the domain that your root certificate was issued from, you must set the user's UPN to the Subject Alternative Name (SAN) contained in the root certificate of the trusted CA. If your root certificate was issued from a server in the smart card user's current domain, you do not need to modify the user's UPN.

---

**NOTE** You might need to set the UPN for built-in Active Directory accounts, even if the certificate is issued from the same domain. Built-in accounts, including Administrator, do not have a UPN set by default.

---

### Prerequisites

- Obtain the SAN contained in the root certificate of the trusted CA by viewing the certificate properties.
- If the ADSI Edit utility is not present on your Active Directory server, download and install the appropriate Windows Support Tools from the Microsoft Web site.

### Procedure

- 1 On your Active Directory server, start the ADSI Edit utility.
- 2 In the left pane, expand the domain the user is located in and double-click CN=Users.
- 3 In the right pane, right-click the user and then click **Properties**.
- 4 Double-click the userPrincipalName attribute and type the SAN value of the trusted CA certificate.
- 5 Click **OK** to save the attribute setting.

## Add the Root Certificate to the Enterprise NTAAuth Store

If you use a CA to issue smart card login or domain controller certificates, you must add the root certificate to the Enterprise NTAAuth store in Active Directory. You do not need to perform this procedure if the Windows domain controller acts as the root CA.

### Procedure

- ◆ On your Active Directory server, use the `certutil` command to publish the certificate to the Enterprise NTAAuth store.

For example: `certutil -dspublish -f path_to_root_CA_cert NTAAuthCA`

The CA is now trusted to issue certificates of this type.

## Add the Root Certificate to Trusted Root Certification Authorities

If you use a certification authority (CA) to issue smart card login or domain controller certificates, you must add the root certificate to the Trusted Root Certification Authorities group policy in Active Directory. You do not need to perform this procedure if the Windows domain controller acts as the root CA.

### Procedure

- 1 On the Active Directory server, navigate to the Group Policy Management plug-in.

AD Version	Navigation Path
Windows 2003	<ol style="list-style-type: none"> <li>a Select <b>Start &gt; All Programs &gt; Administrative Tools &gt; Active Directory Users and Computers</b>.</li> <li>b Right-click your domain and click <b>Properties</b>.</li> <li>c On the <b>Group Policy</b> tab, click <b>Open</b> to open the Group Policy Management plug-in.</li> <li>d Right-click <b>Default Domain Policy</b>, and click <b>Edit</b>.</li> </ol>
Windows 2008	<ol style="list-style-type: none"> <li>a Select <b>Start &gt; Administrative Tools &gt; Group Policy Management</b>.</li> <li>b Expand your domain, right-click <b>Default Domain Policy</b>, and click <b>Edit</b>.</li> </ol>

- 2 Expand the **Computer Configuration** section and open **Windows Settings\Security Settings\Public Key**.
- 3 Right-click **Trusted Root Certification Authorities** and select **Import**.
- 4 Follow the prompts in the wizard to import the root certificate (for example, rootCA.cer) and click **OK**.
- 5 Close the Group Policy window.

All of the systems in the domain now have a copy of the root certificate in their trusted root store.

### What to do next

If an intermediate certification authority (CA) issues your smart card login or domain controller certificates, add the intermediate certificate to the Intermediate Certification Authorities group policy in Active Directory. See [“Add an Intermediate Certificate to Intermediate Certification Authorities,”](#) on page 52.

## Add an Intermediate Certificate to Intermediate Certification Authorities

If you use an intermediate certification authority (CA) to issue smart card login or domain controller certificates, you must add the intermediate certificate to the Intermediate Certification Authorities group policy in Active Directory.

### Procedure

- 1 On the Active Directory server, navigate to the Group Policy Management plug-in.

AD Version	Navigation Path
<b>Windows 2003</b>	<ol style="list-style-type: none"> <li>a Select <b>Start &gt; All Programs &gt; Administrative Tools &gt; Active Directory Users and Computers</b>.</li> <li>b Right-click your domain and click <b>Properties</b>.</li> <li>c On the <b>Group Policy</b> tab, click <b>Open</b> to open the Group Policy Management plug-in.</li> <li>d Right-click <b>Default Domain Policy</b>, and click <b>Edit</b>.</li> </ol>
<b>Windows 2008</b>	<ol style="list-style-type: none"> <li>a Select <b>Start &gt; Administrative Tools &gt; Group Policy Management</b>.</li> <li>b Expand your domain, right-click <b>Default Domain Policy</b>, and click <b>Edit</b>.</li> </ol>

- 2 Expand the **Computer Configuration** section and open the policy for **Windows Settings\Security Settings\Public Key**.
- 3 Right-click **Intermediate Certification Authorities** and select **Import**.
- 4 Follow the prompts in the wizard to import the intermediate certificate (for example, intermediateCA.cer) and click **OK**.
- 5 Close the Group Policy window.

All of the systems in the domain now have a copy of the intermediate certificate in their intermediate certification authority store.

## Verify Your Smart Card Authentication Configuration

After you set up smart card authentication for the first time, or when smart card authentication is not working correctly, you should verify your smart card authentication configuration.

### Procedure

- Verify that each client system has smart card middleware, a smart card with a valid certificate, and a smart card reader. For end users, verify that they have Horizon Client.

See the documentation provided by your smart card vendor for information on configuring smart card software and hardware.

- On each client system, select **Start > Settings > Control Panel > Internet Options > Content > Certificates > Personal** to verify that certificates are available for smart card authentication.

When a user or administrator inserts a smart card into the smart card reader, Windows copies certificates from the smart card to the user's computer. Applications on the client system, including Horizon Client, can use these certificates.

- In the locked.properties file on the View Connection Server or security server host, verify that the useCertAuth property is set to **true** and is spelled correctly.

The locked.properties file is located in *install\_directory\VMware\VMware View\Server\sslgateway\conf*. The useCertAuth property is commonly misspelled as userCertAuth.

- If you configured smart card authentication on a View Connection Server instance, check the smart card authentication setting in View Administrator.
  - a Select **View Configuration > Servers**.
  - b On the **Connection Servers** tab, select the View Connection Server instance and click **Edit**.
  - c If you configured smart card authentication for users, on the **Authentication** tab, verify that **Smart card authentication for users** is set to either **Optional** or **Required**.
  - d If you configured smart card authentication for administrators, on the **Authentication** tab, verify that **Smart card authentication for administrators** is set to either **Optional** or **Required**.

You must restart the View Connection Server service for changes to smart card settings to take effect.
- If the domain a smart card user resides in is different from the domain your root certificate was issued from, verify that the user's UPN is set to the SAN contained in the root certificate of the trusted CA.
  - a Find the SAN contained in the root certificate of the trusted CA by viewing the certificate properties.
  - b On your Active Directory server, select **Start > Administrative Tools > Active Directory Users and Computers**.
  - c Right-click the user in the **Users** folder and select **Properties**.

The UPN appears in the **User logon name** text boxes on the **Account** tab.
- If smart card users select the PCoIP display protocol or the VMware Blast display protocol to connect to single-session desktops, verify that the View Agent or Horizon Agent component called Smartcard Redirection is installed on the single-user machines. The smart card feature lets users log in to single-session desktops with smart cards. RDS hosts, which have the Remote Desktop Services role installed, support the smart card feature automatically and you do not need to install the feature.
- Check the log files in *drive:\Documents and Settings\All Users\Application Data\VMware\VDM\logs* on the View Connection Server or security server host for messages stating that smart card authentication is enabled.

## Using Smart Card Certificate Revocation Checking

You can prevent users who have revoked user certificates from authenticating with smart cards by configuring certificate revocation checking. Certificates are often revoked when a user leaves an organization, loses a smart card, or moves from one department to another.

View supports certificate revocation checking with certificate revocation lists (CRLs) and with the Online Certificate Status Protocol (OCSP). A CRL is a list of revoked certificates published by the CA that issued the certificates. OCSP is a certificate validation protocol that is used to get the revocation status of an X.509 certificate.

You can configure certificate revocation checking on a View Connection Server instance or on a security server. When a View Connection Server instance is paired with a security server, you configure certificate revocation checking on the security server. The CA must be accessible from the View Connection Server or security server host.

You can configure both CRL and OCSP on the same View Connection Server instance or security server. When you configure both types of certificate revocation checking, View attempts to use OCSP first and falls back to CRL if OCSP fails. View does not fall back to OCSP if CRL fails.

- [Logging in with CRL Checking](#) on page 54
 

When you configure CRL checking, View constructs and reads a CRL to determine the revocation status of a user certificate.

- [Logging in with OSCP Certificate Revocation Checking](#) on page 54  
When you configure OSCP certificate revocation checking, View sends a request to an OSCP Responder to determine the revocation status of a specific user certificate. View uses an OSCP signing certificate to verify that the responses it receives from the OSCP Responder are genuine.
- [Configure CRL Checking](#) on page 54  
When you configure CRL checking, View reads a CRL to determine the revocation status of a smart card user certificate.
- [Configure OSCP Certificate Revocation Checking](#) on page 55  
When you configure OSCP certificate revocation checking, View sends a verification request to an OSCP Responder to determine the revocation status of a smart card user certificate.
- [Smart Card Certificate Revocation Checking Properties](#) on page 56  
You set values in the `locked.properties` file to enable and configure smart card certificate revocation checking.

## Logging in with CRL Checking

When you configure CRL checking, View constructs and reads a CRL to determine the revocation status of a user certificate.

If a certificate is revoked and smart card authentication is optional, the Enter your user name and password dialog box appears and the user must provide a password to authenticate. If smart card authentication is required, the user receives an error message and is not allowed to authenticate. The same events occur if View cannot read the CRL.

## Logging in with OSCP Certificate Revocation Checking

When you configure OSCP certificate revocation checking, View sends a request to an OSCP Responder to determine the revocation status of a specific user certificate. View uses an OSCP signing certificate to verify that the responses it receives from the OSCP Responder are genuine.

If the user certificate is revoked and smart card authentication is optional, the Enter your user name and password dialog box appears and the user must provide a password to authenticate. If smart card authentication is required, the user receives an error message and is not allowed to authenticate.

View falls back to CRL checking if it does not receive a response from the OSCP Responder or if the response is invalid.

## Configure CRL Checking

When you configure CRL checking, View reads a CRL to determine the revocation status of a smart card user certificate.

### Prerequisites

Familiarize yourself with the `locked.properties` file properties for CRL checking. See [“Smart Card Certificate Revocation Checking Properties,”](#) on page 56.

### Procedure

- 1 Create or edit the `locked.properties` file in the SSL gateway configuration folder on the View Connection Server or security server host.

For example: `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`

- 2 Add the `enableRevocationChecking` and `crlLocation` properties to the `locked.properties` file.
  - a Set `enableRevocationChecking` to **true** to enable smart card certificate revocation checking.
  - b Set `crlLocation` to the location of the CRL. The value can be a URL or a file path.
- 3 Restart the View Connection Server service or security server service to make your changes take effect.

### Example: locked.properties File

The file shown enables smart card authentication and smart card certificate revocation checking, configures CRL checking, and specifies a URL for the CRL location.

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
enableRevocationChecking=true
crlLocation=http://root.ocsp.net/certEnroll/ocsp-ROOT_CA.crl
```

## Configure OCSP Certificate Revocation Checking

When you configure OCSP certificate revocation checking, View sends a verification request to an OCSP Responder to determine the revocation status of a smart card user certificate.

### Prerequisites

Familiarize yourself with the `locked.properties` file properties for OCSP certificate revocation checking. See [“Smart Card Certificate Revocation Checking Properties,”](#) on page 56.

### Procedure

- 1 Create or edit the `locked.properties` file in the SSL gateway configuration folder on the View Connection Server or security server host.  
  
For example: `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`
- 2 Add the `enableRevocationChecking`, `enableOCSP`, `ocspURL`, and `ocspSigningCert` properties to the `locked.properties` file.
  - a Set `enableRevocationChecking` to **true** to enable smart card certificate revocation checking.
  - b Set `enableOCSP` to **true** to enable OCSP certificate revocation checking.
  - c Set `ocspURL` to the URL of the OCSP Responder.
  - d Set `ocspSigningCert` to the location of the file that contains the OCSP Responder's signing certificate.
- 3 Restart the View Connection Server service or security server service to make your changes take effect.

### Example: locked.properties File

The file shown enables smart card authentication and smart card certificate revocation checking, configures both CRL and OCSP certificate revocation checking, specifies the OCSP Responder location, and identifies the file that contains the OCSP signing certificate.

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
enableRevocationChecking=true
enableOCSP=true
allowCertCRLs=true
ocspSigningCert=te-ca.signing.cer
ocspURL=http://te-ca.lonqa.int/ocsp
```

## Smart Card Certificate Revocation Checking Properties

You set values in the `locked.properties` file to enable and configure smart card certificate revocation checking.

[Table 3-1](#) lists the `locked.properties` file properties for certificate revocation checking.

**Table 3-1.** Properties for Smart Card Certificate Revocation Checking

Property	Description
<code>enableRevocationChecking</code>	Set this property to <b>true</b> to enable certificate revocation checking.  When this property is set to <b>false</b> , certificate revocation checking is disabled and all other certificate revocation checking properties are ignored.  The default value is <b>false</b> .
<code>crlLocation</code>	Specifies the location of the CRL, which can be either a URL or a file path.  If you do not specify a URL, or if the specified URL is invalid, View uses the list of CRLs on the user certificate if <code>allowCertCRLs</code> is set to <b>true</b> or is not specified.  If View cannot access a CRL, CRL checking fails.
<code>allowCertCRLs</code>	When this property is set to <b>true</b> , View extracts a list of CRLs from the user certificate.  The default value is <b>true</b> .
<code>enableOCSP</code>	Set this property to <b>true</b> to enable OCSP certificate revocation checking.  The default value is <b>false</b> .
<code>ocspURL</code>	Specifies the URL of an OCSP Responder.
<code>ocspResponderCert</code>	Specifies the file that contains the OCSP Responder's signing certificate. View uses this certificate to verify that the OCSP Responder's responses are genuine.
<code>ocspSendNonce</code>	When this property is set to <b>true</b> , a nonce is sent with OCSP requests to prevent repeated responses.  The default value is <b>false</b> .
<code>ocspCRLFailover</code>	When this property is set to <b>true</b> , View uses CRL checking if OCSP certificate revocation checking fails.  The default value is <b>true</b> .

# Setting Up Other Types of User Authentication

# 4

View uses your existing Active Directory infrastructure for user and administrator authentication and management. You can also integrate View with other forms of authentication besides smart cards, such as biometric authentication or two-factor authentication solutions, such as RSA SecurID and RADIUS, to authenticate remote desktop and application users.

This chapter includes the following topics:

- [“Using Two-Factor Authentication,”](#) on page 57
- [“Using SAML Authentication,”](#) on page 61
- [“Configure Biometric Authentication,”](#) on page 65

## Using Two-Factor Authentication

You can configure a View Connection Server instance so that users are required to use RSA SecurID authentication or RADIUS (Remote Authentication Dial-In User Service) authentication.

- RADIUS support offers a wide range of alternative two-factor token-based authentication options.
- View also provides an open standard extension interface to allow third-party solution providers to integrate advanced authentication extensions into View.

Because two-factor authentication solutions such as RSA SecurID and RADIUS work with authentication managers, installed on separate servers, you must have those servers configured and accessible to the View Connection Server host. For example, if you use RSA SecurID, the authentication manager would be RSA Authentication Manager. If you have RADIUS, the authentication manager would be a RADIUS server.

To use two-factor authentication, each user must have a token, such as an RSA SecurID token, that is registered with its authentication manager. A two-factor authentication token is a piece of hardware or software that generates an authentication code at fixed intervals. Often authentication requires knowledge of both a PIN and an authentication code.

If you have multiple View Connection Server instances, you can configure two-factor authentication on some instances and a different user authentication method on others. For example, you can configure two-factor authentication only for users who access remote desktops and applications from outside the corporate network, over the Internet.

View is certified through the RSA SecurID Ready program and supports the full range of SecurID capabilities, including New PIN Mode, Next Token Code Mode, RSA Authentication Manager, and load balancing.

- [Logging in Using Two-Factor Authentication](#) on page 58

When a user connects to a View Connection Server instance that has RSA SecurID authentication or RADIUS authentication enabled, a special login dialog box appears in Horizon Client.

- [Enable Two-Factor Authentication in View Administrator](#) on page 58  
You enable a View Connection Server instance for RSA SecurID authentication or RADIUS authentication by modifying View Connection Server settings in View Administrator.
- [Troubleshooting RSA SecurID Access Denial](#) on page 60  
Access is denied when Horizon Client connects with RSA SecurID authentication.
- [Troubleshooting RADIUS Access Denial](#) on page 60  
Access is denied when Horizon Client connects with RADIUS two-factor authentication.

## Logging in Using Two-Factor Authentication

When a user connects to a View Connection Server instance that has RSA SecurID authentication or RADIUS authentication enabled, a special login dialog box appears in Horizon Client.

Users enter their RSA SecurID or RADIUS authentication user name and passcode in the a special login dialog box. A two-factor authentication passcode typically consists of a PIN followed by a token code.

- If RSA Authentication Manager requires users to enter a new RSA SecurID PIN after entering their RSA SecurID username and passcode, a PIN dialog box appears. After setting a new PIN, users are prompted to wait for the next token code before logging in. If RSA Authentication Manager is configured to use system-generated PINs, a dialog box appears to confirm the PIN.
- When logging in to View, RADIUS authentication works much like RSA SecurID. If the RADIUS server issues an access challenge, Horizon Client displays a dialog box similar to the RSA SecurID prompt for the next token code. Currently support for RADIUS challenges is limited to prompting for text input. Any challenge text sent from the RADIUS server is not displayed. More complex forms of challenge, such as multiple choice and image selection, are currently not supported.

After a user enters credentials in Horizon Client, the RADIUS server can send an SMS text message or email, or text using some other out-of-band mechanism, to the user's cell phone with a code. The user can enter this text and code into Horizon Client to complete the authentication.

- Because some RADIUS vendors provide the ability to import users from Active Directory, end users might first be prompted to supply Active Directory credentials before being prompted for a RADIUS authentication user name and passcode.

## Enable Two-Factor Authentication in View Administrator

You enable a View Connection Server instance for RSA SecurID authentication or RADIUS authentication by modifying View Connection Server settings in View Administrator.

### Prerequisites

Install and configure the two-factor authentication software, such as the RSA SecurID software or the RADIUS software, on an authentication manager server.

- For RSA SecurID authentication, export the `sdconf.rec` file for the View Connection Server instance from RSA Authentication Manager. See the RSA Authentication Manager documentation.
- For RADIUS authentication, follow the vendor's configuration documentation. Make a note of the RADIUS server's host name or IP address, the port number on which it is listening for RADIUS authentication (usually 1812), the authentication type (PAP, CHAP, MS-CHAPv1, or MS-CHAPv2) and the shared secret. You will enter these values in View Administrator. You can enter values for a primary and a secondary RADIUS authenticator.

### Procedure

- 1 In View Administrator, select **View Configuration > Servers**.
- 2 On the **Connection Servers** tab, select the server and click **Edit**.

- 3 On the **Authentication** tab, from the **2-factor authentication** drop-down list in the Advanced Authentication section, select **RSA SecureID** or **RADIUS**.
- 4 To force RSA SecurID or RADIUS user names to match user names in Active Directory, select **Enforce SecurID and Windows user name matching** or **Enforce 2-factor and Windows user name matching**.  
If you select this option, users must use the same RSA SecurID or RADIUS user name for Active Directory authentication. If you do not select this option, the names can be different.
- 5 For RSA SecurID, click **Upload File**, type the location of the `sdconf.rec` file, or click **Browse** to search for the file.
- 6 For RADIUS authentication, complete the rest of the fields:
  - a Select **Use the same username and password for RADIUS and Windows authentication** if the initial RADIUS authentication uses Windows authentication that triggers an out-of-band transmission of a token code, and this token code is used as part of a RADIUS challenge.  
If you select this check box, users will not be prompted for Windows credentials after RADIUS authentication if the RADIUS authentication uses the Windows username and password. Users do not have to reenter the Windows username and password after RADIUS authentication.
  - b From the **Authenticator** drop-down list, select **Create New Authenticator** and complete the page.
    - Set **Accounting port** to **0** unless you want to enable RADIUS accounting. Set this port to a non-zero number only if your RADIUS server supports collecting accounting data. If the RADIUS server does not support accounting messages and you set this port to a nonzero number, the messages will be sent and ignored and retried a number of times, resulting in a delay in authentication.  
Accounting data can be used in order to bill users based on usage time and data. Accounting data can also be used for statistical purposes and for general network monitoring.
    - If you specify a realm prefix string, the string is placed at the beginning of the username when it is sent to the RADIUS server. For example, if the username entered in Horizon Client is **jdoe** and the realm prefix **DOMAIN-A\** is specified, the username **DOMAIN-A\jdoe** is sent to the RADIUS server. Similarly if you use the realm suffix, or postfix, string **@mycorp.com**, the username **jdoe@mycorp.com** is sent to the RADIUS server.
- 7 Click **OK** to save your changes.  
You do not need to restart the View Connection Server service. The necessary configuration files are distributed automatically and the configuration settings take effect immediately.

When users open Horizon Client and authenticate to View Connection Server, they are prompted for two-factor authentication. For RADIUS authentication, the login dialog box displays text prompts that contain the token label you specified.

Changes to RADIUS authentication settings affect remote desktop and application sessions that are started after the configuration is changed. Current sessions are not affected by changes to RADIUS authentication settings.

### What to do next

If you have a replicated group of View Connection Server instances and you want to also set up RADIUS authentication on them, you can re-use an existing RADIUS authenticator configuration.

## Troubleshooting RSA SecurID Access Denial

Access is denied when Horizon Client connects with RSA SecurID authentication.

### Problem

A Horizon Client connection with RSA SecurID displays `Access Denied` and the RSA Authentication Manager Log Monitor displays the error `Node Verification Failed`.

### Cause

The RSA Agent host node secret needs to be reset.

### Solution

- 1 In View Administrator, select **View Configuration > Servers**.
- 2 On the **Connection Servers** tab, select the View Connection Server and click **Edit**.
- 3 On the **Authentication** tab, select **Clear node secret**.
- 4 Click **OK** to clear the node secret.
- 5 On the computer that is running RSA Authentication Manager, select **Start > Programs > RSA Security > RSA Authentication Manager Host Mode**.
- 6 Select **Agent Host > Edit Agent Host**.
- 7 Select **View Connection Server** from the list and deselect the **Node Secret Created** check box.  
**Node Secret Created** is selected by default each time you edit it.
- 8 Click **OK**.

## Troubleshooting RADIUS Access Denial

Access is denied when Horizon Client connects with RADIUS two-factor authentication.

### Problem

A Horizon Client connection using RADIUS two-factor authentication displays `Access Denied`.

### Cause

RADIUS does not receive a reply from the RADIUS server, causing View to time out.

### Solution

The following common configuration mistakes most often lead to this situation:

- The RADIUS server has not been configured to accept the View Connection Server instance as a RADIUS client. Each View Connection Server instance using RADIUS must be set up as a client on the RADIUS server. See the documentation for your RADIUS two-factor authentication product.
- The shared secret values on the View Connection Server instance and the RADIUS server do not match.

## Using SAML Authentication

The Security Assertion Markup Language (SAML) is an XML-based standard that is used to describe and exchange authentication and authorization information between different security domains. SAML passes information about users between identity providers and service providers in XML documents called SAML assertions.

You can use SAML authentication to integrate View with VMware Workspace Portal, VMware Identity Manager, or a third-party load balancer or gateway. When SSO is enabled, users who log in to VMware Identity Manager or a third-party device can launch remote desktops and applications without having to go through a second login procedure. You can also use SAML authentication to implement smart card authentication on VMware Access Point, or on third-party devices.

To delegate responsibility for authentication to Workspace Portal, VMware Identity Manager, or a third-party device, you must create a SAML authenticator in View. A SAML authenticator contains the trust and metadata exchange between View and Workspace Portal, VMware Identity Manager, or the third-party device. You associate a SAML authenticator with a View Connection Server instance.

## Using SAML Authentication for VMware Identity Manager Integration

Integration between View and VMware Identity Manager (formerly called Workspace Portal) uses the SAML 2.0 standard to establish mutual trust, which is essential for single sign-on (SSO) functionality. When SSO is enabled, users who log in to VMware Identity Manager or Workspace Portal with Active Directory credentials can launch remote desktops and applications without having to go through a second login procedure.

When VMware Identity Manager and View are integrated, VMware Identity Manager generates a unique SAML artifact whenever a user logs in to VMware Identity Manager and clicks a desktop or application icon. VMware Identity Manager uses this SAML artifact to create a Universal Resource Identifier (URI). The URI contains information about the View Connection Server instance where the desktop or application pool resides, which desktop or application to launch, and the SAML artifact.

VMware Identity Manager sends the SAML artifact to the Horizon client, which in turn sends the artifact to the View Connection Server instance. The View Connection Server instance uses the SAML artifact to retrieve the SAML assertion from VMware Identity Manager.

After a View Connection Server instance receives a SAML assertion, it validates the assertion, decrypts the user's password, and uses the decrypted password to launch the desktop or application.

Setting up VMware Identity Manager and View integration involves configuring VMware Identity Manager with View information and configuring View to delegate responsibility for authentication to VMware Identity Manager.

To delegate responsibility for authentication to VMware Identity Manager, you must create a SAML authenticator in View. A SAML authenticator contains the trust and metadata exchange between View and VMware Identity Manager. You associate a SAML authenticator with a View Connection Server instance.

---

**NOTE** If you intend to provide access to your desktops and applications through VMware Identity Manager, verify that you create the desktop and application pools as a user who has the Administrators role on the root access group in View Administrator. If you give the user the Administrators role on an access group other than the root access group, VMware Identity Manager will not recognize the SAML authenticator you configure in View, and you cannot configure the pool in VMware Identity Manager.

---

## Configure a SAML Authenticator in View Administrator

To launch remote desktops and applications from VMware Identity Manager or to connect to remote desktops and applications through a third-party load balancer or gateway, you must create a SAML authenticator in View Administrator. A SAML authenticator contains the trust and metadata exchange between View and the device to which clients connect.

You associate a SAML authenticator with a View Connection Server instance. If your deployment includes more than one View Connection Server instance, you must associate the SAML authenticator with each instance.

You can allow one static authenticator and multiple dynamic authenticators to go live at a time. You can configure vIDM (Dynamic) and Access Point (Static) authenticators and retain them in active state. You can make connections through either of these authenticators.

You can configure more than one SAML authenticator to a View Connection Server and all the authenticators can be active simultaneously. However, the entity-ID of each of these SAML authenticators configured on the View Connection Server must be different.

The status of the SAML authenticator in dashboard is always green as it is predefined metadata that is static in nature. The red and green toggling is only applicable for dynamic authenticators.

For information about configuring a SAML authenticator for VMware Access Point appliances, see *Deploying and Configuring Access Point*.

### Prerequisites

- Verify that Workspace Portal, VMware Identity Manager, or a third-party gateway or load balancer is installed and configured. See the installation documentation for that product.
- Verify that the root certificate for the signing CA for the SAML server certificate is installed on the connection server host. VMware does not recommend that you configure SAML authenticators to use self-signed certificates. For information about certificate authentication, see the *View Installation* document.
- Make a note of the FQDN or IP address of the Workspace Portal server, VMware Identity Manager server, or external-facing load balancer.
- (Optional) If you are using Workspace Portal or VMware Identity Manager, make a note of the URL of the connector Web interface.
- If you are creating an authenticator for Access Point or a third-party appliance that requires you to generate SAML metadata and create a static authenticator, perform the procedure on the device to generate the SAML metadata, and then copy the metadata.

### Procedure

- 1 In View Administrator, select **Configuration > Servers**.
- 2 On the **Connection Servers** tab, select a server instance to associate with the SAML authenticator and click **Edit**.

- 3 On the **Authentication** tab, select a setting from the **Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator)** drop-down menu to enable or disable the SAML authenticator.

Option	Description
<b>Disabled</b>	SAML authentication is disabled. You can launch remote desktops and applications only from Horizon Client.
<b>Allowed</b>	SAML authentication is enabled. You can launch remote desktops and applications from both Horizon Client and VMware Identity Manager or the third-party device.
<b>Required</b>	SAML authentication is enabled. You can launch remote desktops and applications only from VMware Identity Manager or the third-party device. You cannot launch desktops or applications from Horizon Client manually.

You can configure each View Connection Server instance in your deployment to have different SAML authentication settings, depending on your requirements.

- 4 Click **Manage SAML Authenticators** and click **Add**.
- 5 Configure the SAML authenticator in the Add SAML 2.0 Authenticator dialog box.

Option	Description
<b>Type</b>	For Access Point or a third-party device, select <b>Static</b> . For VMware Identity Manager select <b>Dynamic</b> . For dynamic authenticators, you can specify a metadata URL and an administration URL. For static authenticators, you must first generate the metadata on the Access Point or a third-party device, copy the metadata, and then paste it into the <b>SAML metadata</b> text box.
<b>Label</b>	Unique name that identifies the SAML authenticator.
<b>Description</b>	Brief description of the SAML authenticator. This value is optional.
<b>Metadata URL</b>	(For dynamic authenticators) URL for retrieving all of the information required to exchange SAML information between the SAML identity provider and the View Connection Server instance. In the URL <code>https://&lt;YOUR HORIZON SERVER NAME&gt;/SAAS/API/1.0/GET/metadata/idp.xml</code> , click <b>&lt;YOUR HORIZON SERVER NAME&gt;</b> and replace it with the FQDN or IP address of the VMware Identity Manager server or external-facing load balancer (third-party device).
<b>Administration URL</b>	(For dynamic authenticators) URL for accessing the administration console of the SAML identity provider. For VMware Identity Manager, this URL should point to the VMware Identity Manager Connector Web interface. This value is optional.
<b>SAML metadata</b>	(For static authenticators) Metadata text that you generated and copied from the Access Point or a third-party device.
<b>Enabled for Connection Server</b>	Select this check box to enable the authenticator. You can enable multiple authenticators. Only enabled authenticators are displayed in the list.

- 6 Click **OK** to save the SAML authenticator configuration.

If you provided valid information, you must either accept the self-signed certificate (not recommended) or use a trusted certificate for View and VMware Identity Manager or the third-party device.

The Manage SAML Authenticators dialog box displays the newly created authenticator.

- 7 In the System Health section on the View Administrator dashboard, select **Other components > SAML 2.0 Authenticators**, select the SAML authenticator that you added, and verify the details.

If the configuration is successful, the authenticator's health is green. An authenticator's health can display red if the certificate is untrusted, if VMware Identity Manager is unavailable, or if the metadata URL is invalid. If the certificate is untrusted, you might be able to click **Verify** to validate and accept the certificate.

### What to do next

Extend the expiration period of the View Connection Server metadata so that remote sessions are not terminated after only 24 hours. See [“Change the Expiration Period for Service Provider Metadata on View Connection Server,”](#) on page 64.

## Change the Expiration Period for Service Provider Metadata on View Connection Server

If you do not change the expiration period, View Connection Server will stop accepting SAML assertions from the SAML authenticator, such as Access Point or a third-party identity provider, after 24 hours, and the metadata exchange must be repeated.

Use this procedure to specify the number of days that can elapse before View Connection Server stops accepting SAML assertions from the identity provider. This number is used when the current expiration period ends. For example, if the current expiration period is 1 day and you specify 90 days, after 1 day elapses, View Connection Server generates metadata with an expiration period of 90 days.

### Prerequisites

See the Microsoft TechNet Web site for information on how to use the ADSI Edit utility on your Windows operating system version.

### Procedure

- 1 Start the ADSI Edit utility on your View Connection Server host.
- 2 In the console tree, select **Connect to**.
- 3 In the **Select or type a Distinguished Name or Naming Context** text box, type the distinguished name **DC=vdi, DC=vmware, DC=int**.
- 4 In the Computer pane, select or type **localhost:389** or the fully qualified domain name (FQDN) of the View Connection Server host followed by port 389.

For example: **localhost:389** or **mycomputer.example.com:389**

- 5 Expand the ADSI Edit tree, expand **OU=Properties**, select **OU=Global**, and double-click **CN=Common** in the right pane.
- 6 In the Properties dialog box, edit the **pae-NameValuePair** attribute to add the following values

```
cs-samlencryptionkeyvaliditydays=number-of-days
cs-samlsigningkeyvaliditydays=number-of-days
```

In this example, *number-of-days* is the number of days that can elapse before a remote View Connection Server stops accepting SAML assertions. After this period of time, the process of exchanging SAML metadata must be repeated.

## Generate SAML Metadata So That View Connection Server Can Be Used as a Service Provider

After you create and enable a SAML authenticator for the identity provider you want to use, you might need to generate View Connection Server metadata. You use this metadata to create a service provider on the Access Point appliance or a third-party load balancer that is the identity provider.

### Prerequisites

Verify that you have created a SAML authenticator for the identity provider: Access Point or a third-party load balancer or gateway. In the System Health section on the View Administrator dashboard, you can select **Other components > SAML 2.0 Authenticators**, select the SAML authenticator that you added, and verify the details.

### Procedure

- 1 Open a new browser tab and enter the URL for getting the View Connection Server SAML metadata.

**`https://connection-server.example.com/SAML/metadata/sp.xml`**

In this example, *connection-server.example.com* is the fully qualified domain name of the View Connection Server host.

This page displays the SAML metadata from View Connection Server.

- 2 Use a **Save As** command to save the Web page to an XML file.

For example, you could save the page to a file named `connection-server-metadata.xml`. The contents of this file begin with the following text:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ...
```

### What to do next

Use the appropriate procedure on the identity provider to copy in the View Connection Server SAML metadata. Refer to the documentation for Access Point or a third-party load balancer or gateway.

## Response Time Considerations for Multiple Dynamic SAML Authenticators

If you configure SAML 2.0 Authentication as optional or required on a View Connection Server instance and you associate multiple dynamic SAML authenticators with the View Connection Server instance, if any of the dynamic SAML authenticators become unreachable, the response time to launch remote desktops from the other dynamic SAML authenticators increases.

You can decrease the response time for remote desktop launch on the other dynamic SAML authenticators by using View Administrator to disable the unreachable dynamic SAML authenticators. For information about disabling a SAML authenticator, see [“Configure a SAML Authenticator in View Administrator,”](#) on page 62.

## Configure Biometric Authentication

You can configure biometric authentication by editing the `pae-ClientConfig` attribute in the LDAP database.

### Prerequisites

See the Microsoft TechNet Web site for information on how to use the ADSI Edit utility on your Windows server.

### Procedure

- 1 Start the ADSI Edit utility on the View Connection Server host.

- 2 In the Connection Settings dialog box, select or connect to **DC=vdi,DC=vmware,DC=int**.
- 3 In the Computer pane, select or type **localhost:389** or the fully qualified domain name (FQDN) of the View Connection Server host followed by port 389.

For example: **localhost:389** or **mycomputer.mydomain.com:389**

- 4 On the object **CN=Common, OU=Global, OU=Properties**, edit the **pae-ClientConfig** attribute and add the value **BioMetricsTimeout=<integer>**.

The following BioMetricsTimeout values are valid:

BioMetricsTimeout Value	Description
<b>0</b>	Biometric authentication is not supported. This is the default.
<b>-1</b>	Biometric authentication is supported without any time limit.
<b>Any positive integer</b>	Biometric authentication is supported and can be used for the specified number of minutes.

The new setting takes effect immediately. You do not need to restart the View Connection Server service or the client device.

# Authenticating Users Without Requiring Credentials

---

# 5

After users log in to a client device or to VMware Identity Manager, they can connect to a published application or desktop without being prompted for Active Directory credentials.

Administrators can choose to set up the configuration based on user requirements.

- Provide users unauthenticated access to published applications. Administrators can configure the set up so that users do not need to log in to a Horizon Client with Active Directory (AD) credentials.
- Use Log In as Current User for Windows-Based clients. For Windows clients, administrators can configure the setup so that users do not need to supply additional credentials to log in to a Horizon server after they log in to a Windows client with AD credentials.
- Save credentials in Mobile and Mac Horizon Clients. For mobile and Mac clients, administrators can configure the Horizon server to save credentials. With this feature, users do not need to remember AD credentials for SSO (single sign-on) after supplying them once to a mobile or Mac client.
- Configure True SSO for VMware Identity Manager. For VMware Identity Manager, administrators can configure True SSO so that users who authenticate using some method other than AD credentials can then also log in to a remote desktop or application without being prompted for AD credentials.

This chapter includes the following topics:

- [“Providing Unauthenticated Access for Published Applications,”](#) on page 67
- [“Using the Log In as Current User Feature Available with Windows-Based Horizon Client,”](#) on page 72
- [“Saving Credentials in Mobile and Mac Horizon Clients,”](#) on page 72
- [“Setting Up True SSO,”](#) on page 73

## Providing Unauthenticated Access for Published Applications

Administrators can set up the configuration for unauthenticated users to access their published applications from a Horizon Client without requiring AD credentials. Consider setting up unauthenticated access if your users require access to a seamless application that has its own security and user management.

When a user starts a published application that is configured for unauthenticated access, the RDS host creates a local user session on demand and allocates the session to the user.

This feature requires the Horizon 7 version 7.1 environment set up and Horizon Client version 4.4.

### Workflow for Configuring Unauthenticated Users

- 1 Create users for unauthenticated access. See, [“Create Users for Unauthenticated Access,”](#) on page 69.

- 2 Enable unauthenticated access to users and set a default unauthenticated user. See, [“Enable Unauthenticated Access for Users,”](#) on page 69.
- 3 Entitle unauthenticated users to published applications. See, [“Entitle Unauthenticated Access Users to Published Applications,”](#) on page 70.
- 4 Enable unauthenticated access from the Horizon Client. See, [“Unauthenticated Access From Horizon Client,”](#) on page 71.

## Rules and Guidelines for Configuring Unauthenticated Users

- Two-factor authentication such as RSA and RADIUS, and Smart card authentication are not supported for unauthenticated access.
- Smart card authentication and unauthenticated access are mutually exclusive. When Smart card authentication is set to **Required** in Connection Server, unauthenticated access is disabled even if it was previously enabled.
- VMware Identity Manager and VMware App Volumes are not supported for unauthenticated access.
- Unauthenticated access login from the HTML Access Client is not supported.
- Both PCoIP and VMware Blast display protocols are supported for this feature.
- The unauthenticated access feature does not verify license information for RDS hosts. The administrator must configure and use device licenses.
- The unauthenticated access feature does not retain any user-specific data. The user can verify the data storage requirements for the application.
- You cannot reconnect to unauthenticated application sessions. When a user disconnects from the client, the RDS host logs off the local user session automatically.
- Unauthenticated access is only supported for published applications.
- Unauthenticated access is not supported with a security server or an Access Point appliance.
- User preferences are not preserved for unauthenticated users.
- Virtual desktops are not supported for unauthenticated users.
- Horizon Administrator displays a red status for the Connection Server, if the Connection Server is configured with a CA signed certificate and enabled for unauthenticated access but a default unauthenticated user is not configured.
- The unauthenticated access feature will not work if the AllowSingleSignon group policy for the Horizon Agent installed on an RDS host is disabled. Administrators can also control whether to disable or enable unauthenticated access with the UnAuthenticatedAccessEnabled Horizon Agent group policy setting. The Horizon Agent group policy settings are included in the ADMX template file (vdm\_agent.admx) or ADM template file (vdm\_agent.adm). You must reboot the RDS host for this policy to take effect.

## Create Users for Unauthenticated Access

Administrators can create users for unauthenticated access to published applications. After an administrator configures a user for unauthenticated access, the user can log in to the Connection Server instance from Horizon Client only with unauthenticated access.

### Prerequisites

- Verify that the Active Directory (AD) user for whom you want to configure unauthenticated access for has a valid UPN. Only an AD user can be configured as an unauthenticated access user.

---

**NOTE** Administrators can create only one user for each AD account. Administrators cannot create unauthenticated user groups. If you create an unauthenticated access user and there is an existing client session for that AD user, you must restart the client session to make the changes take effect.

---

### Procedure

- 1 In Horizon Administrator, select **Users and Groups**.
- 2 On the **Unauthenticated Access** tab, click **Add**.
- 3 In the Add Unauthenticated User wizard, select one or more search criteria and click **Find** to find users based on your search criteria.  
The user must have a valid UPN.
- 4 Select a user and click **Next**.  
Repeat this step to add multiple users.
- 5 (Optional) Enter the user alias.  
The default user alias is the user name that was configured for the AD account. End users can use the user alias to log in to the Connection Server instance from Horizon Client.
- 6 (Optional) Review the user details and add comments.
- 7 Click **Finish**.

Connection Server creates the unauthenticated access user and displays the user details including user alias, user name, first and last name, number of source pods, application entitlements, and sessions. You can click the number in the Source Pods column to display pod information.

### What to do next

Enable unauthenticated access for users in Connection Server. See, [“Enable Unauthenticated Access for Users,”](#) on page 69.

## Enable Unauthenticated Access for Users

After you create users for unauthenticated access, you must enable unauthenticated access in the Connection Server to enable users to connect and access published applications.

### Procedure

- 1 In Horizon Administrator, select **View Configuration > Servers**.
- 2 Click the **Connection Servers** tab.
- 3 Select the Connection Server instance and click **Edit**.
- 4 Click the **Authentication** tab.
- 5 Change **Unauthenticated Access** to **Enabled**.

- 6 From the **Default unauthenticated access user** drop-down menu, select a user as the default user.  
The default user must be present on the local pod in a Cloud Pod Architecture environment. If you select a default user from a different pod, Connection Server creates the user on the local pod before it makes the user the default user.
- 7 (Optional) Enter the default session timeout for the user.  
The default session timeout is 10 minutes after being idle.
- 8 Click **OK**.

### What to do next

Entitle unauthenticated users to published applications. See [“Entitle Unauthenticated Access Users to Published Applications,”](#) on page 70.

## Entitle Unauthenticated Access Users to Published Applications

After you create an unauthenticated access user, you must entitle the user to access published applications.

### Prerequisites

- Create a farm based on a group of RDS hosts. See "Creating Farms" in the *Setting Up Published Desktops and Applications in Horizon 7* document.
- Create an application pool for published applications that run on a farm of RDS hosts. See "Creating Application Pools" in the *Setting Up Published Desktops and Applications in Horizon 7* document.

### Procedure

- 1 In Horizon Administrator, select **Catalog > Application Pools** and click the name of the application pool.
- 2 Select **Add entitlement** from the **Entitlements** drop-down menu.
- 3 Click **Add**, select one or more search criteria, click **Find**, and select the **Unauthenticated Users** check box to find unauthenticated access users based on your search criteria.
- 4 Select the users to entitle to the applications in the pool and click **OK**.
- 5 Click **OK** to save your changes.

An unauthenticated access icon appears next to the unauthenticated access user after the entitlement process completes.

### What to do next

Use an unauthenticated access user to log in to Horizon Client. See, [“Unauthenticated Access From Horizon Client,”](#) on page 71.

## Search Unauthenticated Access Sessions

Use Horizon Administrator to list or search for application sessions that unauthenticated access users have connected to. The unauthenticated access user icon appears next to those sessions that unauthenticated access users have connected to.

### Procedure

- 1 In Horizon Administrator, select **Monitoring > Sessions**.
- 2 Click **Applications** to search for application sessions.

- 3 Select search criteria and begin the search.

The search results include the user, type of session (desktop or application), machine, pool or farm, DNS name, client ID and security gateway. The session start time, duration, state, and last session also appear in the search results.

## Delete an Unauthenticated Access User

When you delete an unauthenticated access user, you must also remove the application pool entitlements for the user. You cannot delete an unauthenticated access user who is the default user.

---

**NOTE** If you delete an unauthenticated access user and if there is an existing client session for that AD user, then you must restart the client session to make the changes take effect.

---

### Procedure

- 1 In Horizon Administrator, select **Users and Groups**.
- 2 On the **Unauthenticated Access** tab, click **Delete**.
- 3 Click **OK**.

### What to do next

Remove application entitlements for the user. See "Remove Entitlements from a Desktop or Application Pool" in the *Setting Up Published Desktops and Applications in Horizon 7* document.

## Unauthenticated Access From Horizon Client

Log in to Horizon Client with unauthenticated access and start the published application.

To ensure greater security, the unauthenticated access user has a user alias that you can use to log in to Horizon Client. When you select a user alias, you do not need to provide the AD credentials or UPN for the user. After you log in to Horizon Client, you can click your published applications to start the applications. For more information about installing and setting up Horizon Clients, see the Horizon Client documentation at the [VMware Horizon Clients documentation](#) Web page.

### Prerequisites

- Verify that Horizon 7 version 7.1 Connection Server is configured for unauthenticated access.
- Verify that the unauthenticated access users are created in Horizon Administrator. If the default unauthenticated user is the only unauthenticated access user, Horizon Client connects to the Connection Server instance with the default user.

### Procedure

- 1 Start Horizon Client.
- 2 In Horizon Client, select **Log in anonymously with Unauthenticated Access**.
- 3 Connect to the Connection Server instance.
- 4 Select a user alias from the drop-down menu and click **Login**.  
The default user has the "default" suffix.
- 5 Double-click a published application to start the application.

## Using the Log In as Current User Feature Available with Windows-Based Horizon Client

With Horizon Client for Windows, when users select the **Log in as current user** check box, the credentials that they provided when logging in to the client system are used to authenticate to the View Connection Server instance and to the remote desktop. No further user authentication is required.

To support this feature, user credentials are stored on both the View Connection Server instance and on the client system.

- On the View Connection Server instance, user credentials are encrypted and stored in the user session along with the username, domain, and optional UPN. The credentials are added when authentication occurs and are purged when the session object is destroyed. The session object is destroyed when the user logs out, the session times out, or authentication fails. The session object resides in volatile memory and is not stored in View LDAP or in a disk file.
- On the client system, user credentials are encrypted and stored in a table in the Authentication Package, which is a component of Horizon Client. The credentials are added to the table when the user logs in and are removed from the table when the user logs out. The table resides in volatile memory.

Administrators can use Horizon Client group policy settings to control the availability of the **Log in as current user** check box and to specify its default value. Administrators can also use group policy to specify which View Connection Server instances accept the user identity and credential information that is passed when users select the **Log in as current user** check box in Horizon Client.

The Log in as current user feature has the following limitations and requirements:

- When smart card authentication is set to Required on a View Connection Server instance, authentication fails for users who select the **Log in as current user** check box when they connect to the View Connection Server instance. These users must reauthenticate with their smart card and PIN when they log in to View Connection Server.
- The time on the system where the client logs in and the time on the View Connection Server host must be synchronized.
- If the default **Access this computer from the network** user-right assignments are modified on the client system, they must be modified as described in VMware Knowledge Base (KB) article 1025691.
- The client machine must be able to communicate with the corporate Active Directory server and not use cached credentials for authentication. For example, if users log in to their client machines from outside the corporate network, cached credentials are used for authentication. If the user then attempts to connect to a security server or a View Connection Server instance without first establishing a VPN connection, the user is prompted for credentials, and the Log in as Current User feature does not work.

## Saving Credentials in Mobile and Mac Horizon Clients

Administrators can configure View Connection Server to enable mobile and Mac Horizon Clients to remember a user's user name, password, and domain information.

For Horizon Client for mobile devices, this feature causes the **Save password** check box to appear on the login dialog boxes. For Horizon Client for Mac, this feature causes the **Remember this password** check box to appear on the login dialog box.

If users choose to save their credentials, the credentials are added to the login fields in Horizon Client on subsequent connections.

To enable this feature, you must set a value in View LDAP to indicate how long to save credential information in the client. For Horizon Client for Mac, this feature is supported only in version 4.1 or later.

---

**Note** On Windows-based Horizon clients, the feature for logging in as the current user avoids requiring users to supply credentials multiple times.

---

## Configure a Timeout Limit to Save Horizon Client Credentials

You configure a timeout limit that indicates how long to save Horizon Client credential information on mobile devices and Mac client systems by setting a value in View LDAP. The timeout limit is set in minutes. When you change View LDAP on a View Connection Server instance, the change is propagated to all replicated View Connection Server instances.

### Prerequisites

See the Microsoft TechNet Web site for information on how to use the ADSI Edit utility on your Windows operating system version.

### Procedure

- 1 Start the ADSI Edit utility on your View Connection Server host.
- 2 In the Connection Settings dialog box, select or connect to **DC=vdi,DC=vmware,DC=int**.
- 3 In the Computer pane, select or type **localhost:389** or the fully qualified domain name (FQDN) of the View Connection Server host followed by port 389.

For example: **localhost:389** or **mycomputer.mydomain.com:389**

- 4 On the object **CN=Common, OU=Global, OU=Properties**, edit the **clientCredentialCacheTimeout** attribute value.

When **clientCredentialCacheTimeout** is not set or is set to **0**, the feature is disabled. To enable this feature, you can set the number of minutes to retain the credential information, or set a value of **-1**, meaning that there is no timeout.

On View Connection Server, the new setting takes effect immediately. You do not need to restart the View Connection Server service or the client computer.

## Setting Up True SSO

With the True SSO (single sign-on) feature, after users log in to VMware Identity Manager using a smart card or RSA SecurID or RADIUS authentication, users are not required to also enter Active Directory credentials in order to use a remote desktop or application.

If a user authenticates by using Active Directory credentials, the True SSO feature is not necessary, but you can configure True SSO to be used even in this case, so that the AD credentials that the user provides are ignored and True SSO is used.

When connecting to a virtual desktop or remote application, users can select to use either the native Horizon Client or HTML Access.

This feature has the following limitations:

- This feature does not work for virtual desktops that are provided by using the View Agent Direct Connection plug-in.
- This feature is supported only in IPv4 environments.

Following is a list of tasks you must perform to set up your environment for True SSO:

- 1 [“Determining an Architecture for True SSO,”](#) on page 74

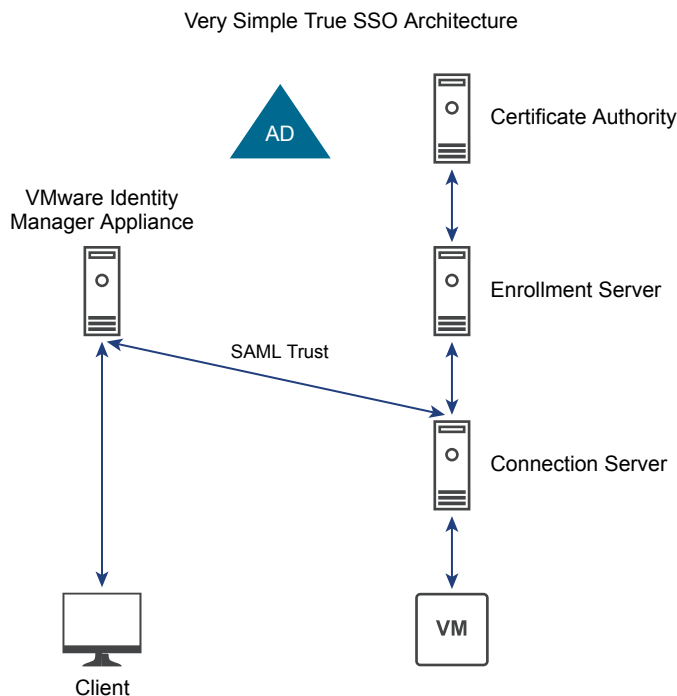
- 2 [“Set Up an Enterprise Certificate Authority,”](#) on page 76
- 3 [“Create Certificate Templates Used with True SSO,”](#) on page 78
- 4 [“Install and Set Up an Enrollment Server,”](#) on page 79
- 5 [“Export the Enrollment Service Client Certificate,”](#) on page 81
- 6 [“Configure SAML Authentication to Work with True SSO,”](#) on page 83
- 7 [“Configure View Connection Server for True SSO,”](#) on page 84

## Determining an Architecture for True SSO

To use True SSO, you must have or add a certificate authority and create an enrollment server. These two servers communicate to create the short-lived Horizon virtual certificate that enables a password-free Windows logon. You can use True SSO in a single domain, in a single-forest with multiple domains, and in a multiple-forest, multiple-domain setup.

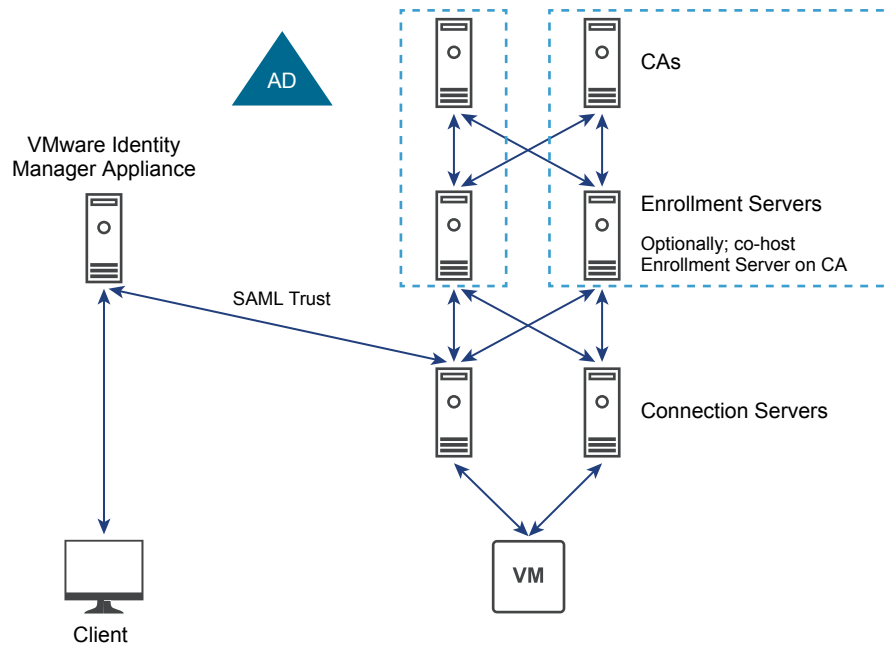
VMware recommends to have two CAs and two ESs deployed to use True SSO. The following examples illustrate True SSO in different architectures.

The following figure illustrates a simple True SSO architecture.



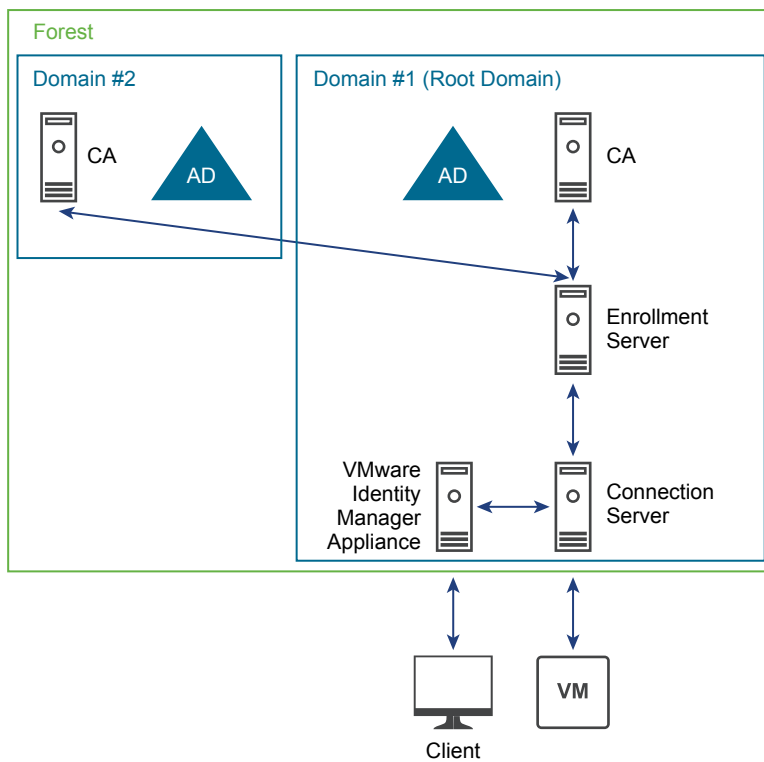
The following figure illustrates True SSO in a single domain architecture.

Typical HA True SSO Architecture (Single Domain)

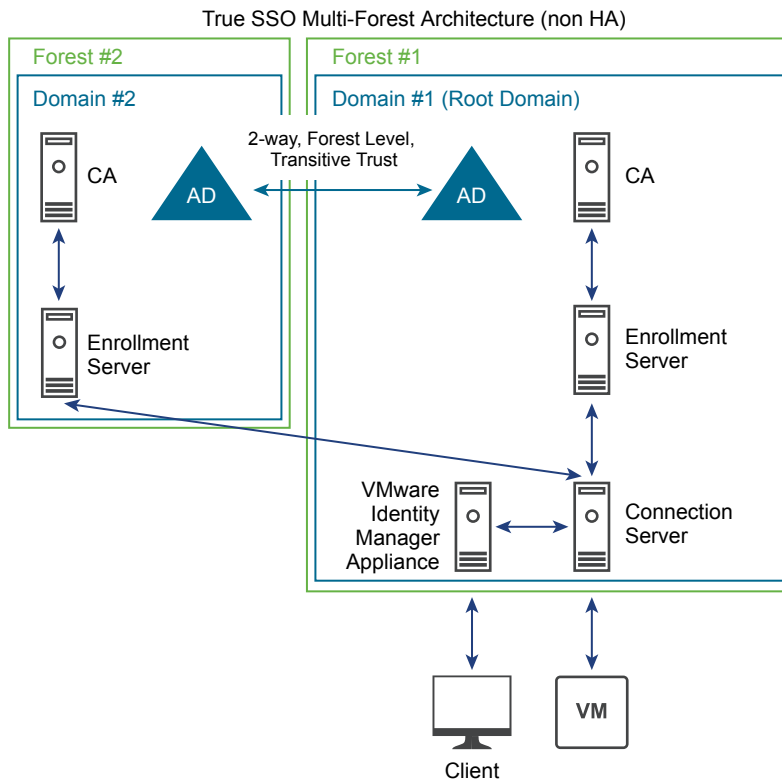


The following figure illustrates True SSO in a single-forest with multiple domains architecture.

True SSO Single Forest Multiple Domain Architecture (non HA)



The following figure illustrates True SSO in a multiple-forest architecture.



## Set Up an Enterprise Certificate Authority

If you do not already have a certificate authority set up, you must add the Active Directory Certificate Services (AD CS) role to a Windows server and configure the server to be an enterprise CA.

If you do already have an enterprise CA set up, verify that you are using the settings described in this procedure.

You must have at least one enterprise CA, and VMware recommends that you have two for purposes of failover and load balancing. The enrollment server you will create for True SSO communicates with the enterprise CA. If you configure the enrollment server to use multiple enterprise CAs, the enrollment server will alternate between the CAs available. If you install the enrollment server on the same machine that hosts the enterprise CA, you can configure the enrollment server to prefer using the local CA. This configuration is recommended for best performance.

Part of this procedure involves enabling non-persistent certificate processing. By default, certificate processing includes storing a record of each certificate request and issued certificate in the CA database. A sustained high volume of requests increases the CA database growth rate and could consume all available disk space if not monitored. Enabling non-persistent certificate processing can help reduce the CA database growth rate and frequency of database management tasks.

### Prerequisites

- Create a Windows Server 2008 R2 or Windows Server 2012 R2 virtual machine.
- Verify that the virtual machine is part of the Active Directory domain for the Horizon 7 deployment.
- Verify that you are using an IPv4 environment. This feature is currently not supported in an IPv6 environment.
- Verify that the system has a static IP address.

## Procedure

- 1 Log in to the virtual machine operating system as an administrator and start Server Manager.
- 2 Select the settings for adding roles.

Operating System	Selections
<b>Windows Server 2012 R2</b>	<ol style="list-style-type: none"> <li>a Select <b>Add roles and features</b>.</li> <li>b On the Select Installation Type page, select <b>Role-based or feature-based installation</b>.</li> <li>c On the Select Destination Server page, select a server.</li> </ol>
<b>Windows Server 2008 R2</b>	<ol style="list-style-type: none"> <li>a Select <b>Roles</b> in the navigation tree.</li> <li>b Click <b>Add Roles</b> to start the Add Role wizard.</li> </ol>

- 3 On the Select Server Roles page, select **Active Directory Certificate Services**.
- 4 In the Add Roles and Features wizard, click **Add Features**, and leave the **Include management tools** check box selected.
- 5 On the Select Features page, accept the defaults.
- 6 On the Select Role Services page, select **Certification Authority**.
- 7 Follow the prompts and finish the installation.
- 8 When installation is complete, on the Installation Progress page, click the **Configure Active Directory Certificate Services on destination server** link to open the AD CS Configuration wizard.
- 9 On the Credentials page, click **Next** and complete the AD CS Configuration wizard pages as described in the following table.

Option	Action
<b>Role Services</b>	Select <b>Certification Authority</b> , and click <b>Next</b> (rather than <b>Configure</b> ).
<b>Setup Type</b>	Select <b>Enterprise CA</b> .
<b>CA Type</b>	Select <b>Root CA</b> or <b>Subordinate CA</b> . Some enterprises prefer two-tier PKI deployment. For more information, see <a href="http://social.technet.microsoft.com/wiki/contents/articles/15037.ad-cs-step-by-step-guide-two-tier-pki-hierarchy-deployment.aspx">http://social.technet.microsoft.com/wiki/contents/articles/15037.ad-cs-step-by-step-guide-two-tier-pki-hierarchy-deployment.aspx</a> .
<b>Private Key</b>	Select <b>Create a new private key</b> .
<b>Cryptography for CA</b>	For hash algorithm, you can select <b>SHA1</b> , <b>SHA256</b> , <b>SHA384</b> , or <b>SHA512</b> . For key length, you can select <b>1024</b> , <b>2048</b> , <b>3072</b> , or <b>4096</b> . VMware recommends a minimum of SHA256 and a 2048 key.
<b>CA Name</b>	Accept the default or change the name.
<b>Validity Period</b>	Accept the default of 5 years.
<b>Certificate Database</b>	Accept the defaults.

- 10 On the Confirmation page, click **Configure**, and when the wizard reports a successful configuration, close the wizard.
- 11 Open a command prompt and enter the following command to configure the CA for non-persistent certificate processing:

```
certutil -setreg DBFlags +DBFLAGS_ENABLEVOLATILEREQUESTS
```

- 12 Enter the following command to ignore offline CRL (certificate revocation list) errors on the CA:

```
certutil -setreg ca\CRLFlags +CRLF_REVCHECK_IGNORE_OFFLINE
```

This flag is required because the root certificate that True SSO uses will usually be offline, and thus revocation checking will fail, which is expected.

- 13 Enter the following commands to restart the service:

```
sc stop certsvc
sc start certsvc
```

### What to do next

Create a certificate template. See [“Create Certificate Templates Used with True SSO,”](#) on page 78.

## Create Certificate Templates Used with True SSO

You must create a certificate template that can be used for issuing short-lived certificates, and you must specify which computers in the domain can request this type of certificate.

You can create more than one certificate template, but you can configure only one template to be used at any one time.

### Prerequisites

- Verify that you have an enterprise CA to use for creating the template described in this procedure. See [“Set Up an Enterprise Certificate Authority,”](#) on page 76.
- Verify that you have prepared Active Directory for smart card authentication. For more information, see the *View Installation* document.
- Create a security group in the domain and forest for the enrollment servers, and add the computer accounts of the enrollment servers to that group.

### Procedure

- 1 On the machine that you are using for the certificate authority, log in to the operating system as an administrator and go to **Administrative Tools > Certification Authority**.
- 2 Expand the tree in the left pane, right-click **Certificate Templates** and select **Manage**.
- 3 Right-click the **Smartcard Logon** template and select **Duplicate**.
- 4 Make the following changes on the following tabs:

Tab	Action
<b>Compatibility tab</b>	<ul style="list-style-type: none"> <li>■ For <b>Certificate Authority</b>, select <b>Windows Server 2008 R2</b>.</li> <li>■ For <b>Certificate Recipient</b>, select <b>Windows 7/Windows Server 2008 R2</b>.</li> </ul>
<b>General tab</b>	<ul style="list-style-type: none"> <li>■ Change the template display name to <b>True SSO</b>.</li> <li>■ Change the validity period to a period that is as long as a typical working day; that is, as long as the user is likely to remain logged into the system.  So that the user does not lose access to network resources while logged on, the validity period must be longer than the Kerberos TGT renewal time in the users domain.  (The default maximum lifetime of the ticket is 10 hours. To find the default domain policy, you can go to <b>Computer Configuration &gt; Policies &gt; Windows Settings &gt; Security Settings &gt; Account Policies &gt; Kerberos Policy:Maximum lifetime for user ticket</b>.)</li> <li>■ Change the renewal period to 1 day.</li> </ul>
<b>Request Handling tab</b>	<ul style="list-style-type: none"> <li>■ For <b>Purpose</b>, select <b>Signature and smartcard logon</b>.</li> <li>■ Select, <b>For automatic renewal of smart cards, ...</b></li> </ul>
<b>Cryptography tab</b>	<ul style="list-style-type: none"> <li>■ For <b>Provider Category</b>, select <b>Key Storage Provider</b>.</li> <li>■ For <b>Algorithm name</b>, select <b>RSA</b>.</li> </ul>

Tab	Action
<b>Server tab</b>	Select <b>Do not store certificates and requests in the CA database</b> . <b>IMPORTANT</b> Make sure to deselect <b>Do not include revocation information in issued certificates</b> . (This box gets selected when you select the first one, and you have to deselect (clear) it.)
<b>Issuance Requirements tab</b>	<ul style="list-style-type: none"> <li>■ Select <b>This number of authorized signatures</b>, and type <b>1</b> in the box.</li> <li>■ For <b>Policy type</b>, select <b>Application Policy</b> and set the policy to <b>Certificate Request Agent</b>.</li> <li>■ For, <b>Require the following for reenrollment</b>, select <b>Valid existing certificate</b>.</li> </ul>
<b>Security tab</b>	For the security group that you created for the enrollment server computer accounts, as described in the prerequisites, provide the following permissions: Read, Enroll <ol style="list-style-type: none"> <li>a Click <b>Add</b>.</li> <li>b Specify which computers to allow to enroll for certificates.</li> <li>c For these computers select the appropriate check boxes to give the computers the following permissions: Read, Enroll.</li> </ol>

- 5 Click **OK** in the Properties of New Template dialog box.
- 6 Close the Certificate Templates Console window.
- 7 Right-click **Certificate Templates** and select **New > Certificate Template to Issue**.

---

**NOTE** This step is required for all certificate authorities that issue certificates based on this template.

---

- 8 In the Enable Certificate Templates window, select the template you just created (for example, **True SSO Template**) and click **OK**.
- 9 In the Enable Certificate Templates window, select **Enrollment Agent Computer** and click **OK**.

### What to do next

Create an enrollment service. See [“Install and Set Up an Enrollment Server,”](#) on page 79.

## Install and Set Up an Enrollment Server

You run the Connection Server installer and select the Horizon 7 Enrollment Server option to install an enrollment server. The enrollment server requests short-lived certificates on behalf of the users you specify. These short-term certificates are the mechanism True SSO uses for authentication to avoid prompting users for Active Directory credentials.

You must install and set up at least one enrollment server, and the enrollment server cannot be installed on the same host as View Connection Server. VMware recommends that you have two enrollment servers for purposes of failover and load balancing. If you have two enrollment servers, by default one is preferred and the other is used for failover. You can change this default, however, so that the connection server alternates sending certificate requests to both enrollment servers.

If you install the enrollment server on the same machine that hosts the enterprise CA, you can configure the enrollment server to prefer using the local CA. For best performance, VMware recommends combining the configuration to prefer using the local CA with the configuration to load balance the enrollment servers. As a result, when certificate requests arrive, the connection server will use alternate enrollment servers, and each enrollment server will service the requests using the local CA. For information about the configuration settings to use, see [“Enrollment Server Configuration Settings,”](#) on page 90 and [“Connection Server Configuration Settings,”](#) on page 92.

## Prerequisites

- Create a Windows Server 2008 R2 or Windows Server 2012 R2 virtual machine with at least 4GB of memory, or use the virtual machine that hosts the enterprise CA. Do not use a machine that is a domain controller.
- Verify that no other View component, including View Connection Server, View Composer, security server, Horizon Client, or View Agent or Horizon Agent is installed on the virtual machine.
- Verify that the virtual machine is part of the Active Directory domain for the Horizon 7 deployment.
- Verify that you are using an IPv4 environment. This feature is currently not supported in an IPv6 environment
- VMware recommends that the system must have a static IP address.
- Verify that you can log in to the operating system as a domain user with Administrator privileges. You must log in as an administrator to run the installer.

## Procedure

- 1 On the machine that you plan to use for the enrollment server, add the Certificate snap-in to MMC:
  - a Open the MMC console and select **File > Add/Remove Snap-in**
  - b Under **Available snap-ins**, select **Certificates** and click **Add**.
  - c In the Certificates snap-in window, select **Computer account**, click **Next**, and click **Finish**.
  - d In the Add or Remove Snap-in window, click **OK**.
- 2 Issue an enrollment agent certificate:
  - a In the Certificates console, expand the console root tree, right-click the **Personal** folder, and select **All Tasks > Request New Certificate**.
  - b In the Certificate Enrollment wizard, accept the defaults until you get to the Request Certificates page.
  - c On the Request Certificates page, select the **Enrollment Agent (Computer)** check box and click **Enroll**.
  - d Accept the defaults on the other wizard pages, and click **Finish** on the last page.

In the MMC console, if you expand the **Personal** folder and select **Certificates** in the left pane, you will see a new certificate listed in the right pane.

- 3 Install the enrollment server:
  - a Download the View Connection Server installer file from the VMware download site at <https://my.vmware.com/web/vmware/downloads>.  
Under Desktop & End-User Computing, select the VMware Horizon 7 download, which includes View Connection Server.  
The installer filename is `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`, where `xxxxxx` is the build number and `y.y.y` is the version number.
  - b Double-click the installer file to start the wizard, and follow the prompts until you get to the Installation Options page.
  - c On the Installation Options page, select **Horizon 7 Enrollment Server** and click **Next**.
  - d Follow the prompts to finish the installation.

You must enable the incoming connections on Port 32111 (TCP) for enrollment server to be functional. The installer opens the port by default during installation.

### What to do next

- If you installed the enrollment server on the same machine that hosts an enterprise CA, configure the enrollment server to prefer using the local CA. See “[Enrollment Server Configuration Settings](#),” on page 90.
- If you install and set up more than one enrollment server, configure connection servers to enable load balancing between the enrollment servers. See “[Connection Server Configuration Settings](#),” on page 92.
- Pair connection servers with enrollment servers. See “[Export the Enrollment Service Client Certificate](#),” on page 81.

## Export the Enrollment Service Client Certificate

To accomplish pairing, you can use the MMC Certificates snap-in to export automatically generated, self-signed Enrollment Service Client certificate from one connection server in the cluster. This certificate is called a client certificate because the connection server is a client of the Enrollment Service provided by the enrollment server.

Enrollment Service must trust the VMware Horizon View Connection Server when it prompts the Enrollment Servers to issue the short lived certificates for Active Directory users. Hence, the VMware Horizon View Connection Server clusters or pods must be paired with Enrollment Servers.

The Enrollment Service Client certificate is automatically created when a Horizon 7 or later connection server is installed and the VMware Horizon View Connection Server service starts. The certificate is distributed through View LDAP to other Horizon 7 connection servers that get added to the cluster later. The certificate is then stored in a custom container (VMware Horizon View Certificates\Certificates) in the Windows Certificate Store on the computer.

### Prerequisites

Verify that you have a Horizon 7 or later connection server. For installation instructions, see *View Installation*. For upgrade instructions, see *View Upgrades*.

---

**IMPORTANT** Customers can use their own certificates for pairing, rather than using the self-generated certificate created by the connection server. To do so, place the preferred certificate (and the associated private key) in the custom container (VMware Horizon View Certificates\Certificates) in the Windows Certificate Store on the connection server machine. You must then set the friendly name of the certificate to **vdm.ec.new**, and restart the server. The other servers in the cluster will fetch this certificate from LDAP. You can then perform the steps in this procedure.

---

### Procedure

- 1 On one of the connection server machines in the cluster, add the Certificates snap-in to MMC:
  - a Open the MMC console and select **File > Add/Remove Snap-in**
  - b Under **Available snap-ins**, select **Certificates** and click **Add**.
  - c In the Certificates snap-in window, select **Computer account**, click **Next**, and click **Finish**.
  - d In the Add or Remove Snap-in window, click **OK**.
- 2 In the MMC console, in the left pane, expand the **VMware Horizon View Certificates** folder and select the **Certificates** folder.
- 3 In the right pane, right-click the certificate file with the friendly name **vdm.ec**, and select **All Tasks > Export**.
- 4 In the Certificate Export wizard, accept the defaults, including leaving the **No, do not export the private key** radio button selected.

- 5 When you are prompted to name the file, type a file name such as **EnrollClient**, for Enrollment Service Client certificate, and follow the prompts to finish exporting the certificate.

### What to do next

Import the certificate into the enrollment server. See [“Import the Enrollment Service Client Certificate on the Enrollment Server,”](#) on page 82.

## Import the Enrollment Service Client Certificate on the Enrollment Server

To complete the pairing process, you use the MMC Certificates snap-in to import the Enrollment Service Client certificate into the enrollment server. You must perform this procedure on every enrollment server.

### Prerequisites

- Verify that you have a Horizon 7 or later enrollment server. See [“Install and Set Up an Enrollment Server,”](#) on page 79.
- Verify that you have the correct certificate to import. You can use either your own certificate or the automatically generated, self-signed Enrollment Service Client certificate from one connection server in the cluster, as described in [“Export the Enrollment Service Client Certificate,”](#) on page 81.

---

**IMPORTANT** To use your own certificates for pairing, place the preferred certificate (and the associated private key) in the custom container (VMware Horizon View Certificates\Certificates) in the Windows Certificate Store on the connection server machine. You must then set the friendly name of the certificate to **vdm.ec.new**, and restart the server. The other servers in the cluster will fetch this certificate from LDAP. You can then perform the steps in this procedure.

---

If you have your own client certificate, the certificate that you must copy to the enrollment server is the root certificate used to generate the client certificate.

---

### Procedure

- 1 Copy the appropriate certificate file to the enrollment server machine.  
To use the automatically generated certificate, copy the Enrollment Service Client certificate from the connection server. To use your own certificate, copy the root certificate that was used to generate the client certificate.
- 2 On the enrollment server, add the Certificates snap-in to MMC:
  - a Open the MMC console and select **File > Add/Remove Snap-in**
  - b Under **Available snap-ins**, select **Certificates** and click **Add**.
  - c In the Certificates snap-in window, select **Computer account**, click **Next**, and click **Finish**.
  - d In the Add or Remove Snap-in window, click **OK**.
- 3 In the MMC console, in the left pane, right-click the **VMware Horizon View Enrollment Server Trusted Roots** folder and select **All Tasks > Import**.
- 4 In the Certificate Import wizard, follow the prompts to browse to and open the **EnrollClient** certificate file.
- 5 Follow the prompts and accept the defaults to finish importing the certificate.
- 6 Right-click the imported certificate and add a friendly name such as **vdm.ec** (for Enrollment Client certificate).

VMware recommends you use a friendly name that identifies the View cluster, but you can use any name that helps you easily identify the client certificate.

## What to do next

Configure the SAML authenticator used for delegating authentication to VMware Identity Manager. See [“Configure SAML Authentication to Work with True SSO,”](#) on page 83.

## Configure SAML Authentication to Work with True SSO

With the True SSO feature introduced in Horizon 7, users can log in to VMware Identity Manager 2.6 and later releases using smart card, RADIUS, or RSA SecurID authentication, and they will no longer be prompted for Active Directory credentials, even when they launch a remote desktop or application for the first time.

With earlier releases, SSO (single sign-on) worked by prompting users for their Active Directory credentials the first time they launched a remote desktop or published application if they had not previously authenticated with their Active Directory credentials. The credentials were then cached so that subsequent launches would not require users to re-enter their credentials. With True SSO, short-term certificates are created and used instead of AD credentials.

Although the process for configuring SAML authentication for VMware Identity Manager has not changed, one additional step has been added for True SSO. You must configure VMware Identity Manager so that password pop-ups are suppressed.

---

**NOTE** If your deployment includes more than one View Connection Server instance, you must associate the SAML authenticator with each instance.

---

### Prerequisites

- Verify that single sign-on is enabled as a global setting. In View Administrator, select **Configuration > Global Settings**, and verify that **Single sign-on (SSO)** is set to **Enabled**.
- Verify that VMware Identity Manager is installed and configured. See the VMware Identity Manager documentation, available at [https://www.vmware.com/support/pubs/vidm\\_pubs.html](https://www.vmware.com/support/pubs/vidm_pubs.html)
- Verify that the root certificate for the signing CA for the SAML server certificate is installed on the connection server host. VMware does not recommend that you configure SAML authenticators to use self-signed certificates. See the topic "Import a Root Certificate and Intermediate Certificates into a Windows Certificate Store," in the chapter "Configuring SSL Certificates for View Servers," in the *View Installation* document.
- Make a note of the FQDN of the VMware Identity Manager server instance.

### Procedure

- 1 In Horizon Administrator, select **Configuration > Servers**.
- 2 On the **Connection Servers** tab, select a server instance to associate with the SAML authenticator and click **Edit**.
- 3 On the **Authentication** tab, from the **Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator)** drop-down menu, select **Allowed** or **Required**.

You can configure each View Connection Server instance in your deployment to have different SAML authentication settings, depending on your requirements.

- 4 Click **Manage SAML Authenticators** and click **Add**.
- 5 Configure the SAML authenticator in the Add SAML 2.0 Authenticator dialog box.

Option	Description
<b>Label</b>	You can use the FQDN of the VMware Identity Manager server instance.
<b>Description</b>	(Optional) You can use the FQDN of the VMware Identity Manager server instance.

Option	Description
<b>Metadata URL</b>	URL for retrieving all of the information required to exchange SAML information between the SAML identity provider and the View Connection Server instance. In the URL <code>https://&lt;YOUR HORIZON SERVER NAME&gt;/SAAS/API/1.0/GET/metadata/idp.xml</code> , click <b>&lt;YOUR HORIZON SERVER NAME&gt;</b> and replace it with the FQDN of the VMware Identity Manager server instance.
<b>Administration URL</b>	URL for accessing the administration console of the SAML identity provider (VMware Identity Manager instance). This URL has the format <code>https://&lt;Identity-Manager-FQDN&gt;:8443</code> .

- 6 Click **OK** to save the SAML authenticator configuration.

If you provided valid information, you must either accept the self-signed certificate (not recommended) or use a trusted certificate for View and VMware Identity Manager.

The **SAML 2.0 Authenticator** drop-down menu displays the newly created authenticator, which is now set as the selected authenticator.

- 7 In the System Health section on the View Administrator dashboard, select **Other components > SAML 2.0 Authenticators**, select the SAML authenticator that you added, and verify the details.

If the configuration is successful, the authenticator's health is green. An authenticator's health can display red if the certificate is untrusted, if the VMware Identity Manager service is unavailable, or if the metadata URL is invalid. If the certificate is untrusted, you might be able to click **Verify** to validate and accept the certificate.

- 8 Log in to the VMware Identity Manager administration console, go to the View Pools page, and select the **Suppress Password Popup** check box.

#### What to do next

- Extend the expiration period of the View Connection Server metadata so that remote sessions are not terminated after only 24 hours. See [“Change the Expiration Period for Service Provider Metadata on View Connection Server,”](#) on page 64.
- Use the `vdmutl` command-line interface to configure True SSO on a connection server. See [“Configure View Connection Server for True SSO,”](#) on page 84.

For more information about how SAML authentication works, see [“Using SAML Authentication,”](#) on page 61.

## Configure View Connection Server for True SSO

You can use the `vdmutl` command-line interface to configure and enable or disable True SSO.

This procedure is required to be performed on only one connection server in the cluster.

---

**IMPORTANT** This procedure uses only the commands necessary for enabling True SSO. For a list of all the configuration options available for managing True SSO configurations, and a description of each option, see [“Command-line Reference for Configuring True SSO,”](#) on page 86.

---

#### Prerequisites

- Verify that you can run the command as a user who has the Administrators role. You can use View Administrator to assign the Administrators role to a user. See [Chapter 6, “Configuring Role-Based Delegated Administration,”](#) on page 95.
- Verify that you have the fully qualified domain name (FQDN) for the following servers:
  - Connection server

- Enrollment server  
For more information, see [“Install and Set Up an Enrollment Server,”](#) on page 79.
- Enterprise certificate authority  
For more information, see [“Set Up an Enterprise Certificate Authority,”](#) on page 76.
- Verify that you have the Netbios name or the FQDN of the domain.
- Verify that you have created a certificate template. See [“Create Certificate Templates Used with True SSO,”](#) on page 78.
- Verify that you have created a SAML authenticator to delegate authentication to VMware Identity Manager. See [“Configure SAML Authentication to Work with True SSO,”](#) on page 83.

## Procedure

- 1 On a connection server in the cluster, open a command prompt and enter the command to add an enrollment server.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password
--truesso --environment --add --enrollmentServer enroll-server-fqdn
```

The enrollment server is added to the global list.

- 2 Enter the command to list the information for that enrollment server.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password
--truesso --environment --list --enrollmentServer enroll-server-fqdn --domain domain-fqdn
```

The output shows the forest name, whether the certificate for the enrollment server is valid, the name and details of the certificate template you can use, and the common name of the certificate authority. To configure which domains the enrollment server can connect to, you can use a Windows Registry setting on the enrollment server. The default is to connect to all trusting domains.

---

**IMPORTANT** You will be required to specify the common name of the certificate authority in the next step.

---

- 3 Enter the command to create a True SSO connector, which will hold the configuration information, and enable the connector.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password
--truesso --create --connector --domain domain-fqdn --template TrueSSO-template-name --
primaryEnrollmentServer enroll-server-fqdn --certificateServer ca-common-name --mode enabled
```

In this command, *TrueSSO-template-name* is the name of the template shown in the output for the previous step, and *ca-common-name* is the common name of the enterprise certificate authority shown in that output.

The True SSO connector is enabled on a pool or cluster for the domain specified. To disable True SSO at the pool level, run `vdmUtil --certsso --edit --connector <domain> --mode disabled`. To disable true SSO for an individual virtual machine, you can use GPO (`vdm_agent.adm`).

- 4 Enter the command to discover which SAML authenticators are available.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password
--truesso --list --authenticator
```

Authenticators are created when you configure SAML authentication between VMware Identity Manager and a connection server, using View Administrator.

The output shows the name of the authenticator and shows whether True SSO is enabled.

---

**IMPORTANT** You will be required to specify the authenticator name in the next step.

---

- 5 Enter the command to enable the authenticator to use True SSO mode.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password
--truesso --authenticator --edit --name authenticator-fqdn --truessoMode {ENABLED|ALWAYS}
```

For `--truessoMode`, use `ENABLED` if you want True SSO to be used only if no password was supplied when the user logged in to VMware Identity Manager. In this case if a password was used and cached, the system will use the password. Set `--truessoMode` to `ALWAYS` if you want True SSO to be used even if a password was supplied when the user logged in to VMware Identity Manager.

### What to do next

In View Administrator, verify the health status of the True SSO configuration. For more information, see [“Using the System Health Dashboard to Troubleshoot Issues Related to True SSO,”](#) on page 92.

To configure advanced options, use Windows advanced settings on the appropriate system. See [“Advanced Configuration Settings for True SSO,”](#) on page 90.

## Command-line Reference for Configuring True SSO

You can use the `vdmutil` command-line interface to configure and manage the True SSO feature.

### Location of the Utility

By default, the path to the `vdmutil` command executable file is `C:\Program Files\VMware\VMware View\Server\tools\bin`. To avoid entering the path on the command line, add the path to your `PATH` environment variable.

### Syntax and Authentication

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

```
vdmutil authentication options --truesso additional options and arguments
```

The additional options that you can use depend on the command option. This topic focuses on the options for configuring True SSO (`--truesso`). Following is an example of a command for listing connectors that have been configured for True SSO:

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --
truesso --list --connector
```

The `vdmutil` command includes authentication options to specify the user name, domain, and password to use for authentication.

**Table 5-1.** vdmutil Command Authentication Options

Option	Description
<code>--authAs</code>	Name of a View administrator user. Do not use <code>domain\username</code> or user principal name (UPN) format.
<code>--authDomain</code>	Fully qualified domain name or Netbios name of the domain for the View administrator user specified in the <code>--authAs</code> option.
<code>--authPassword</code>	Password for the View administrator user specified in the <code>--authAs</code> option. Entering "*" instead of a password causes the <code>vdmutil</code> command to prompt for the password and does not leave sensitive passwords in the command history on the command line.

You must use the authentication options with all `vdmutil` command options except for `--help` and `--verbose`.

## Command Output

The `vdmutil` command returns 0 when an operation succeeds and a failure-specific non-zero code when an operation fails. The `vdmutil` command writes error messages to standard error. When an operation produces output, or when verbose logging is enabled by using the `--verbose` option, the `vdmutil` command writes output to standard output, in US English.

## Commands for Managing Enrollment Servers

You must add one enrollment server for each domain. You can also add a second enrollment server and later designate that server to be used as a backup.

For readability, the options shown in the following table do not represent the complete command you would enter. Only the options specific to the particular task are included. For example, one row shows the `--environment --list --enrollmentServers` options, but the `vdmutil` command you would actually enter also contains options for authentication and for specifying that you are configuring True SSO:

```
vdmutil --authAs admin-role-user --authDomain netbios-name --authPassword admin-user-password --truesso --environment --list --enrollmentServers
```

For more information about the authentication options, see [“Command-line Reference for Configuring True SSO,”](#) on page 86.

**Table 5-2.** `vdmutil truesso` Command Options for Managing Enrollment Servers

Command and Options	Description
<code>--environment --add --enrollmentServer enroll-server-fqdn</code>	Adds the specified enrollment server to the environment, where <i>enroll-server-fqdn</i> is the FQDN of the enrollment server. If the enrollment server has already been added, when you run this command, nothing happens.
<code>--environment --remove --enrollmentServer enroll-server-fqdn</code>	Removes the specified enrollment server from the environment, where <i>enroll-server-fqdn</i> is the FQDN of the enrollment server. If the enrollment server has already been removed, when you run this command, nothing happens.
<code>--environment --list --enrollmentServers</code>	Lists the FQDNs of all enrollment servers in the environment.
<code>--environment --list --enrollmentServer enroll-server-fqdn</code>	<p>Lists the FQDNs of the domains and forests that are trusted by the domains and forests to which the enrollment server belongs, and the state of the enrollment certificate, which can be VALID or INVALID. VALID means the enrollment server has an Enrollment Agent certificate installed. The state might be INVALID for any of several reasons:</p> <ul style="list-style-type: none"> <li>■ The certificate has not been installed.</li> <li>■ The certificate is not yet valid, or has expired.</li> <li>■ The certificate was not issued by a trusted Enterprise CA.</li> <li>■ The private key is not available.</li> <li>■ The certificate has been corrupted.</li> </ul> <p>The log file on the enrollment server can provide the reason for the INVALID state.</p>
<code>--environment --list --enrollmentServer enroll-server-fqdn --domain domain-fqdn</code>	For the enrollment server in the specified domain, lists the CNs (common names) of the available certificate authorities, and provides the following information about each certificate template that can be used for True SSO: name, minimum key length, and hash algorithm.

## Commands for Managing Connectors

You create one connector for each domain. The connector defines the parameters that are used for True SSO.

For readability, the options shown in the following table do not represent the complete command you would enter. Only the options specific to the particular task are included. For example, one row shows the `--list --connector` options, but the `vdmUtil` command you would actually enter also contains options for authentication and for specifying that you are configuring True SSO:

```
vdmUtil --authAs admin-role-user --authDomain netbios-name --authPassword admin-user-password --truesso --list --connector
```

For more information about the authentication options, see [“Command-line Reference for Configuring True SSO,”](#) on page 86.

**Table 5-3.** vdmutil truesso Command Options for Managing Connectors

Options	Description
<code>--create --connector --domain domain-fqdn</code> <code>--template template-name</code> <code>--primaryEnrollmentServer enroll-server1-fqdn</code> [ <code>--secondaryEnrollmentServer enroll-server2-fqdn</code> ] <code>--certificateServer CA-common-name</code> <code>--mode {enabled  disabled}</code>	<p>Creates a connector for the specified domain and configures the connector to use the following settings:</p> <ul style="list-style-type: none"> <li>■ <i>template-name</i> is the name of the certificate template to use.</li> <li>■ <i>enroll-server1-fqdn</i> is the FQDN of the primary enrollment server to use.</li> <li>■ <i>enroll-server2-fqdn</i> is the FQDN of the secondary enrollment server to use. This setting is optional.</li> <li>■ <i>CA-common-name</i> is the common name of the certificate authority to use. This can be a comma-separated list of CAs.</li> </ul> <p>To determine which certificate template and certificate authority are available for a particular enrollment server, you can run the <code>vdmutil</code> command with the <code>--truesso --environment --list --enrollmentServer enroll-server-fqdn --domain domain-fqdn</code> options.</p>
<code>--list --connector</code>	Lists the FQDNs of the domains that already have a connector created.
<code>--list --connector --verbose</code>	<p>Lists all the domains that have connectors, and for each connector, provides the following information:</p> <ul style="list-style-type: none"> <li>■ Primary enrollment server</li> <li>■ Secondary enrollment server, if there is one</li> <li>■ Name of the certificate template</li> <li>■ Whether the connector is enabled or disabled</li> <li>■ Common name of the certificate authority server or servers, if there are more than one</li> </ul>
<code>--edit --connector domain-fqdn</code> [ <code>--template template-name</code> ] [ <code>--mode {enabled  disabled}</code> ] [ <code>--primaryEnrollmentServer enroll-server1-fqdn</code> ] [ <code>--secondaryEnrollmentServer enroll-server2-fqdn</code> ] [ <code>--certificateServer CA-common-name</code> ]	<p>For the connector created for the domain specified by <i>domain-fqdn</i>, allows you to change any of the following settings:</p> <ul style="list-style-type: none"> <li>■ <i>template-name</i> is the name of the certificate template to use.</li> <li>■ The mode can be either <code>enabled</code> or <code>disabled</code>.</li> <li>■ <i>enroll-server1-fqdn</i> is the FQDN of the primary enrollment server to use.</li> <li>■ <i>enroll-server2-fqdn</i> is the FQDN of the secondary enrollment server to use. This setting is optional.</li> <li>■ <i>CA-common-name</i> is the common name of the certificate authority to use. This can be a comma-separated list of CAs.</li> </ul>
<code>--delete --connector domain-fqdn</code>	Deletes the connector that has been created for the domain specified by <i>domain-fqdn</i> .

## Commands for Managing Authenticators

Authenticators are created when you configure SAML authentication between VMware Identity Manager and a connection server. The only management task is to enable or disable True SSO for the authenticator.

For readability, the options shown in the following table do not represent the complete command you would enter. Only the options specific to the particular task are included. For example, one row shows the `--list --authenticator` options, but the `vdmUtil` command you would actually enter also contains options for authentication and for specifying that you are configuring True SSO:

```
vdmUtil --authAs admin-role-user --authDomain netbios-name --authPassword admin-user-password --truessso --list --authenticator
```

For more information about the authentication options, see [“Command-line Reference for Configuring True SSO,”](#) on page 86.

**Table 5-4.** vdmutil truessso Command Options for Managing Authenticators

Command and Options	Description
<code>--list --authenticator [--verbose]</code>	Lists the fully qualified domain names (FQDNs) of all SAML authenticators found in the domain. For each one, specifies whether True SSO is enabled. If you use the <code>--verbose</code> option, the FQDNs of the associated connection servers are also listed.
<code>--list --authenticator --name label</code>	For the specified authenticator, lists whether True SSO is enabled, and lists the FQDNs of the associated connection servers. For <i>label</i> use one of the names listed when you use the <code>--authenticator</code> option without the <code>--name</code> option.
<code>--edit --authenticator --name label</code> <code>--truesssoMode mode-value</code>	For the specified authenticator, sets the True SSO mode to the value you specify, where <i>mode-value</i> can be one of the following values: <ul style="list-style-type: none"> <li>■ <b>ENABLED.</b> True SSO is used only when the Active Directory credentials of the user is not available.</li> <li>■ <b>ALWAYS.</b> True SSO is always used even if vIDM has the AD credentials of the user.</li> <li>■ <b>DISABLED.</b> True SSO is disabled.</li> </ul> For <i>label</i> use one of the names listed when you use the <code>--authenticator</code> option without the <code>--name</code> option.

## Advanced Configuration Settings for True SSO

You can manage the True SSO advanced settings by using the GPO template on the Horizon Agent machine, registry settings on the enrollment server, and LDAP entries on the connection server. These settings include default timeout, configure load balancing, specify domains to be included, and more.

### Horizon Agent Configuration Settings

You can use GPO template on the agent OS to turn off True SSO at the pool level or to change defaults for certificate settings such as key size and count and settings for reconnect attempts.

**NOTE** The following table shows the settings to use for configuring the agent on individual virtual machines, but you can alternatively use the Horizon Agent Configuration template files. The ADMX template file is named (`vdm_agent.admx`). The ADM template file is named (`vdm_agent.adm`). Use the template files to make these policy settings apply to all the virtual machines in a desktop or application pool. If a policy is set the policy takes precedence over the registry settings. In Horizon 7 version 7.1, the ADM template files are deprecated and the ADMX template files are added.

The ADMX files are available in a bundled .zip file named `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip`, which you can download from the VMware download site at <https://my.vmware.com/web/vmware/downloads>. Under Desktop & End-User Computing, select the VMware Horizon 7 download, which includes the bundled .zip file.

**Table 5-5.** Keys for Configuring True SSO on Horizon Agent

Key	Min & Max	Description
Disable True SSO	N/A	Set this key to <b>true</b> to disable the feature on the agent. Use this setting in the group policy to disable True SSO at the pool level. The default is <b>false</b> .
Certificate wait timeout	10 -120	Specifies timeout period of certificates to arrive on the agent, in seconds. The default is <b>40</b> .
Minimum key size	1024 - 8192	Minimum allowed size for a key. The default is <b>1024</b> , meaning that by default, if the key size is below 1024, the key cannot be used.
All key sizes	N/A	Comma-separated list of key sizes that can be used. Up to 5 sizes can be specified; for example: <b>1024, 2048, 3072, 4096</b> . The default is <b>2048</b> .
Number of keys to pre-create	1-100	Number of keys to pre-create on RDS servers that provide remote desktops and hosted Windows applications. The default is <b>5</b> .
Minimum validity period required for a certificate	N/A	Minimum validity period, in minutes, required for a certificate when it is being reused to reconnect a user. The default is <b>5</b> .

### Enrollment Server Configuration Settings

You can use Windows Registry settings on the enrollment server OS to configure which domains to connect to, various timeout periods, polling periods, and retries, and whether to prefer using the certificate authority that is installed on the same local server (recommended).

To change the advanced configuration settings, you can open the Windows Registry Editor (`regedit.exe`) on the enrollment server machine and navigate to the following registry key:

`HKLM\SOFTWARE\VMware, Inc.\VMware VDM\Enrollment Service`

**Table 5-6.** Registry Keys for Configuring True SSO on the Enrollment Server

Registry Key	Min & Max	Type	Description
ConnectToDomains	N/A	REG_MULTI_SZ	List of domains the enrollment server attempts to connect to automatically. For this multi-string registry type, the DNS fully qualified domain name (FQDN) of each domain is listed on its own line. The default is to trust all domains.
ExcludeDomains	N/A	REG_MULTI_SZ	List of domains the enrollment server does not connect to automatically. If the connection server provides a configuration set with any of the domains, the enrollment server will attempt to connect to that domain or domains. For this multi-string registry type, the DNS FQDN of each domain is listed on its own line. The default is to exclude no domains.
ConnectToDomainsInForest	N/A	REG_SZ	Specifies whether to connect to and use all domains in the forest that the enrollment server is a member of. The default is TRUE. Use one of the following values: <ul style="list-style-type: none"> <li>■ 0 means false; do not connect to the domains of the forest being used.</li> <li>■ !=0 means true.</li> </ul>
ConnectToTrustingDomains	N/A	REG_SZ	Specifies whether to connect to explicitly trusting/incoming domains. The default is TRUE. Use one of the following values: <ul style="list-style-type: none"> <li>■ 0 means false; do not connect to explicitly trusting/incoming domains.</li> <li>■ !=0 means true.</li> </ul>
PreferLocalCa	N/A	REG_SZ	Specifies whether to prefer the locally installed CA, if available, for performance benefits. If set to TRUE, the enrollment server will send requests to the local CA. If the connection to the local CA fails, the enrollment server will try to send certificates requests to alternate CAs. The default is FALSE. Use one of the following values: <ul style="list-style-type: none"> <li>■ 0 means false.</li> <li>■ !=0 means true.</li> </ul>
MaxSubmitRetryTime	9500-59000	DWORD	Amount of time to wait before retrying to submit a certificate signing request, in milliseconds. The default is <b>25000</b> .
SubmitLatencyWarningTime	500 - 5000	DWORD	Submit latency warning time when the interface is marked "Degraded" (in milliseconds). The default is <b>1500</b> . The enrollment server uses this setting to determine whether a CA should be considered to be in a degraded state. If the last three certificate requests took more milliseconds to complete than are specified by this setting, the CA is considered degraded, and this status appears in the View Administrator Health Status dashboard. A CA usually issues a certificate within 20 ms, but if the CA has been idle for a few hours, any initial request might take longer to complete. This setting allows an administrator to find out that a CA is slow, without necessary having the CA marked as slow. Use this setting to configure the threshold for marking the CA as slow.

## Connection Server Configuration Settings

You can edit View LDAP on View Connection Server to configure a timeout for generating certificates and whether to enable load balancing certificate requests between enrollment server (recommended).

To change the advanced configuration settings, you must use ADSI Edit on a View Connection Server host. You can connect by typing in the distinguished name **DC=vdi**, **DC=vmware**, **DC=int** as the connection point, and typing in the server name and port for the computer **localhost:389**. Expand **OU=Properties**, select **OU=Global**, and double-click **CN=Common** in the right pane.

You can then edit the **pae-NameValuePair** attribute to add one or more of the values listed in the following table. You must use the syntax *name=value* when adding values.

**Table 5-7.** Advanced True SSO Settings for Connection Servers

Registry Key	Description
<code>cs-view-certss-enable-es-loadbalance=[true false]</code>	Specifies whether to enable load balancing CSR requests between two enrollment servers. The default is false.  For example, add <code>cs-view-certss-enable-es-loadbalance=true</code> to enable load balancing so that when certificate requests arrive, the connection server will use alternate enrollment servers. Each enrollment server can service the requests using the local CA, if you have the enrollment server and CA on the same host.
<code>cs-view-certss-certgen-timeout-sec=number</code>	Amount of time to wait for generating a certificate after receiving a CSR, in seconds. The default is <b>35</b> .

## Using the System Health Dashboard to Troubleshoot Issues Related to True SSO

You can use the system health dashboard in View Administrator to quickly see problems that might affect the operation of the True SSO feature.

For end users, if True SSO stops working, when the system attempts to log the user in to the remote desktop or application, the user sees the following message: "The user name or password is incorrect." After the user clicks **OK**, the user is taken to the login screen. On the Windows login screen the user sees an extra tile labeled **VMware SSO User**. If the user has the Active Directory credentials for an entitled user, the user can log in with AD credentials.

The system health dashboard in the top-left portion of the View Administrator display contains a couple of items that pertain to True SSO.

**Note** The True SSO feature provides information to the dashboard only once per minute. Click the refresh icon in the upper-right corner to refresh the information immediately.

- You can click to expand **View Components > True SSO** to see a list of the domains that are using True SSO.

You can click a domain name to see the following information: a list of enrollment servers configured for that domain, a list of enterprise certificate authorities, the name of the certificate template being used, and the status. If there is a problem, the Status field explains what it is.

To change any of the configuration settings shown in the True SSO Domain Details dialog box, use the `vdmutl` command-line interface to edit the True SSO connector. For more information, see [“Commands for Managing Connectors,”](#) on page 88.

- You can click to expand **Other Components > SAML 2.0 Authenticators** to see a list of the SAML authenticators that have been created for delegating authentication to VMware Identity Manager instances. You can click the authenticator name to examine the details and status.

**Note** In order for True SSO to be used, the global setting for SSO must be enabled. In View Administrator, select **Configuration > Global Settings**, and verify that **Single sign-on (SSO)** is set to **Enabled**.

**Table 5-8.** Broker to Enrollment Server Connection Status

Status Text	Description
Failed to fetch True SSO health information.	The dashboard is unable to retrieve the health information from the broker.
The <FQDN> enrollment server cannot be contacted by the True SSO configuration service.	In a POD, one of the brokers is elected to send the configuration information to all enrollment servers used by the POD. This broker will refresh the enrollment server configuration once every minute. This message is displayed if the configuration task has failed to update the enrollment server. For additional information, see the table for Enrollment Server Connectivity.
The <FQDN> enrollment server cannot be contacted to manage sessions on this connection server.	The current broker is unable to connect to the enrollment server. This status is only displayed for the broker that your browser is pointing to. If there are multiple brokers in the pod, you need to change your browser to point to the other brokers in order to check their status. For additional information, see the table for Enrollment Server Connectivity.

**Table 5-9.** Enrollment Server Connectivity

Status Text	Description
This domain <Domain Name> does not exist on the <FQDN> enrollment server.	The True SSO connector has been configured to use this enrollment server for this domain, but the enrollment server has not yet been configured to connect to this domain. If the state remains for longer than one minute, you need to check the state of the broker currently responsible for refreshing the enrollment configuration.
The <FQDN> enrollment server's connection to the domain <Domain Name> is still being established.	The enrollment server has not been able to connect to a domain controller in this domain. If this state remains for longer than a minute, you might have to verify that name resolution from the enrollment server to the domain is correct, and that there is network connectivity between the enrollment server and the domain.
The <FQDN> enrollment server's connection to the domain <Domain Name> is stopping or in a problematic state.	The enrollment server has connected to a domain controller in the domain, but it has not been able to read the PKI information from the domain controller. If this happens, then there is likely a problem with the actual domain controller. This issue can also happen if DNS is not configured correctly. Check the log file on the enrollment server to see what domain controller the enrollment server is trying to use, and verify that the domain controller is fully operational.
The <FQDN> enrollment server has not yet read the enrollment properties from a domain controller.	This state is transitional, and is only displayed during startup of the enrollment server, or when a new domain has been added to the environment. This state usually lasts less than one minute. If this state lasts longer than a minute, either the network is extremely slow, or there is an issue causing difficulties accessing the domain controller.
The <FQDN> enrollment server has read the enrollment properties at least once, but has not been able to reach a domain controller for some time.	As long as the enrollment server reads the PKI configuration from a domain controller, it keeps polling for changes once every two minutes. This status will be set if the domain controller (DC) has been unreachable for a short period of time. Typically this inability to contact the DC might mean the enrollment server cannot detect any changes in PKI configuration. As long as the certificate servers can still access a domain controller, certificates can still be issued.
The <FQDN> enrollment server has read the enrollment properties at least once but either has not been able to reach a domain controller for an extended time or another issue exists.	If the enrollment server has not been able to reach the domain controller for an extended period, then this state is displayed. The enrollment server will then try to discover an alternative domain controller for this domain. If a certificate server can still access a domain controller, then certificates can still be issued, but if this state remains for more than one minute, it means the enrollment server has lost access to all domain controllers for the domain, and it is likely that certificates can no longer be issued.

**Table 5-10.** Enrollment Certificate Status

Status Text	Description
A valid enrollment certificate for this domain's <domain name> forest is not installed on the <FQDN> enrollment server, or it may have expired	No enrollment certificate for this domain has been installed, or the certificate is invalid or has expired. The enrollment certificate must be issued by an enterprise CA that is trusted by the forest this domain is a member of. Verify that you have completed the steps in the <i>View Administration</i> document, which describes how to install the enrollment certificate on the enrollment server. You can also open the MMC, certificate management snap-in, opening the local computer store. Open the Personal certificate container and verify that the certificate is installed, and that it is valid. You can also open the enrollment server log file. The enrollment server will log additional information about the state of any certificate it located.

**Table 5-11.** Certificate Template Status

Status Text	Description
The template <name> does not exist on the <FQDN> enrollment server domain.	Check that you specified the correct template name.
Certificates generated by this template can NOT be used to log on to windows.	This template does not have the smart card usage enabled and data signing enabled. Check that you specified the correct template name. Verify that you have .completed the steps described in <a href="#">“Create Certificate Templates Used with True SSO,”</a> on page 78.
The template <name> is smartcard logon enabled, but cannot be used.	This template is enabled for smart card logon, but the template cannot be used with True SSO. Check that you specified the correct template name, verify that you have gone through the steps described in <a href="#">“Create Certificate Templates Used with True SSO,”</a> on page 78. You can also check the enrollment server log file, since it will log what setting in the template is preventing it from being used for True SSO.

**Table 5-12.** Certificate Server Configuration Status

Status Text	Description
The certificate server <CN of CA> does not exist in the domain.	Verify that you specified the correct name for the CA. You must specify the Common Name (CN).
The certificate is not in the NTAUTH (Enterprise) store.	This CA is not an enterprise CA or its CA certificate has not been added to the NTAUTH store. If this CA is not a member of the forest, you must manually add the CA certificate to the NTAUTH store of this forest.

**Table 5-13.** Certificate Server Connection Status

Status Text	Description
The <FQDN> enrollment server is not connected to the certificate server <CN of CA>.	The enrollment server is not connected to the certificate server. This state might be a transitional state if the enrollment server just started, or if the CA was recently added to a True SSO connector. If the state remains for longer than one minute, it means that the enrollment server failed to connect to the CA. Validate that name resolution is working correctly, and that you have network connectivity to the CA, and that the system account for the enrollment server has permission to access the CA.
The <FQDN> enrollment server has connected to the certificate server <CN of CA>, but the certificate server is in a degraded state	This state is displayed if the CA is slow at issuing certificates. If the CA remains in this state, check the load of the CA or the domain controllers used by the CA. <b>NOTE</b> If the CA has been marked as slow, it will retain this state until at least one certificate request has been completed successfully, and that certificate was issued within a normal time frame.
The <FQDN> enrollment server can connect to the certificate server <CN of CA>, but the service is unavailable.	This state is issued if the enrollment server has an active connection to the CA but it is unable to issue certificates. This state is typically a transitional state. If the CA does not become available quickly, the state will be changed to disconnected.

# Configuring Role-Based Delegated Administration

---

# 6

One key management task in a View environment is to determine who can use View Administrator and what tasks those users are authorized to perform. With role-based delegated administration, you can selectively assign administrative rights by assigning administrator roles to specific Active Directory users and groups.

This chapter includes the following topics:

- [“Understanding Roles and Privileges,”](#) on page 95
- [“Using Access Groups to Delegate Administration of Pools and Farms,”](#) on page 96
- [“Understanding Permissions,”](#) on page 97
- [“Manage Administrators,”](#) on page 98
- [“Manage and Review Permissions,”](#) on page 99
- [“Manage and Review Access Groups,”](#) on page 101
- [“Manage Custom Roles,”](#) on page 103
- [“Predefined Roles and Privileges,”](#) on page 105
- [“Required Privileges for Common Tasks,”](#) on page 109
- [“Best Practices for Administrator Users and Groups,”](#) on page 111

## Understanding Roles and Privileges

The ability to perform tasks in View Administrator is governed by an access control system that consists of administrator roles and privileges. This system is similar to the vCenter Server access control system.

An administrator role is a collection of privileges. Privileges grant the ability to perform specific actions, such as entitling a user to a desktop pool. Privileges also control what an administrator can see in View Administrator. For example, if an administrator does not have privileges to view or modify global policies, the **Global Policies** setting is not visible in the navigation panel when the administrator logs in to View Administrator.

Administrator privileges are either global or object-specific. Global privileges control system-wide operations, such as viewing and changing global settings. Object-specific privileges control operations on specific types of objects.

Administrator roles typically combine all of the individual privileges required to perform a higher-level administration task. View Administrator includes predefined roles that contain the privileges required to perform common administration tasks. You can assign these predefined roles to your administrator users and groups, or you can create your own roles by combining selected privileges. You cannot modify the predefined roles.

To create administrators, you select users and groups from your Active Directory users and groups and assign administrator roles. Administrators obtain privileges through their role assignments. You cannot assign privileges directly to administrators. An administrator that has multiple role assignments acquires the sum of all the privileges contained in those roles.

## Using Access Groups to Delegate Administration of Pools and Farms

By default, automated desktop pools, manual desktop pools, and farms are created in the root access group, which appears as / or Root(/) in View Administrator. RDS desktop pools and application pools inherit their farm's access group. You can create access groups under the root access group to delegate the administration of specific pools or farms to different administrators.

---

**NOTE** You cannot change the access group of an RDS desktop pool or an application pool directly. You must change the access group of the farm that the RDS desktop pool or the application pool belongs to.

---

A virtual or physical machine inherits the access group from its desktop pool. An attached persistent disk inherits the access group from its machine. You can have a maximum of 100 access groups, including the root access group.

You configure administrator access to the resources in an access group by assigning a role to an administrator on that access group. Administrators can access the resources that reside only in access groups for which they have assigned roles. The role that an administrator has on an access group determines the level of access that the administrator has to the resources in that access group.

Because roles are inherited from the root access group, an administrator that has a role on the root access group has that role on all access groups. Administrators who have the Administrators role on the root access group are super administrators because they have full access to all of the objects in the system.

A role must contain at least one object-specific privilege to apply to an access group. Roles that contain only global privileges cannot be applied to access groups.

You can use View Administrator to create access groups and to move existing desktop pools to access groups. When you create an automated desktop pool, a manual pool, or a farm, you can accept the default root access group or select a different access group.

---

**NOTE** If you intend to provide access to your desktops and applications through VMware Identity Manager, verify that you create the desktop and application pools as a user who has the Administrators role on the root access group in View Administrator. If you give the user the Administrators role on an access group other than the root access group, VMware Identity Manager will not recognize the SAML authenticator you configure in View, and you cannot configure the pool in VMware Identity Manager.

---

- [Different Administrators for Different Access Groups](#) on page 96

You can create a different administrator to manage each access group in your configuration.

- [Different Administrators for the Same Access Group](#) on page 97

You can create different administrators to manage the same access group.

### Different Administrators for Different Access Groups

You can create a different administrator to manage each access group in your configuration.

For example, if your corporate desktop pools are in one access group and your desktop pools for software developers are in another access group, you can create different administrators to manage the resources in each access group.

[Table 6-1](#) shows an example of this type of configuration.

**Table 6-1.** Different Administrators for Different Access Groups

Administrator	Role	Access Group
view-domain.com\Admin1	Inventory Administrators	/CorporateDesktops
view-domain.com\Admin2	Inventory Administrators	/DeveloperDesktops

In this example, the administrator called Admin1 has the Inventory Administrators role on the access group called CorporateDesktops and the administrator called Admin2 has the Inventory Administrators role on the access group called DeveloperDesktops.

## Different Administrators for the Same Access Group

You can create different administrators to manage the same access group.

For example, if your corporate desktop pools are in one access group, you can create one administrator that can view and modify those pools and another administrator that can only view them.

Table 6-2 shows an example of this type of configuration.

**Table 6-2.** Different Administrators for the Same Access Group

Administrator	Role	Access Group
view-domain.com\Admin1	Inventory Administrators	/CorporateDesktops
view-domain.com\Admin2	Inventory Administrators (Read only)	/CorporateDesktops

In this example, the administrator called Admin1 has the Inventory Administrators role on the access group called CorporateDesktops and the administrator called Admin2 has the Inventory Administrators (Read only) role on the same access group.

## Understanding Permissions

View Administrator presents the combination of a role, an administrator user or group, and an access group as a permission. The role defines the actions that can be performed, the user or group indicates who can perform the action, and the access group contains the objects that are the target of the action.

Permissions appear differently in View Administrator depending on whether you select an administrator user or group, an access group, or a role.

Table 6-3 shows how permissions appear in View Administrator when you select an administrator user or group. The administrator user is called Admin 1 and it has two permissions.

**Table 6-3.** Permissions on the Administrators and Groups Tab for Admin 1

Role	Access Group
Inventory Administrators	MarketingDesktops
Administrators (Read only)	/

The first permission shows that Admin 1 has the Inventory Administrators role on the access group called MarketingDesktops. The second permission shows that Admin 1 has the Administrators (Read only) role on the root access group.

Table 6-4 shows how the same permissions appear in View Administrator when you select the MarketingDesktops access group.

**Table 6-4.** Permissions on the Folders Tab for MarketingDesktops

Admin	Role	Inherited
view-domain.com\Admin1	Inventory Administrators	
view-domain.com\Admin1	Administrators (Read only)	Yes

The first permission is the same as the first permission shown in [Table 6-3](#). The second permission is inherited from the second permission shown in [Table 6-3](#). Because access groups inherit permissions from the root access group, Admin1 has the Administrators (Read only) role on the MarketingDesktops access group. When a permission is inherited, Yes appears in the Inherited column.

[Table 6-5](#) shows how the first permission in [Table 6-3](#) appears in View Administrator when you select the Inventory Administrators role.

**Table 6-5.** Permissions on the Role Tab for Inventory Administrators

Administrator	Access Group
view-domain.com\Admin1	/MarketingDesktops

## Manage Administrators

Users who have the Administrators role can use View Administrator to add and remove administrator users and groups.

The Administrators role is the most powerful role in View Administrator. Initially, members of the View Administrators account are given the Administrators role. You specify the View Administrators account when you install View Connection Server. The View Administrators account can be the local Administrators group (BUILTIN\Administrators) on the View Connection Server computer or a domain user or group account.

**NOTE** By default, the Domain Admins group is a member of the local Administrators group. If you specified the View Administrators account as the local Administrators group, and you do not want domain administrators to have full access to inventory objects and View configuration settings, you must remove the Domain Admins group from the local Administrators group.

- [Create an Administrator](#) on page 98

To create an administrator, you select a user or group from your Active Directory users and groups in View Administrator and assign an administrator role.

- [Remove an Administrator](#) on page 99

You can remove an administrator user or group. You cannot remove the last super administrator in the system. A super administrator is an administrator that has the Administrators role on the root access group.

## Create an Administrator

To create an administrator, you select a user or group from your Active Directory users and groups in View Administrator and assign an administrator role.

### Prerequisites

- Become familiar with the predefined administrator roles. See [“Predefined Roles and Privileges,”](#) on page 105.
- Become familiar with the best practices for creating administrator users and groups. See [“Best Practices for Administrator Users and Groups,”](#) on page 111.

- To assign a custom role to the administrator, create the custom role. See [“Add a Custom Role,”](#) on page 104.
- To create an administrator that can manage specific desktop pools, create an access group and move the desktop pools to that access group. See [“Manage and Review Access Groups,”](#) on page 101.

### Procedure

- 1 In View Administrator, select **View Configuration > Administrators**.
- 2 On the **Administrators and Groups** tab, click **Add User or Group**.
- 3 Click **Add**, select one or more search criteria, and click **Find** to filter Active Directory users or groups based on your search criteria.
- 4 Select the Active Directory user or group that you want to be an administrator user or group, click **OK** and click **Next**.

You can press the Ctrl and Shift keys to select multiple users and groups.

- 5 Select a role to assign to the administrator user or group.

The Applies to an access group column indicates whether a role applies to access groups. Only roles that contain object-specific privileges apply to access groups. Roles that contain only global privileges do not apply to access groups.

Option	Action
<b>The role you selected applies to access groups</b>	Select one or more access groups and click <b>Next</b> .
<b>You want the role to apply to all access groups</b>	Select the root access group and click <b>Next</b> .

- 6 Click **Finish** to create the administrator user or group.

The new administrator user or group appears in the left pane and the role and access group that you selected appear in the right pane on the **Administrators and Groups** tab.

## Remove an Administrator

You can remove an administrator user or group. You cannot remove the last super administrator in the system. A super administrator is an administrator that has the Administrators role on the root access group.

### Procedure

- 1 In View Administrator, select **View Configuration > Administrators**.
- 2 On the **Administrators and Groups** tab, select the administrator user or group, click **Remove User or Group**, and click **OK**.

The administrator user or group no longer appears on the **Administrators and Groups** tab.

## Manage and Review Permissions

You can use View Administrator to add, delete, and review permissions for specific administrator users and groups, for specific roles, and for specific access groups.

- [Add a Permission](#) on page 100

You can add a permission that includes a specific administrator user or group, a specific role, or a specific access group.

- [Delete a Permission](#) on page 100

You can delete a permission that includes a specific administrator user or group, a specific role, or a specific access group.

- [Review Permissions](#) on page 101

You can review the permissions that include a specific administrator or group, a specific role, or a specific access group.

## Add a Permission

You can add a permission that includes a specific administrator user or group, a specific role, or a specific access group.

### Procedure

- 1 In View Administrator, select **View Configuration > Administrators**.
- 2 Create the permission.

Option	Action
<b>Create a permission that includes a specific administrator user or group</b>	<ol style="list-style-type: none"> <li>a On the <b>Administrators and Groups</b> tab, select the administrator or group and click <b>Add Permission</b>.</li> <li>b Select a role.</li> <li>c If the role does not apply to access groups, click <b>Finish</b>.</li> <li>d If the role applies to access groups, click <b>Next</b>, select one or more access groups, and click <b>Finish</b>. A role must contain at least one object-specific privilege to apply to an access group.</li> </ol>
<b>Create a permission that includes a specific role</b>	<ol style="list-style-type: none"> <li>a On the <b>Roles</b> tab, select the role, click <b>Permissions</b>, and click <b>Add Permission</b>.</li> <li>b Click <b>Add</b>, select one or more search criteria, and click <b>Find</b> to find administrator users or groups that match your search criteria.</li> <li>c Select an administrator user or group to include in the permission and click <b>OK</b>. You can press the Ctrl and Shift keys to select multiple users and groups.</li> <li>d If the role does not apply to access groups, click <b>Finish</b>.</li> <li>e If the role applies to access groups, click <b>Next</b>, select one or more access groups, and click <b>Finish</b>. A role must contain at least one object-specific privilege to apply to an access group.</li> </ol>
<b>Create a permission that includes a specific access group</b>	<ol style="list-style-type: none"> <li>a On the <b>Access Groups</b> tab, select the access group and click <b>Add Permission</b>.</li> <li>b Click <b>Add</b>, select one or more search criteria, and click <b>Find</b> to find administrator users or groups that match your search criteria.</li> <li>c Select an administrator user or group to include in the permission and click <b>OK</b>. You can press the Ctrl and Shift keys to select multiple users and groups.</li> <li>d Click <b>Next</b>, select a role, and click <b>Finish</b>. A role must contain at least one object-specific privilege to apply to an access group.</li> </ol>

## Delete a Permission

You can delete a permission that includes a specific administrator user or group, a specific role, or a specific access group.

If you remove the last permission for an administrator user or group, that administrator user or group is also removed. Because at least one administrator must have the Administrators role on the root access group, you cannot remove a permission that would cause that administrator to be removed. You cannot delete an inherited permission.

**Procedure**

- 1 In View Administrator, select **View Configuration > Administrators**.
- 2 Select the permission to delete.

Option	Action
<b>Delete a permission that applies to a specific administrator or group</b>	Select the administrator or group on the <b>Administrators and Groups</b> tab.
<b>Delete a permission that applies to a specific role</b>	Select the role on the <b>Roles</b> tab.
<b>Delete a permission that applies to a specific access group</b>	Select the folder on the <b>Access Groups</b> tab.

- 3 Select the permission and click **Delete Permission**.

**Review Permissions**

You can review the permissions that include a specific administrator or group, a specific role, or a specific access group.

**Procedure**

- 1 Select **View Configuration > Administrators**.
- 2 Review the permissions.

Option	Action
<b>Review the permissions that include a specific administrator or group</b>	Select the administrator or group on the <b>Administrators and Groups</b> tab.
<b>Review the permissions that include a specific role</b>	Select the role on the <b>Roles</b> tab and click <b>Permissions</b> .
<b>Review the permissions that include a specific access group</b>	Select the folder on the <b>Access Groups</b> tab.

**Manage and Review Access Groups**

You can use View Administrator to add and delete access groups and to review the desktop pools and machines in a particular access group.

- [Add an Access Group](#) on page 102  
You can delegate the administration of specific machines, desktop pools, or farms to different administrators by creating access groups. By default, desktop pools, application pools, and farms reside in the root access group.
- [Move a Desktop Pool or a Farm to a Different Access Group](#) on page 102  
After you create an access group, you can move automated desktop pools, manual pools, or farms to the new access group.
- [Remove an Access Group](#) on page 102  
You can remove an access group if it does not contain any object. You cannot remove the root access group.
- [Review the Desktop Pools, Application Pools, or Farms in an Access Group](#) on page 103  
You can see the desktop pools, the application pools, or the farms in a particular access group in View Administrator.

- [Review the vCenter Virtual Machines in an Access Group](#) on page 103

You can see the vCenter virtual machines in a particular access group in View Administrator. A vCenter virtual machine inherits the access group from its pool.

## Add an Access Group

You can delegate the administration of specific machines, desktop pools, or farms to different administrators by creating access groups. By default, desktop pools, application pools, and farms reside in the root access group.

You can have a maximum of 100 access groups, including the root access group.

### Procedure

- 1 In View Administrator, navigate to the Add Access Group dialog box.

Option	Action
<b>From Catalog</b>	<ul style="list-style-type: none"> <li>■ Select <b>Catalog &gt; Desktop Pools</b>.</li> <li>■ From the <b>Access Group</b> drop-down menu in the top window pane, select <b>New Access Group</b>.</li> </ul>
<b>From Resources</b>	<ul style="list-style-type: none"> <li>■ Select <b>Resources &gt; Farms</b>.</li> <li>■ From the <b>Access Group</b> drop-down menu in the top window pane, select <b>New Access Group</b>.</li> </ul>
<b>From View Configuration</b>	<ul style="list-style-type: none"> <li>■ Select <b>View Configuration &gt; Administrators</b>.</li> <li>■ From the <b>Access Groups</b> tab, select <b>Add Access Group</b>.</li> </ul>

- 2 Type a name and description for the access group and click **OK**.

The description is optional.

### What to do next

Move one or more objects to the access group.

## Move a Desktop Pool or a Farm to a Different Access Group

After you create an access group, you can move automated desktop pools, manual pools, or farms to the new access group.

### Procedure

- 1 In View Administrator, select **Catalog > Desktop Pools** or **Resources > Farms**.
- 2 Select a pool or a farm.
- 3 Select **Change Access Group** from the **Access Group** drop-down menu in the top window pane.
- 4 Select the access group and click **OK**.

View Administrator moves the pool to the access group that you selected.

## Remove an Access Group

You can remove an access group if it does not contain any object. You cannot remove the root access group.

### Prerequisites

If the access group contains objects, move the objects to another access group or to the root access group. See [“Move a Desktop Pool or a Farm to a Different Access Group,”](#) on page 102.

**Procedure**

- 1 In View Administrator, select **View Configuration > Administrators**.
- 2 On the **Access Groups** tab, select the access group and click **Remove Access Group**.
- 3 Click **OK** to remove the access group.

**Review the Desktop Pools, Application Pools, or Farms in an Access Group**

You can see the desktop pools, the application pools, or the farms in a particular access group in View Administrator.

**Procedure**

- 1 In View Administrator, navigate to the main page for the objects.

Object	Action
<b>Desktop Pools</b>	Select <b>Catalog &gt; Desktop Pools</b> .
<b>Application Pools</b>	Select <b>Catalog &gt; Application Pools</b> .
<b>Farms</b>	Select <b>Resources &gt; Farms</b> .

By default, the objects in all access groups are displayed.

- 2 Select an access group from the **Access Group** drop-down menu in the main window pane.  
The objects in the access group that you selected are displayed.

**Review the vCenter Virtual Machines in an Access Group**

You can see the vCenter virtual machines in a particular access group in View Administrator. A vCenter virtual machine inherits the access group from its pool.

**Procedure**

- 1 In View Administrator, select **Resources > Machines**.
- 2 Select the **vCenter VMs** tab.

By default, the vCenter virtual machines in all access groups are displayed.

- 3 Select an access group from the **Access Group** drop-down menu.  
The vCenter virtual machines in the access group that you selected are displayed.

**Manage Custom Roles**

You can use View Administrator to add, modify, and delete custom roles.

- [Add a Custom Role](#) on page 104

If the predefined administrator roles do not meet your needs, you can combine specific privileges to create your own roles in View Administrator.

- [Modify the Privileges in a Custom Role](#) on page 104

You can modify the privileges in a custom role. You cannot modify the predefined administrator roles.

- [Remove a Custom Role](#) on page 104

You can remove a custom role if it is not included in a permission. You cannot remove the predefined administrator roles.

## Add a Custom Role

If the predefined administrator roles do not meet your needs, you can combine specific privileges to create your own roles in View Administrator.

### Prerequisites

Familiarize yourself with the administrator privileges that you can use to create custom roles. See [“Predefined Roles and Privileges,”](#) on page 105.

### Procedure

- 1 In View Administrator, select **View Configuration > Administrators**.
- 2 On the **Roles** tab, click **Add Role**.
- 3 Type a name and description for the new role, select one or more privileges, and click **OK**.  
The new role appears in the left pane.

## Modify the Privileges in a Custom Role

You can modify the privileges in a custom role. You cannot modify the predefined administrator roles.

### Prerequisites

Familiarize yourself with the administrator privileges that you can use to create custom roles. See [“Predefined Roles and Privileges,”](#) on page 105.

### Procedure

- 1 In View Administrator, select **View Configuration > Administrators**.
- 2 On the **Roles** tab, select the role.
- 3 Click **Privileges** to display the privileges in the role and click **Edit**.
- 4 Select or deselect privileges.
- 5 Click **OK** to save your changes.

## Remove a Custom Role

You can remove a custom role if it is not included in a permission. You cannot remove the predefined administrator roles.

### Prerequisites

If the role is included in a permission, delete the permission. See [“Delete a Permission,”](#) on page 100.

### Procedure

- 1 In View Administrator, select **View Configuration > Administrators**.
- 2 On the **Roles** tab, select the role and click **Remove Role**.  
The **Remove Role** button is not available for predefined roles or for custom roles that are included in a permission.
- 3 Click **OK** to remove the role.

## Predefined Roles and Privileges

View Administrator includes predefined roles that you can assign to your administrator users and groups. You can also create your own administrator roles by combining selected privileges.

- [Predefined Administrator Roles](#) on page 105  
The predefined administrator roles combine all of the individual privileges required to perform common administration tasks. You cannot modify the predefined roles.
- [Global Privileges](#) on page 107  
Global privileges control system-wide operations, such as viewing and changing global settings. Roles that contain only global privileges cannot be applied to access groups.
- [Object-Specific Privileges](#) on page 108  
Object-specific privileges control operations on specific types of inventory objects. Roles that contain object-specific privileges can be applied to access groups.
- [Internal Privileges](#) on page 108  
Some of the predefined administrator roles contain internal privileges. You cannot select internal privileges when you create custom roles.

### Predefined Administrator Roles

The predefined administrator roles combine all of the individual privileges required to perform common administration tasks. You cannot modify the predefined roles.

[Table 6-6](#) describes the predefined roles and indicates whether a role can be applied to an access group.

**Table 6-6.** Predefined Roles in View Administrator

Role	User Capabilities	Applies to an Access Group
Administrators	<p>Perform all administrator operations, including creating additional administrator users and groups. In a Cloud Pod Architecture environment, administrators that have this role can configure and manage a pod federation and manage remote pod sessions.</p> <p>Administrators that have the Administrators role on the root access group are super users because they have full access to all of the inventory objects in the system. Because the Administrators role contains all privileges, you should assign it to a limited set of users. Initially, members of the local Administrators group on your View Connection Server host are given this role on the root access group.</p> <p><b>IMPORTANT</b> An administrator must have the Administrators role on the root access group to perform the following tasks:</p> <ul style="list-style-type: none"> <li>■ Add and delete access groups.</li> <li>■ Manage ThinApp applications and configuration settings in View Administrator.</li> <li>■ Use the <code>vdmin</code>, <code>vdimport</code>, and <code>lmvutil</code> commands.</li> </ul>	Yes
Administrators (Read only)	<ul style="list-style-type: none"> <li>■ View, but not modify, global settings and inventory objects.</li> <li>■ View, but not modify, ThinApp applications and settings.</li> <li>■ Run all PowerShell commands and command line utilities, including <code>vdexport</code> but excluding <code>vdmin</code>, <code>vdimport</code> and <code>lmvutil</code>.</li> </ul> <p>In a Cloud Pod Architecture environment, administrators that have this role can view inventory objects and settings in the Global Data Layer.</p> <p>When administrators have this role on an access group, they can only view the inventory objects in that access group.</p>	Yes
Agent Registration Administrators	Register unmanaged machines such as physical systems, standalone virtual machines, and RDS hosts.	No
Global Configuration and Policy Administrators	View and modify global policies and configuration settings except for administrator roles and permissions, and ThinApp applications and settings.	No
Global Configuration and Policy Administrators (Read only)	View, but not modify, global policies and configuration settings except for administrator roles and permissions, and ThinApp applications and settings.	No
Inventory Administrators	<ul style="list-style-type: none"> <li>■ Perform all machine, session, and pool-related operations.</li> <li>■ Manage persistent disks.</li> <li>■ Resync, Refresh, and Rebalance linked-clone pools and change the default pool image.</li> </ul> <p>When administrators have this role on an access group, they can only perform these operations on the inventory objects in that access group.</p>	Yes
Inventory Administrators (Read only)	<p>View, but not modify, inventory objects.</p> <p>When administrators have this role on an access group, they can only view the inventory objects in that access group.</p>	Yes

**Table 6-6.** Predefined Roles in View Administrator (Continued)

Role	User Capabilities	Applies to an Access Group
Local Administrators	Perform all local administrator operations, except for creating additional administrator users and groups. In a Cloud Pod Architecture environment, administrators that have this role cannot perform operations on the Global Data Layer or manage sessions on remote pods.	Yes
Local Administrators (Read Only)	Same as the Administrators (Read Only) role, except for viewing inventory objects and settings in the Global Data Layer. Administrators that have this role have read-only rights only on the local pod.	Yes

## Global Privileges

Global privileges control system-wide operations, such as viewing and changing global settings. Roles that contain only global privileges cannot be applied to access groups.

[Table 6-7](#) describes the global privileges and lists the predefined roles that contain each privilege.

**Table 6-7.** Global Privileges

Privilege	User Capabilities	Predefined Roles
<b>Console Interaction</b>	Log in to and use View Administrator.	Administrators Administrators (Read only) Inventory Administrators Inventory Administrators (Read only) Global Configuration and Policy Administrators Global Configuration and Policy Administrators (Read only)
<b>Direct Interaction</b>	Run all PowerShell commands and command line utilities, except for <code>vdmin</code> and <code>vdimport</code> . Administrators must have the Administrators role on the root access group to use the <code>vdmin</code> , <code>vdimport</code> , and <code>lmvutil</code> commands.	Administrators Administrators (Read only)
<b>Manage Global Configuration and Policies</b>	View and modify global policies and configuration settings except for administrator roles and permissions.	Administrators Global Configuration and Policy Administrators
<b>Manage Global Sessions</b>	Manage global sessions in a Cloud Pod Architecture environment.	Administrators
<b>Manage Roles and Permissions</b>	Create, modify, and delete administrator roles and permissions.	Administrators
<b>Register Agent</b>	Install Horizon Agent on unmanaged machines, such as physical systems, standalone virtual machines, and RDS hosts. During Horizon Agent installation, you must provide your administrator login credentials to register the unmanaged machine with the View Connection Server instance.	Administrators Agent Registration Administrators

## Object-Specific Privileges

Object-specific privileges control operations on specific types of inventory objects. Roles that contain object-specific privileges can be applied to access groups.

[Table 6-8](#) describes the object-specific privileges. The predefined roles Administrators and Inventory Administrators contain all of these privileges.

**Table 6-8.** Object-Specific Privileges

Privilege	User Capabilities	Object
Enable Farms and Desktop Pools	Enable and disable desktop pools.	Desktop pool, farm
Entitle Desktop and Application Pools	Add and remove user entitlements.	Desktop pool, application pool
Manage Composer Desktop Pool Image	Resync, Refresh, and Rebalance linked-clone pools and change the default pool image.	Desktop pool
Manage Machine	Perform all machine and session-related operations.	Machine
Manage Persistent Disks	Perform all View Composer persistent disk operations, including attaching, detaching, and importing persistent disks.	Persistent disk
Manage Farms and Desktop and Application Pools	Add, modify, and delete farms. Add, modify, delete, and entitle desktop and application pools. Add and remove machines.	Desktop pool, application pool, farm
Manage Sessions	Disconnect and log off sessions and send messages to users.	Session
Manage Reboot Operation	Reset virtual machines or restart virtual desktops.	Machine

## Internal Privileges

Some of the predefined administrator roles contain internal privileges. You cannot select internal privileges when you create custom roles.

[Table 6-9](#) describes the internal privileges and lists the predefined roles that contain each privilege.

**Table 6-9.** Internal Privileges

Privilege	Description	Predefined Roles
Full (Read only)	Grants read-only access to all settings.	Administrators (Read only)
Manage Inventory (Read only)	Grants read-only access to inventory objects.	Inventory Administrators (Read only)
Manage Global Configuration and Policies (Read only)	Grants read-only access to configuration settings and global policies except for administrators and roles.	Global Configuration and Policy Administrators (Read only)

## Required Privileges for Common Tasks

Many common administration tasks require a coordinated set of privileges. Some operations require permission at the root access group in addition to access to the object that is being manipulated.

### Privileges for Managing Pools

An administrator must have certain privileges to manage pools in View Administrator.

[Table 6-10](#) lists common pool management tasks and shows the privileges that are required to perform each task.

**Table 6-10.** Pool Management Tasks and Privileges

Task	Required Privileges
Enable or disable a desktop pool	Enable Farms and Desktop Pools
Entitle or unentitle users to a pool	Entitle Desktop and Application Pools
Add a pool	Manage Farms and Desktop and Application Pools
Modify or delete a pool	Manage Farms and Desktop and Application Pools
Add or remove desktops from a pool	Manage Farms and Desktop and Application Pools
Refresh, Recompose, Rebalance, or change the default View Composer image	Manage Composer Desktop Pool Image
Change access groups	Manage Farms and Desktop and Application Pools on both the source and target access groups.

### Privileges for Managing Machines

An administrator must have certain privileges to manage machines in View Administrator.

[Table 6-11](#) lists common machine management tasks and shows the privileges that are required to perform each task.

**Table 6-11.** Machine Management Tasks and Privileges

Task	Required Privileges
Remove a virtual machine	Manage Machine
Reset a virtual machine	Manage Reboot Operation
Restart a virtual desktop	Manage Reboot Operation
Assign or remove user ownership	Manage Machine
Enter or exit maintenance mode	Manage Machine
Disconnect or log off sessions	Manage Sessions

### Privileges for Managing Persistent Disks

An administrator must have certain privileges to manage persistent disks in View Administrator.

[Table 6-12](#) lists common persistent disk management tasks and shows the privileges that are required to perform each task. You perform these tasks on the Persistent Disks page in View Administrator.

**Table 6-12.** Persistent Disk Management Tasks and Privileges

Task	Required Privileges
Detach a disk	<b>Manage Persistent Disks</b> on the disk and <b>Manage Farms and Desktop and Application Pools</b> on the pool.
Attach a disk	<b>Manage Persistent Disks</b> on the disk and <b>Manage Farms and Desktop and Application Pools</b> on the machine.
Edit a disk	<b>Manage Persistent Disks</b> on the disk and <b>Manage Farms and Desktop and Application Pools</b> on the selected pool.
Change access groups	<b>Manage Persistent Disks</b> on the source and target access groups.
Recreate desktop	<b>Manage Persistent Disks</b> on the disk and <b>Manage Farms and Desktop and Application Pools</b> on the last pool.
Import from vCenter	<b>Manage Persistent Disks</b> on the folder and <b>Manage Pool</b> on the pool.
Delete a disk	<b>Manage Persistent Disks</b> on the disk.

## Privileges for Managing Users and Administrators

An administrator must have certain privileges to manage users and administrators in View Administrator.

[Table 6-13](#) lists common user and administrator management tasks and shows the privileges that are required to perform each task. You manage users on the Users and Groups page in View Administrator. You manage administrators on the Global Administrators View page in View Administrator.

**Table 6-13.** User and Administrator Management Tasks and Privileges

Task	Required Privileges
Update general user information	<b>Manage Global Configuration and Policies</b>
Send messages to users	<b>Manage Remote Sessions</b> on the machine.
Add an administrator user or group	<b>Manage Roles and Permissions</b>
Add, modify, or delete an administrator permission	<b>Manage Roles and Permissions</b>
Add, modify, or delete an administrator role	<b>Manage Roles and Permissions</b>

## Privileges for General Administration Tasks and Commands

An administrator must have certain privileges to perform general administration tasks and run command line utilities.

[Table 6-14](#) shows the privileges that are required to perform general administration tasks and run command line utilities.

**Table 6-14.** Privileges for General Administration Tasks and Commands

Task	Required Privileges
Add or delete an access group	Must have the Administrators role on the root access group.
Manage ThinApp applications and settings in View Administrator	Must have the Administrators role on the root access group.
Install Horizon Agent on an unmanaged machine, such as a physical system, standalone virtual machine, or RDS host	<b>Register Agent</b>
View or modify configuration settings (except for administrators) in View Administrator	<b>Manage Global Configuration and Policies</b>
Run all PowerShell commands and command line utilities except for <code>vdmin</code> and <code>vdimport</code> .	<b>Direct Interaction</b>

**Table 6-14.** Privileges for General Administration Tasks and Commands (Continued)

Task	Required Privileges
Use the <code>vdmadmin</code> and <code>vdmimport</code> commands	Must have the Administrators role on the root access group.
Use the <code>vdmexport</code> command	Must have the Administrators role or the Administrators (Read only) role on the root access group.

## Best Practices for Administrator Users and Groups

To increase the security and manageability of your View environment, you should follow best practices when managing administrator users and groups.

- Create new user groups in Active Directory and assign View administrative roles to these groups. Avoid using Windows built-in groups or other existing groups that might contain users who do not need or should not have View privileges.
- Keep the number of users with View administrative privileges to a minimum.
- Because the Administrators role has every privilege, it should not be used for day-to-day administration.
- Because it is highly visible and easily guessed, avoid using the name Administrator when creating administrator users and groups.
- Create access groups to segregate sensitive desktops and farms. Delegate the administration of those access groups to a limited set of users.
- Create separate administrators that can modify global policies and View configuration settings.



# Configuring Policies in Horizon Administrator and Active Directory

---

# 7

You can use Horizon Administrator to set policies for client sessions. You can configure Active Directory group policy settings to control the behavior of View Connection Server, the PCoIP display protocol, and Horizon 7 logging and performance alarms.

You can also configure Active Directory group policy settings to control the behavior of Horizon Agent, Horizon Client for Windows, Horizon Persona Management, and certain features. For information about these policy settings, see the *Configuring Remote Desktop Features in Horizon 7* document.

This chapter includes the following topics:

- [“Setting Policies in View Administrator,”](#) on page 113
- [“Using Horizon 7 Group Policy Administrative Template Files,”](#) on page 115

## Setting Policies in View Administrator

You use View Administrator to configure policies for client sessions.

You can set these policies to affect specific users, specific desktop pools, or all client sessions users. Policies that affect specific users and desktop pools are called user-level policies and desktop pool-level policies. Policies that affect all sessions and users are called global policies.

User-level policies inherit settings from the equivalent desktop pool-level policy settings. Similarly, desktop pool-level policies inherit settings from the equivalent global policy settings. A desktop pool-level policy setting takes precedence over the equivalent global policy setting. A user-level policy setting takes precedence over the equivalent global and desktop pool-level policy settings.

Lower-level policy settings can be more or less restrictive than the equivalent higher-level settings. For example, you can set a global policy to **Deny** and the equivalent desktop pool-level policy to **Allow**, or vice versa.

---

**NOTE** Only global policies are available for RDS desktop and application pools. You cannot set user-level policies or pool-level policies for RDS desktop and application pools.

---

- [Configure Global Policy Settings](#) on page 114  
You can configure global policies to control the behavior of all client sessions users.
- [Configure Policies for Desktop Pools](#) on page 114  
You can configure desktop-level policies to affect specific desktop pools. Desktop-level policy settings take precedence over their equivalent global policy settings.
- [Configure Policies for Users](#) on page 114  
You can configure user-level policies to affect specific users. User-level policy settings always take precedence over their equivalent global and desktop pool-level policy settings.

- [View Policies](#) on page 115

You can configure View policies to affect all client sessions, or you can apply them to affect specific desktop pools or users.

## Configure Global Policy Settings

You can configure global policies to control the behavior of all client sessions users.

### Prerequisites

Familiarize yourself with the policy descriptions. See [“View Policies,”](#) on page 115.

### Procedure

- 1 In View Administrator, select **Policies > Global Policies**.
- 2 Click **Edit policies** in the **View Policies** pane.
- 3 Click **OK** to save your changes.

## Configure Policies for Desktop Pools

You can configure desktop-level policies to affect specific desktop pools. Desktop-level policy settings take precedence over their equivalent global policy settings.

### Prerequisites

Familiarize yourself with the policy descriptions. See [“View Policies,”](#) on page 115.

### Procedure

- 1 In View Administrator, select **Catalog > Desktop Pools**.
- 2 Double-click the ID of the desktop pool and click the **Policies** tab.  
The **Policies** tab shows the current policy settings. When a setting is inherited from the equivalent global policy, **Inherit** appears in the **Desktop Pool Policy** column.
- 3 Click **Edit Policies** in the **View Policies** pane.
- 4 Click **OK** to save your changes.

## Configure Policies for Users

You can configure user-level policies to affect specific users. User-level policy settings always take precedence over their equivalent global and desktop pool-level policy settings.

### Prerequisites

Familiarize yourself with the policy descriptions. See [“View Policies,”](#) on page 115.

### Procedure

- 1 In View Administrator, select **Catalog > Desktop Pools**.
- 2 Double-click the ID of the desktop pool and click the **Policies** tab.  
The **Policies** tab shows the current policy settings. When a setting is inherited from the equivalent global policy, **Inherit** appears in the **Desktop Pool Policy** column.
- 3 Click **User Overrides** and then click **Add User**.
- 4 To find a user, click **Add**, type the name or description of the user, and then click **Find**.

- 5 Select one or more users from the list, click **OK**, and then click **Next**.

The Add Individual Policy dialog box appears.

- 6 Configure the View policies and click **Finish** to save your changes.

## View Policies

You can configure View policies to affect all client sessions, or you can apply them to affect specific desktop pools or users.

Table 7-1 describes each View policy setting.

**Table 7-1.** View Policies

Policy	Description
Multimedia redirection (MMR)	<p>Determines whether MMR is enabled for client systems.</p> <p>MMR is a Windows Media Foundation filter that forwards multimedia data from specific codecs on remote desktops directly through a TCP socket to the client system. The data is then decoded directly on the client system, where it is played.</p> <p>The default value is <b>Deny</b>.</p> <p>If client systems have insufficient resources to handle local multimedia decoding, leave the setting as <b>Deny</b>.</p> <p>Multimedia Redirection (MMR) data is sent across the network without application-based encryption and might contain sensitive data, depending on the content being redirected. To ensure that this data cannot be monitored on the network, use MMR only on a secure network.</p>
USB Access	<p>Determines whether remote desktops can use USB devices connected to the client system.</p> <p>The default value is <b>Allow</b>. To prevent the use of external devices for security reasons, change the setting to <b>Deny</b>.</p>
PCoIP hardware acceleration	<p>Determines whether to enable hardware acceleration of the PCoIP display protocol and specifies the acceleration priority that is assigned to the PCoIP user session.</p> <p>This setting has an effect only if a PCoIP hardware acceleration device is present on the physical computer that hosts the remote desktop.</p> <p>The default value is <b>Allow</b> at <b>Medium</b> priority.</p>

## Using Horizon 7 Group Policy Administrative Template Files

Horizon 7 provides several component-specific Group Policy Administrative (ADM and ADMX) template files. You can optimize and secure remote desktops and applications by adding the policy settings in these ADM and ADMX template files to a new or existing GPO in Active Directory.

**NOTE** In Horizon 7 version 7.1, the ADM template files are deprecated and the ADMX template files are added.

All ADMX files that provide group policy settings for Horizon 7 are available in a bundled .zip file named `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip`, where `x.x.x` is the version and `yyyyyy` is the build number. You can download the file from the VMware download site at <https://my.vmware.com/web/vmware/downloads>. Under Desktop & End-User Computing, select the VMware Horizon 7 download, which includes the bundled .zip file.

The Horizon 7 ADM and ADMX template files contain both Computer Configuration and User Configuration group policies.

- The Computer Configuration policies set policies that apply to all remote desktops, regardless of who connects to the desktop.

- The User Configuration policies set policies that apply to all users, regardless of the remote desktop or application they connect to. User Configuration policies override equivalent Computer Configuration policies.

Microsoft Windows applies policies at desktop startup and when users log in.

## Horizon 7 ADMX and ADM Template Files

The Horizon 7 ADMX and ADM template files provide group policy settings that let you control and optimize Horizon 7 components.

**Note** In Horizon 7 version 7.1, the ADM template files are deprecated and the ADMX template files are added.

**Table 7-2.** Horizon ADMX and ADM Template Files

Template Name	Template File	Description
Horizon Agent Configuration	vdm_agent.admx vdm_agent.adm	Contains policy settings related to the authentication and environmental components of Horizon Agent. <i>See the <a href="#">Configuring Remote Desktop Features in Horizon 7</a> document.</i>
Horizon Client Configuration	vdm_client.admx vdm_client.adm	Contains policy settings related to Horizon Client for Windows. Clients that connect from outside the Connection Server host domain are not affected by policies applied to Horizon Client. <i>See the <a href="#">Using VMware Horizon Client for Windows</a> document.</i>
VMware Horizon URL Redirection	urlRedirection-enUS.admx urlRedirection-enUS.adm	Contains policy settings related to the URL Content Redirection Feature. If you add this template to a GPO for a remote desktop pool or application pool, certain URL links clicked inside the remote desktops or app can be redirected to a Windows-based client and opened in a client-side browser. If you add this template to a client-side GPO, when a user clicks certain URL links in a Windows-based client system, the URL can be opened in a remote desktop or application. <i>See the <a href="#">Configuring Remote Desktop Features in Horizon 7</a> document and see the <a href="#">Using VMware Horizon Client for Windows</a> document.</i>
Connection Server Configuration	vdm_server.admx vdm_server.adm	Contains policy settings related to Connection Server. <i>See <a href="#">“Horizon Connection Server Configuration ADMX or ADM Template Settings,”</a> on page 117.</i>
View Common Configuration	vdm_common.admx vdm_common.adm	Contains policy settings that are common to all Horizon components. <i>See <a href="#">“Horizon 7 Common Configuration ADMX and ADM Template Settings,”</a> on page 118.</i>
PCoIP Session Variables	pcoip.admx pcoip.adm	Contains policy settings related to the PCoIP display protocol. <i>See the <a href="#">Configuring Remote Desktop Features in Horizon 7</a> document.</i>

**Table 7-2.** Horizon ADMX and ADM Template Files (Continued)

Template Name	Template File	Description
PCoIP Client Session Variables	pcoip.client.admx pcoip.client.adm	Contains policy settings related to the PCoIP display protocol that affect Horizon Client for Windows. <i>See the Using VMware Horizon Client for Windows document.</i>
Horizon Persona Management Configuration	ViewPM.admx ViewPM.adm	Contains policy settings related to Horizon Persona Management. <i>See the Setting Up Virtual Desktops in Horizon 7 document.</i>
Remote Desktop Services	vmware_rdsh.admx vmware_rdsh.adm	Contains policy settings related to Remote Desktop Services. <i>See the Configuring Remote Desktop Features in Horizon 7 document.</i>
Real-Time Audio-Video Configuration	vdm_agent_rtav.admx vdm_agent_rtav.adm	Contains policy settings related to webcams that are used with the Real-Time Audio-Video feature. <i>See the Configuring Remote Desktop Features in Horizon 7 document.</i>
Scanner Redirection	vdm_agent_scanner.admx vdm_agent_scanner.adm	Contains policy settings related to scanning devices that are redirected for use in published desktops and applications. <i>See the Configuring Remote Desktop Features in Horizon 7 document.</i>
Serial Port Redirection	vdm_agent_serialport.admx vdm_agent_serialport.adm	Contains policy settings related to serial (COM) ports that are redirected for use in virtual desktops. <i>See the Configuring Remote Desktop Features in Horizon 7 document.</i>

## Horizon Connection Server Configuration ADMX or ADM Template Settings

The View Server Configuration ADMX (`vdm_server.admx`) or ADM (`vdm_server.adm`) template files contain policy settings related to all Horizon Connection Servers.

[Table 7-3](#) describes each policy setting in the Connection Server configuration ADMX or ADM template file. The template contains only Computer Configuration settings. All of the settings are in the **Computer Configuration > Policies > Administrative Templates > VMware View Server Configuration** folder in the Group Policy Management Editor.

**NOTE** In Horizon 7 version 7.1, the ADM template files are deprecated and the ADMX template files are added.

**Table 7-3.** Horizon Server Configuration Template Settings

Setting	Properties
Enumerate Forest Trust Child Domains	<p>Determines if every domain trusted by the domain in which the server resides is enumerated. In order to establish a complete chain of trust, the domains trusted by each trusted domain are also enumerated and the process continues recursively until all trusted domains are discovered. This information is passed to Connection Server in order to ensure that all trusted domains are available to the client on login.</p> <p>This property is enabled by default. When disabled, only directly trusted domains are enumerated and connection to remote domain controllers does not take place.</p> <p><b>NOTE</b> In environments with complex domain relationships, such as those that use multiple forest structures with trust between domains in their forests, the process can take a few minutes to complete.</p>
Recursive Enumeration of Trusted Domains	<p>Determines whether every domain trusted by the domain in which the server resides is enumerated. To establish a complete chain of trust, the domains trusted by each trusted domain are also enumerated and the process continues recursively until all trusted domains are discovered. This information is passed to View Connection Server so that all trusted domains are available to the client on login.</p> <p>This setting is enabled by default. When it is disabled, only directly trusted domains are enumerated and connection to remote domain controllers does not take place.</p> <p>In environments with complex domain relationships, such as those that use multiple forest structures with trust between domains in their forests, this process can take a few minutes to complete.</p>
Windows Password Authentication Mode	<p>Select the windows password authentication mode.</p> <ul style="list-style-type: none"> <li>■ KerberosOnly. Authenticate using Kerberos.</li> <li>■ KerberosWithFallbackToNTLM. Authenticate using Kerberos, but fallback to using NTLM on failure.</li> <li>■ Legacy. Authenticate using NTLM, but fallback to using Kerberos on failure. Used to support legacy NT domain controllers.</li> </ul> <p>Default is KerberosOnly.</p>

## Horizon 7 Common Configuration ADMX and ADM Template Settings

The Horizon 7 Common Configuration ADMX (`vdm_common.admx`) and ADM (`vdm_common.adm`) template files contain policy settings common to all Horizon components. These templates contain only Computer Configuration settings. In Horizon 7 version 7.1, the ADM template files are deprecated and the ADMX template files are added.

### Log Configuration Settings

[Table 7-4](#) describes the log configuration policy setting in the Horizon Common Configuration ADMX and ADM template files. All of the settings are in the **Computer Configuration > Policies > Administrative Templates > VMware View Common Configuration > Log Configuration** folder in the Group Policy Management Editor.

**Table 7-4.** View Common Configuration Template: Log Configuration Settings

Setting	Properties
Number of days to keep production logs	Specifies the number of days for which log files are retained on the system. If no value is set, the default applies and log files are kept for seven days.
Maximum number of debug logs	Specifies the maximum number of debug log files to retain on the system. When a log file reaches its maximum size, no further entries are added and a new log file is created. When the number of previous log files reaches this value, the oldest log file is deleted.

**Table 7-4.** View Common Configuration Template: Log Configuration Settings (Continued)

Setting	Properties
Maximum debug log size in Megabytes	Specifies the maximum size in megabytes that a debug log can reach before the log file is closed and a new log file is created.
Log Directory	Specifies the full path to the directory for log files. If the location is not writeable, the default location is used. For client log files, an extra directory with the client name is created.
Send logs to a Syslog server	<p>Allows View server logs to be sent to a Syslog server such as VMware vCenter Log Insight. Logs are sent from all View servers in the OU or domain in which this GPO is configured.</p> <p>You can send Horizon Agent logs to a Syslog server by enabling this setting in a GPO that is linked to an OU that contains your desktops.</p> <p>To send log data to a Syslog server, enable this setting and specify the log level and the server's fully qualified domain name (FQDN) or IP address. You can specify an alternate port if you do not want to use default port 514. Separate each element in your specification with a vertical bar ( ). Use the following syntax:</p> <p>Log Level Server FQDN or IP [ Port number(514 default)]</p> <p>For example: Debug 192.0.2.2</p> <p><b>IMPORTANT</b> Syslog data is sent across the network without software-based encryption. Because View server logs might contain sensitive data, avoid sending Syslog data on an insecure network. If possible, use link-layer security such as IPsec to prevent the possibility of this data being monitored on the network.</p>

## Performance Alarm Settings

Table 7-5 describe the performance alarm settings in the Horizon Common Configuration ADMX and ADM template files. All of the settings are in the **Computer Configuration > Policies > Administrative Templates > VMware View Common Configuration > Performance Alarms** folder in the Group Policy Management Editor.

**Table 7-5.** View Common Configuration Template: Performance Alarm Settings

Setting	Properties
CPU and Memory Sampling Interval in Seconds	Specifies the CPU and memory polling interval CPU. A low sampling interval can result in an high level of output to the log.
Overall CPU usage percentage to issue log info	Specifies the threshold at which the overall CPU use of the system is logged. When multiple processors are available, this percentage represents the combined usage.
Overall memory usage percentage to issue log info	Specifies the threshold at which the overall committed system memory use is logged. Committed system memory is memory that has been allocated by processes and to which the operating system has committed physical memory or a page slot in the pagefile.
Process CPU usage percentage to issue log info	Specifies the threshold at which the CPU usage of any individual process is logged.

**Table 7-5.** View Common Configuration Template: Performance Alarm Settings (Continued)

Setting	Properties
Process memory usage percentage to issue log info	Specifies the threshold at which the memory usage of any individual process is logged.
Process to check, comma separated name list allowing wild cards and exclusion	<p>Specifies a comma-separated list of queries that correspond to the name of one or more processes to be examined. You can filter the list by using wildcards within each query.</p> <ul style="list-style-type: none"> <li>■ An asterisk (*) matches zero or more characters.</li> <li>■ A question mark (?) matches exactly one character.</li> <li>■ An exclamation mark (!) at the beginning of a query excludes any results produced by that query.</li> </ul> <p>For example, the following query selects all processes starting with <b>ws</b> and excludes all processes ending with <b>sys</b>:</p> <p><code>'!*sys,ws*'</code></p>

**NOTE** Performance alarm settings apply to Horizon Connection Server and Horizon Agent systems only. They do not apply to Horizon Client systems.

## Security Settings

[Table 7-6](#) describe the security settings in the Horizon Common Configuration ADMX and ADM template files. All of the settings are in the **Computer Configuration > Policies > Administrative Templates > VMware View Common Configuration > Security Settings** folder in the Group Policy Management Editor.

**Table 7-6.** View Common Configuration Template: Security Settings

Setting	Properties
Only use cached revocation URLs	<p>Certificate revocation checking will only access cached URLs.</p> <p>Default if not configured is false.</p>
Revocation URL check timeout milliseconds	<p>The cumulative timeout across all revocation URL wire retrievals in milliseconds.</p> <p>Not configured or value set to 0 means that Microsoft default handling is used.</p>
Type of certificate revocation check	<p>Select the type of certificate revocation check to be done:</p> <ul style="list-style-type: none"> <li>■ None</li> <li>■ EndCertificateOnly</li> <li>■ WholeChain</li> <li>■ WholeChain</li> </ul> <p>Default is WholeChainButRoot.</p>

## General Settings

[Table 7-7](#) describes the general settings in the Horizon Common Configuration ADMX and ADM template files. All of the settings are in the **Computer Configuration > Policies > Administrative Templates > VMware View Common Configuration** folder in the Group Policy Management Editor.

**Table 7-7.** View Common Configuration Template: General Settings

Setting	Properties
Disk threshold for log and events in Megabytes	Specifies the minimum remaining disk space threshold for logs and events. If no value is specified, the default is 200. When the specified value is met, event logging stops.
Enable extended logging	Determines whether trace and debug events are included in the log files.
Override the default View Windows event generation	<p>The following values are supported:</p> <ul style="list-style-type: none"> <li>■ 0 = Event log entries are only produced for view events (no event log entries are generated for log messages)</li> <li>■ 1 = Event log entries are produced in 4.5 (and earlier) compatibility mode. Event log entries are not produced for standard view events. Event log entries are based solely on log file text.</li> <li>■ 2 = Event log entries are produced in 4.5 (and earlier) compatibility mode with view events also being included.</li> </ul>



# Maintaining View Components

---

To keep your View components available and running, you can perform a variety of maintenance tasks.

This chapter includes the following topics:

- [“Backing Up and Restoring View Configuration Data,”](#) on page 123
- [“Monitor View Components,”](#) on page 131
- [“Monitor Machine Status,”](#) on page 131
- [“Understanding View Services,”](#) on page 132
- [“Change the Product License Key,”](#) on page 134
- [“Monitoring Product License Usage,”](#) on page 134
- [“Update General User Information from Active Directory,”](#) on page 135
- [“Migrate View Composer to Another Machine,”](#) on page 136
- [“Update the Certificates on a View Connection Server Instance, Security Server, or View Composer,”](#) on page 141
- [“Information Collected by the Customer Experience Improvement Program,”](#) on page 142

## Backing Up and Restoring View Configuration Data

You can back up your View and View Composer configuration data by scheduling or running automatic backups in View Administrator. You can restore your View configuration by manually importing the backed-up View LDAP files and View Composer database files.

You can use the backup and restore features to preserve and migrate View configuration data.

### Backing Up View Connection Server and View Composer Data

After you complete the initial configuration of View Connection Server, you should schedule regular backups of your View and View Composer configuration data. You can preserve your View and View Composer data by using View Administrator.

View stores View Connection Server configuration data in the View LDAP repository. View Composer stores configuration data for linked-clone desktops in the View Composer database.

When you use View Administrator to perform backups, View backs up the View LDAP configuration data and View Composer database. Both sets of backup files are stored in the same location. The View LDAP data is exported in encrypted LDAP data interchange format (LDIF). For a description of View LDAP, see [“View LDAP Directory,”](#) on page 40.

You can perform backups in several ways.

- Schedule automatic backups by using the View configuration backup feature.
- Initiate a backup immediately by using the **Backup Now** feature in View Administrator.
- Manually export View LDAP data by using the `vdmexport` utility. This utility is provided with each instance of View Connection Server.

The `vdmexport` utility can export View LDAP data as encrypted LDIF data, plain text, or plain text with passwords and other sensitive data removed.

---

**NOTE** The `vdmexport` tool backs up the View LDAP data only. This tool does not back up View Composer database information.

---

For more information about `vdmexport`, see [“Export Configuration Data from View Connection Server,”](#) on page 125.

The following guidelines apply to backing up View configuration data:

- View can export configuration data from any View Connection Server instance.
- If you have multiple View Connection Server instances in a replicated group, you only need to export the data from one instance. All replicated instances contain the same configuration data.
- Do not rely on using replicated instances of View Connection Server to act as your backup mechanism. When View synchronizes data in replicated instances of View Connection Server, any data lost in one instance might be lost in all members of the group.
- If View Connection Server uses multiple vCenter Server instances with multiple View Composer services, View backs up all the View Composer databases associated with the vCenter Server instances.

## Schedule View Configuration Backups

You can schedule your View configuration data to be backed up at regular intervals. View backs up the contents of the View LDAP repository in which your View Connection Server instances store their configuration data.

You can back up the configuration immediately by selecting the View Connection Server instance and clicking **Backup Now**.

### Prerequisites

Familiarize yourself with the backup settings. See [“View Configuration Backup Settings,”](#) on page 125.

### Procedure

- 1 In View Administrator, select **View Configuration > Servers**.
- 2 On the **Connection Servers** tab, select the View Connection Server instance to be backed up and click **Edit**.
- 3 On the **Backup** tab, specify the View configuration backup settings to configure the backup frequency, maximum number of backups, and the folder location of the backup files.
- 4 (Optional) Change the data recovery password.
  - a Click **Change data recovery password**.
  - b Type and retype the new password.
  - c (Optional) Type a password reminder.
  - d Click **OK**.
- 5 Click **OK**.

## View Configuration Backup Settings

View can back up your View Connection Server and View Composer configuration data at regular intervals. In View Administrator, you can set the frequency and other aspects of the backup operations.

**Table 8-1.** View Configuration Backup Settings

Setting	Description
Automatic backup frequency	<p>Every Hour. Backups take place every hour on the hour.</p> <p>Every 6 Hours. Backups take place at midnight, 6 am, noon, and 6 pm.</p> <p>Every 12 Hours. Backups take place at midnight and noon.</p> <p>Every Day. Backups take place every day at midnight.</p> <p>Every 2 Days. Backups occur at midnight on Saturday, Monday, Wednesday, and Friday.</p> <p>Every Week. Backups take place weekly at midnight on Saturday.</p> <p>Every 2 Weeks. Backups take place every other week at midnight on Saturday.</p> <p>Never. Backups do not take place automatically.</p>
Max number of backups	<p>Number of backup files that can be stored on the View Connection Server instance. The number must be an integer greater than 0.</p> <p>When the maximum number is reached, View deletes the oldest backup file.</p> <p>This setting also applies to backup files that are created when you use <b>Backup Now</b>.</p>
Folder location	<p>Default location of the backup files on the computer where View Connection Server is running: C:\Programdata\VMware\VDM\backups</p> <p>When you use <b>Backup Now</b>, View also stores the backup files in this location.</p>

## Export Configuration Data from View Connection Server

You can back up configuration data of a View Connection Server instance by exporting the contents of its View LDAP repository.

You use the `vdmexport` command to export the View LDAP configuration data to an encrypted LDIF file. You can also use the `vdmexport -v` (verbatim) option to export the data to a plain text LDIF file, or the `vdmexport -c` (cleansed) option to export the data as plain text with passwords and other sensitive data removed.

You can run the `vdmexport` command on any View Connection Server instance. If you have multiple View Connection Server instances in a replicated group, you only need to export the data from one instance. All replicated instances contain the same configuration data.

**NOTE** The `vdmexport.exe` command backs up the View LDAP data only. This command does not back up View Composer database information.

### Prerequisites

- Locate the `vdmexport.exe` command executable file installed with View Connection Server in the default path.  
C:\Program Files\VMware\VMware View\Server\tools\bin
- Log in to a View Connection Server instance as a user in the Administrators or Administrators (Read only) role.

### Procedure

- 1 Select **Start > Command Prompt**.
- 2 At the command prompt, type the `vdmexport` command and redirect the output to a file. For example:  
`vdmexport > Myexport.LDF`  
By default, the exported data is encrypted.

You can specify the output file name as an argument to the `-f` option. For example:

```
vdmexport -f Myexport.LDF
```

You can export the data in plain text format (verbatim) by using the `-v` option. For example:

```
vdmexport -f Myexport.LDF -v
```

You can export the data in plain text format with passwords and sensitive data removed (cleansed) by using the `-c` option. For example:

```
vdmexport -f Myexport.LDF -c
```

---

**NOTE** Do not plan on using cleansed backup data to restore a View LDAP configuration. The cleansed configuration data is missing passwords and other critical information.

---

For more information about the `vdmexport` command, see the *View Integration* document.

### What to do next

You can restore or transfer the configuration information of View Connection Server by using the `vdmimport` command.

For details about importing the LDIF file, see [“Restoring View Connection Server and View Composer Configuration Data,”](#) on page 126.

## Restoring View Connection Server and View Composer Configuration Data

You can manually restore the View Connection Server LDAP configuration files and View Composer database files that were backed up by View.

You manually run separate utilities to restore View Connection Server and View Composer configuration data.

Before you restore configuration data, verify that you backed up the configuration data in View Administrator. See [“Backing Up View Connection Server and View Composer Data,”](#) on page 123.

You use the `vdmimport` utility to import the View Connection Server data from the LDIF backup files to the View LDAP repository in the View Connection Server instance.

You can use the `SviConfig` utility to import the View Composer data from the `.svi` backup files to the View Composer SQL database.

---

**NOTE** In certain situations, you might have to install the current version of a View Connection Server instance and restore the existing View configuration by importing the View Connection Server LDAP configuration files. You might require this procedure as part of a business continuity and disaster recovery (BC/DR) plan, as a step in setting up a second datacenter with the existing View configuration, or for other reasons. For more information, see "Reinstall View Connection Server with a Backup Configuration" in the *View Installation* document.

---

### Import Configuration Data into View Connection Server

You can restore configuration data of a View Connection Server instance by importing a backup copy of the data stored in an LDIF file.

You use the `vdmimport` command to import the data from the LDIF file to the View LDAP repository in the View Connection Server instance.

If you backed up your View LDAP configuration by using View Administrator or the default `vdmexport` command, the exported LDIF file is encrypted. You must decrypt the LDIF file before you can import it.

If the exported LDIF file is in plain text format, you do not have to decrypt the file.

---

**Note** Do not import an LDIF file in cleansed format, which is plain text with passwords and other sensitive data removed. If you do, critical configuration information will be missing from the restored View LDAP repository.

---

For information about backing up the View LDAP repository, see [“Backing Up View Connection Server and View Composer Data,”](#) on page 123.

### Prerequisites

- Locate the `vdmimport` command executable file installed with View Connection Server in the default path.  
`C:\Program Files\VMware\VMware View\Server\tools\bin`
- Log in to a View Connection Server instance as a user with the Administrators role.
- Verify that you know the data recovery password. If a password reminder was configured, you can display the reminder by running the `vdmimport` command without the password option.

### Procedure

- 1 Stop all instances of View Composer by stopping the Windows service VMware Horizon View Composer on the servers where View Composer runs.
- 2 Stop all security server instances by stopping the Windows service VMware Horizon Security Server on all security servers.
- 3 Uninstall all instances of View Connection Server.  
 Uninstall both VMware Horizon View Connection Server and AD LDS Instance VMwareVDMDS.
- 4 Install one instance of View Connection Server.
- 5 Stop the View Connection Server instance by stopping the Windows service VMware Horizon Connection Server.
- 6 Click **Start > Command Prompt**.
- 7 Decrypt the encrypted LDIF file.

At the command prompt, type the `vdmimport` command. Specify the `-d` option, the `-p` option with the data recovery password, and the `-f` option with an existing encrypted LDIF file followed by a name for the decrypted LDIF file. For example:

```
vdmimport -d -p mypassword
-f MyEncryptedexport.LDF > MyDecryptedexport.LDF
```

If you do not remember your data recovery password, type the command without the `-p` option. The utility displays the password reminder and prompts you to enter the password.

- 8 Import the decrypted LDIF file to restore the View LDAP configuration.  
 Specify the `-f` option with the decrypted LDIF file. For example:  

```
vdmimport -f MyDecryptedexport.LDF
```
- 9 Uninstall View Connection Server.  
 Uninstall only the package VMware Horizon View Connection Server.
- 10 Reinstall View Connection Server.
- 11 Log in to View Administrator and validate that the configuration is correct.
- 12 Start the View Composer instances.

- 13 Reinstall the replica server instances.
- 14 Start the security server instances.

If there is a risk that the security servers have inconsistent configuration, they should also be uninstalled rather than stopped and then reinstalled at the end of the process.

The `vdmimport` command updates the View LDAP repository in View Connection Server with the configuration data from the LDIF file. For more information about the `vdmimport` command, see the *View Integration* document.

---

**NOTE** Make sure that the configuration that is being restored matches the virtual machines that are known to vCenter Server, and to View Composer if it is in use. If necessary, restore the View Composer configuration from backup. See [“Restore a View Composer Database,”](#) on page 128. After you restore the View Composer configuration, you may need to manually resolve inconsistencies if the virtual machines in vCenter Server have changed since the backup of the View Composer configuration.

---

## Restore a View Composer Database

You can import the backup files for your View Composer configuration into the View Composer database that stores linked-clone information.

You can use the `SviConfig restoredata` command to restore View Composer database data after a system failure or to revert your View Composer configuration to an earlier state.

---

**IMPORTANT** Only experienced View Composer administrators should use the `SviConfig` utility. This utility is intended to resolve issues relating to the View Composer service.

---

### Prerequisites

Verify the location of the View Composer database backup files. By default, View stores the backup files on the C: drive of the View Connection Server computer, at `C:\Programdata\VMware\VDM\backups`.

View Composer backup files use a naming convention with a date stamp and an `.svi` suffix.

Backup-YearMonthDayCount-vCenter Server Name\_Domain Name.svi

For example: Backup-20090304000010-foobar\_test\_org.svi

Familiarize yourself with the `SviConfig restoredata` parameters:

- `DsnName` - The DSN that is used to connect to the database. The `DsnName` parameter is mandatory and cannot be an empty string.
- `Username` - The user name that is used to connect to the database. If this parameter is not specified, Windows authentication is used.
- `Password` - The password for the user that connects to the database. If this parameter is not specified and Windows authentication is not used, you are prompted to enter the password later.
- `BackupFilePath` - The path to the View Composer backup file.

The `DsnName` and `BackupFilePath` parameters are required and cannot be empty strings. The `Username` and `Password` parameters are optional.

### Procedure

- 1 Copy the View Composer backup files from the View Connection Server computer to a location that is accessible from the computer where the VMware Horizon View Composer service is installed.
- 2 On the computer where View Composer is installed, stop the VMware Horizon View Composer service.

- 3 Open a Windows command prompt and navigate to the SviConfig executable file.

The file is located with the View Composer application. The default path is C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe.

- 4 Run the SviConfig `restoredata` command.

```
sviconfig -operation=restoredata
          -DsnName=target_database_source_name_(DSN)
          -Username=database_administrator_username
          -Password=database_administrator_password
          -BackupFilePath=path_to_View_Composer_backup_file
```

For example:

```
sviconfig -operation=restoredata -dsname=LinkedClone
          -username=Admin -password=Pass
          -backupfilepath="C:\Program Files (x86)\VMware\VMware View
Composer\Backup-20090304000010-foobar_test_org.SVI"
```

- 5 Start the VMware Horizon View Composer service.

### What to do next

For output result codes for the SviConfig `restoredata` command, see [“Result Codes for Restoring the View Composer Database,”](#) on page 129.

## Result Codes for Restoring the View Composer Database

When you restore a View Composer database, the SviConfig `restoredata` command displays a result code.

**Table 8-2.** Restoredata Result Codes

Code	Description
0	The operation ended successfully.
1	The supplied DSN could not be found.
2	Invalid database administrator credentials were provided.
3	The driver for the database is not supported.
4	An unexpected problem occurred and the command failed to complete.
14	Another application is using the VMware Horizon View Composer service. Shut down the service before executing the command.
15	A problem occurred during the restore process. Details are provided in the onscreen log output.

## Export Data in View Composer Database

You can export data from your View Composer database to file.

---

**IMPORTANT** Use the SviConfig utility only if you are an experienced View Composer administrator.

---

### Prerequisites

By default, View stores the backup files on the C: drive of the View Connection Server computer, at C:\Programdata\VMWare\VDM\backups.

Familiarize yourself with the SviConfig `exportdata` parameters:

- **DsnName** - The DSN that is used to connect to the database. If it is not specified, DSN name, user name and password will be retrieved from server configuration file.

- Username - The user name that is used to connect to the database. If this parameter is not specified, Windows authentication is used.
- Password - The password for the user that connects to the database. If this parameter is not specified and Windows authentication is not used, you are prompted to enter the password later.
- OutputFilePath - The path to the output file.

### Procedure

- 1 On the computer where View Composer is installed, stop the VMware Horizon View Composer service.
- 2 Open a Windows command prompt and navigate to the SviConfig executable file.

The file is located with the View Composer application.

*View-Composer-installation-directory\sviconfig.exe*

- 3 Run the SviConfig exportdata command.

```
sviconfig -operation=exportdata
          -DsnName=target_database_source_name_(DSN)
          -Username=database_administrator_username
          -Password=database_administrator_password
          -OutputFilePath=path_to_View_Composer_output_file
```

For example:

```
sviconfig -operation=exportdata -dsnname=LinkedClone
          -username=Admin -password=Pass
          -outputfilepath="C:\Program Files\VMware\VMware View
Composer\Export-20090304000010-foobar_test_org.SVI"
```

### What to do next

For export result codes for the SviConfig exportdata command, see [“Result Codes for Exporting the View Composer Database,”](#) on page 130.

## Result Codes for Exporting the View Composer Database

When you export a View Composer database, the SviConfig exportdata command displays an exit code.

**Table 8-3.** Exportdata ExitStatus Codes

Code	Description
0	Exporting data ended successfully.
1	The supplied DSN name can not be found.
2	The supplied credentials are invalid.
3	Unsupported driver for the provided database.
4	An unexpected problem has occurred.
18	Unable to connect to the database server.
24	Unable to open the output file.

## Monitor View Components

You can quickly survey the status of the View and vSphere components in your View deployment by using the View Administrator dashboard.

View Administrator displays monitoring information about View Connection Server instances, the event database, security servers, View Composer services, datastores, vCenter Server instances, and domains.

---

**Note** View cannot determine status information about Kerberos domains. View Administrator displays Kerberos domain status as unknown, even when a domain is configured and working.

---

### Procedure

- 1 In View Administrator, click **Dashboard**.
- 2 In the System Health pane, expand **View components**, **vSphere components**, or **Other components**.
  - A green up arrow indicates that a component has no problems.
  - A red down arrow indicates that a component is unavailable or not functioning.
  - A yellow double arrow indicates that a component is in a warning state.
  - A question mark indicates that the status of a component is unknown.
- 3 Click a component name.  
A dialog displays the name, version, status, and other component information.

### What to do next

Use vCenter Server to monitor any Virtual SAN clusters and the disks that participate in a Virtual SAN datastore. For more information about monitoring Virtual SAN in vSphere 5.5 Update 1, see the *vSphere Storage* document and the *vSphere Monitoring and Performance* documentation. For more information about monitoring Virtual SAN in vSphere 6 or later, see the *Administering VMware Virtual SAN* document.

## Monitor Machine Status

You can quickly survey the status of machines in your View deployment by using the View Administrator dashboard. For example, you can display all disconnected machines or machines that are in maintenance mode.

### Prerequisites

Familiarize yourself with the virtual machine status values. See [“Status of vCenter Server Virtual Machines,”](#) on page 185.

### Procedure

- 1 In View Administrator, click **Dashboard**.
- 2 In the Machine Status pane, expand a status folder.

Option	Description
<b>Preparing</b>	Lists the states while the machine is being provisioned, deleted, or in maintenance mode.
<b>Problem Machines</b>	Lists the error states.
<b>Prepared for use</b>	Lists the states when the machine is ready for use.

- 3 Locate the machine status and click the hyperlinked number next to it.

The **Machines** page displays all machines with the selected status.

### What to do next

You can click a machine name to see details about the machine or click the View Administrator back arrow to return to the Dashboard page.

## Understanding View Services

The operation of View Connection Server instances and security servers depends on several services that run on the system. These systems are started and stopped automatically, but you might sometimes find it necessary to adjust the operation of these services manually.

You use the Microsoft Windows Services tool to stop or start View services. If you stop View services on a View Connection Server host or a security server, end users cannot connect to their remote desktops or applications until you restart the services. You might also need to restart a service if it has stopped running or if the View functionality that it controls appears to be unresponsive.

## Stop and Start View Services

The operation of View Connection Server instances and security servers depends on several services that run on the system. You might sometimes find it necessary to stop and start these services manually when troubleshooting problems with the operation of View.

When you stop View services, end users cannot connect to their remote desktops and applications. You should perform such an action at a time that is already scheduled for system maintenance, or warn end users that their desktops and applications will be unavailable temporarily.

---

**NOTE** Stop only the VMware Horizon View Connection Server service on a View Connection Server host, or the VMware Horizon View Security Server service on a security server. Do not stop any other component services.

---

### Prerequisites

Familiarize yourself with the services that run on View Connection Server hosts and security servers as described in [“Services on a View Connection Server Host,”](#) on page 133 and [“Services on a Security Server,”](#) on page 133.

### Procedure

- 1 Start the Windows Services tool by entering **services.msc** at the command prompt.
- 2 Select the VMware Horizon View Connection Server service on a View Connection Server host, or the VMware Horizon View Security Server service on a security server, and click **Stop**, **Restart**, or **Start** as appropriate.
- 3 Verify that the status of the listed service changes as expected.

## Services on a View Connection Server Host

The operation of View depends on several services that run on a View Connection Server host.

**Table 8-4.** View Connection Server Host Services

Service Name	Startup Type	Description
VMware Horizon View Blast Secure Gateway	Automatic	Provides secure HTML Access and Blast Extreme services. This service must be running if clients connect to View Connection Server through the Blast Secure Gateway.
VMware Horizon View Connection Server	Automatic	Provides connection broker services. This service must always be running. If you start or stop this service, it also starts or stops the Framework, Message Bus, Security Gateway, and Web services. This service does not start or stop the VMwareVDMDS service or the VMware Horizon View Script Host service.
VMware Horizon View Framework Component	Manual	Provides event logging, security, and COM+ framework services. This service must always be running.
VMware Horizon View Message Bus Component	Manual	Provides messaging services between the View components. This service must always be running.
VMware Horizon View PCoIP Secure Gateway	Manual	Provides PCoIP Secure Gateway services. This service must be running if clients connect to View Connection Server through the PCoIP Secure Gateway.
VMware Horizon View Script Host	Disabled	Provides support for third-party scripts that run when you delete virtual machines. This service is disabled by default. You should enable this service if you want to run scripts.
VMware Horizon View Security Gateway Component	Manual	Provides common gateway services. This service must always be running.
VMware Horizon View Web Component	Manual	Provides web services. This service must always be running.
VMwareVDMDS	Automatic	Provides LDAP directory services. This service must always be running. During upgrades of View, this service ensures that existing data is migrated correctly.

## Services on a Security Server

The operation of View depends on several services that run on a security server.

**Table 8-5.** Security Server Services

Service Name	Startup Type	Description
VMware Horizon View Blast Secure Gateway	Automatic	Provides secure HTML Access and Blast Extreme services. This service must be running if clients connect to this security server through the Blast Secure Gateway.
VMware Horizon View Security Server	Automatic	Provides security server services. This service must always be running. If you start or stop this service, it also starts or stops the Framework and Security Gateway services.
VMware Horizon View Framework Component	Manual	Provides event logging, security, and COM+ framework services. This service must always be running.

**Table 8-5.** Security Server Services (Continued)

Service Name	Startup Type	Description
VMware Horizon View PCoIP Secure Gateway	Manual	Provides PCoIP Secure Gateway services. This service must be running if clients connect to this security server through the PCoIP Secure Gateway.
VMware Horizon View Security Gateway Component	Manual	Provides common gateway services. This service must always be running.

## Change the Product License Key

If the current license on a system expires, or if you want to access View features that are currently unlicensed, you can use View Administrator to change the product license key.

You can add a license to View while View is running. You do not need to reboot the system, and access to desktops and applications is not interrupted.

### Prerequisites

For the successful operation of View and add-on features such as View Composer and remote applications, obtain a valid product license key.

### Procedure

- 1 In View Administrator, select **View Configuration > Product Licensing and Usage**.  
The first and last five characters of the current license key are displayed in the **Licensing** panel.
- 2 Click **Edit License**.
- 3 Enter the license serial number and click **OK**.  
The Product Licensing window shows the updated licensing information.
- 4 Verify the license expiration date.
- 5 Verify that the Desktop, Application Remoting, and View Composer licenses are enabled or disabled, based on the edition of VMware Horizon 7 that your product license entitles you to use.  
Not all features and capabilities of VMware Horizon 7 are available in all editions. For a comparison of feature sets in each edition, see <http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf>.
- 6 Verify that the licensing usage model matches the model that is used in your product license.  
Usage is counted by the number of named users or concurrent users, depending on the edition and usage agreement for your product license.

## Monitoring Product License Usage

In View Administrator, you can monitor the active users who are concurrently connected to View. The **Product Licensing and Usage** page displays the current and highest historical usage numbers. You can use these numbers to keep track of your product license usage. You can also reset the historical usage data and start over with the current data.

View provides two licensing usage models, one for named users and one for concurrent users. View counts the named users and concurrent users in your environment, regardless of your product license edition or usage model agreement.

For named users, View counts the number of unique users that have accessed the View environment. If a named user runs multiple single-user desktops, RDS desktops, and remote applications, the user is counted once.

For named users, the **Current** column on the **Product Licensing and Usage** page displays the number of users since your View deployment was first configured or since you last reset the **Named Users Count**. The **Highest** column is not applicable to named users.

For concurrent users, View counts single-user desktop connections per session. If a concurrent user runs multiple single-user desktops, each connected desktop session is counted separately.

For concurrent users, RDS desktop and application connections are counted per user. If a concurrent user runs multiple RDS desktop sessions and applications, the user is counted only once, even if different RDS desktops or applications are hosted on different RDS hosts. If a concurrent user runs a single-user desktop and additional RDS desktops and applications, the user is counted only once.

For concurrent users, the **Highest** column on the **Product Licensing and Usage** page displays the highest number of concurrent desktop sessions and RDS desktop and application users since your View deployment was first configured or since you last reset the **Highest Count**.

## Reset Product License Usage Data

In View Administrator, you can reset the historical product usage data and start over with the current data.

An administrator with the **Manage Global Configuration and Policies** privilege can select the **Reset Highest Count** and **Reset Named Users Count** settings. To restrict access to these settings, give this privilege to designated administrators only.

### Prerequisites

Familiarize yourself with product license usage. See [“Monitoring Product License Usage,”](#) on page 134.

### Procedure

- 1 In View Administrator, select **View Configuration > Product Licensing and Usage**.
- 2 (Optional) In the **Usage** pane, select **Reset Highest Count**.

The highest historical number of concurrent connections is reset to the current number.

- 3 (Optional) In the **Usage** pane, select **Reset Named Users Count**.

The highest historical number of named users is reset to 0.

---

**NOTE** Selecting **Update General User Information** on the **Users and Groups** page also resets the highest historical number of named users to 0.

---

## Update General User Information from Active Directory

You can update View with the current user information that is stored in Active Directory. This feature updates the name, phone, email, user name, and default Windows domain of View users. The trusted external domains are also updated.

Use this feature if you modify the list of trusted external domains in Active Directory, especially if the altered trust relationships between domains affect user permissions in View.

This feature scans Active Directory for the latest user information and refreshes the View configuration.

Updating the general user information also resets the number of named users to 0. This number appears on the **Product Licensing and Usage** page in View Administrator. See [“Reset Product License Usage Data,”](#) on page 135.

You can also use the `vdmadmin` command to update user and domain information. See [“Updating Foreign Security Principals Using the -F Option,”](#) on page 256.

### Prerequisites

Verify that you can log in to View Administrator as an administrator with the **Manage Global Configuration and Policies** privilege.

### Procedure

- 1 In View Administrator, click **Users and Groups**.
- 2 Choose whether to update information for all users or an individual user.

Option	Action
<b>For all users</b>	Click <b>Update General User Information</b> . Updating all users and groups can take a long time.
<b>For an individual user</b>	<ol style="list-style-type: none"> <li>a Click the user name to update.</li> <li>b Click <b>Update General User Information</b>.</li> </ol>

## Migrate View Composer to Another Machine

In some situations, you might need to migrate a VMware Horizon View Composer service to a new Windows Server virtual or physical machine. For example, you might migrate View Composer and vCenter Server to a new ESXi host or cluster to expand your View deployment. In addition, View Composer and vCenter Server do not have to be installed on the same Windows Server machine.

You can migrate View Composer from the vCenter Server machine to a standalone machine or from a standalone machine to the vCenter Server machine.

- [Guidelines for Migrating View Composer](#) on page 137  
The steps you take to migrate the VMware Horizon View Composer service depend on whether you intend to preserve existing linked-clone virtual machines.
- [Migrate View Composer with an Existing Database](#) on page 137  
When you migrate View Composer to another physical or virtual machine, if you intend to preserve your current linked-clone virtual machines, the new VMware Horizon View Composer service must continue to use the existing View Composer database.
- [Migrate View Composer Without Linked-Clone Virtual Machines](#) on page 139  
If the current VMware Horizon View Composer service does not manage any linked-clone virtual machines, you can migrate View Composer to a new physical or virtual machine without migrating the RSA keys to the new machine. The migrated VMware Horizon View Composer service can connect to the original View Composer database, or you can prepare a new database for View Composer.
- [Prepare a Microsoft .NET Framework for Migrating RSA Keys](#) on page 140  
To use an existing View Composer database, you must migrate the RSA key container between machines. You migrate the RSA key container by using the ASP.NET IIS registration tool provided with the Microsoft .NET Framework.
- [Migrate the RSA Key Container to the New View Composer Service](#) on page 140  
To use an existing View Composer database, you must migrate the RSA key container from the source physical or virtual machine on which the existing VMware Horizon View Composer service resides to the machine on which you want to install the new VMware Horizon View Composer service.

## Guidelines for Migrating View Composer

The steps you take to migrate the VMware Horizon View Composer service depend on whether you intend to preserve existing linked-clone virtual machines.

To preserve the linked-clone virtual machines in your deployment, the VMware Horizon View Composer service that you install on the new virtual or physical machine must continue to use the existing View Composer database. The View Composer database contains data that is required to create, provision, maintain, and delete the linked clones.

When you migrate the VMware Horizon View Composer service, you can also migrate the View Composer database to a new machine.

Whether or not you migrate the View Composer database, the database must be configured on an available machine in the same domain as the new machine on which you install the VMware Horizon View Composer service, or on a trusted domain.

View Composer creates RSA key pairs to encrypt and decrypt authentication information stored in the View Composer database. To make this data source compatible with the new VMware Horizon View Composer service, you must migrate the RSA key container that was created by the original VMware Horizon View Composer service. You must import the RSA key container to the machine on which you install the new service.

If the current VMware Horizon View Composer service does not manage any linked-clone virtual machines, you can migrate the service without using the existing View Composer database. You do not have to migrate the RSA keys, whether or not you use the existing database.

---

**NOTE** Each instance of the VMware Horizon View Composer service must have its own View Composer database. Multiple VMware Horizon View Composer services cannot share a View Composer database.

---

## Migrate View Composer with an Existing Database

When you migrate View Composer to another physical or virtual machine, if you intend to preserve your current linked-clone virtual machines, the new VMware Horizon View Composer service must continue to use the existing View Composer database.

Follow the steps in this procedure when you migrate View Composer in any of the following directions:

- From a vCenter Server machine to a standalone machine
- From a standalone machine to a vCenter Server machine
- From a standalone machine to another standalone machine
- From a vCenter Server machine to another vCenter Server machine

When you migrate the VMware Horizon View Composer service, you can also migrate the View Composer database to a new location. For example, you might need to migrate the View Composer database if the current database is located on a vCenter Server machine that you are migrating as well.

When you install the VMware Horizon View Composer service on the new machine, you must configure the service to connect to the View Composer database.

### Prerequisites

- Familiarize yourself with the View Composer migration requirements. See [“Guidelines for Migrating View Composer,”](#) on page 137.
- Familiarize yourself with the steps for migrating the RSA key container to the new VMware Horizon View Composer service. See [“Prepare a Microsoft .NET Framework for Migrating RSA Keys,”](#) on page 140 and [“Migrate the RSA Key Container to the New View Composer Service,”](#) on page 140.

- Familiarize yourself with installing the VMware Horizon View Composer service. See "Installing View Composer" in the *View Installation* document.
- Familiarize yourself with configuring an SSL certificate for View Composer. See "Configuring SSL Certificates for View Servers" in the *View Installation* document.
- Familiarize yourself with configuring View Composer in View Administrator. See "[Configure View Composer Settings](#)," on page 16 and "[Configure View Composer Domains](#)," on page 17.

## Procedure

- 1 Disable virtual machine provisioning in the vCenter Server instance that is associated with the VMware Horizon View Composer service.
  - a In View Administrator, select **View Configuration > Servers**.
  - b On the **vCenter Servers** tab, select the vCenter Server instance and click **Disable Provisioning**.
- 2 (Optional) Migrate the View Composer database to a new location.  
If you need to take this step, consult your database administrator for migration instructions.
- 3 Uninstall the VMware Horizon View Composer service from the current machine.
- 4 (Optional) Migrate the RSA key container to the new machine.
- 5 Install the VMware Horizon View Composer service on the new machine.  
During the installation, specify the DSN of the database that was used by the original VMware Horizon View Composer service. Also specify the domain administrator user name and password that were provided for the ODBC data source for that database.  
If you migrated the database, the DSN and data source information must point to the new location of the database. Whether or not you migrated the database, the new VMware Horizon View Composer service must have access to the original database information about the linked clones.
- 6 Configure an SSL server certificate for View Composer on the new machine.  
You might be able to copy the certificate that was installed for View Composer on the original machine, or you can install a new certificate.
- 7 In View Administrator, configure the new View Composer settings.
  - a In View Administrator, select **View Configuration > Servers**.
  - b On the **vCenter Servers** tab, select the vCenter Server instance that is associated with this View Composer service and click **Edit**.
  - c In the View Composer Server Settings pane, click **Edit** and provide the new View Composer settings.  
If you are installing View Composer with vCenter Server on the new machine, select **View Composer co-installed with the vCenter Server**.  
If you are installing View Composer on a standalone machine, select **Standalone View Composer Server** and provide the FQDN of the View Composer machine and the user name and password of the View Composer user.
  - d In the Domains pane, click **Verify Server Information** and add or edit the View Composer domains as needed.
  - e Click **OK**.

## Migrate View Composer Without Linked-Clone Virtual Machines

If the current VMware Horizon View Composer service does not manage any linked-clone virtual machines, you can migrate View Composer to a new physical or virtual machine without migrating the RSA keys to the new machine. The migrated VMware Horizon View Composer service can connect to the original View Composer database, or you can prepare a new database for View Composer.

### Prerequisites

- Familiarize yourself with installing the VMware Horizon View Composer service. See "Installing View Composer" in the *View Installation* document.
- Familiarize yourself with configuring an SSL certificate for View Composer. See "Configuring SSL Certificates for View Servers" in the *View Installation* document.
- Familiarize yourself with the steps for removing View Composer from View Administrator. See ["Remove View Composer from View,"](#) on page 24.

Before you can remove View Composer, verify that it no longer manages any linked-clone desktops. If any linked clones remain, you must delete them.

- Familiarize yourself with configuring View Composer in View Administrator. See ["Configure View Composer Settings,"](#) on page 16 and ["Configure View Composer Domains,"](#) on page 17.

### Procedure

- 1 In View Administrator, remove View Composer from View Administrator.
  - a Select **View Configuration > Servers**.
  - b On the **vCenter Servers** tab, select the vCenter Server instance that is associated with the View Composer service and click **Edit**.
  - c In the View Composer Server Settings pane, click **Edit**.
  - d Select **Do not use View Composer** and click **OK**.
- 2 Uninstall the VMware Horizon View Composer service from the current machine.
- 3 Install the VMware Horizon View Composer service on the new machine.
 

During the installation, configure View Composer to connect to the DSN of the original or new View Composer database.
- 4 Configure an SSL server certificate for View Composer on the new machine.
 

You might be able to copy the certificate that was installed for View Composer on the original machine, or you can install a new certificate.
- 5 In View Administrator, configure the new View Composer settings.
  - a In View Administrator, select **View Configuration > Servers**.
  - b On the **vCenter Servers** tab, select the vCenter Server instance that is associated with this View Composer service and click **Edit**.
  - c In the View Composer Server Settings pane, click **Edit**.
  - d Provide the new View Composer settings.

If you are installing View Composer with vCenter Server on the new machine, select **View Composer co-installed with the vCenter Server**.

If you are installing View Composer on a standalone machine, select **Standalone View Composer Server** and provide the FQDN of the View Composer machine and the user name and password of the View Composer user.

- e In the Domains pane, click **Verify Server Information** and add or edit the View Composer domains as needed.
- f Click **OK**.

## Prepare a Microsoft .NET Framework for Migrating RSA Keys

To use an existing View Composer database, you must migrate the RSA key container between machines. You migrate the RSA key container by using the ASP.NET IIS registration tool provided with the Microsoft .NET Framework.

### Prerequisites

Download the .NET Framework and read about the ASP.NET IIS registration tool. Go to <http://www.microsoft.com/net>.

### Procedure

- 1 Install the .NET Framework on the physical or virtual machine on which the VMware Horizon View Composer service associated with the existing database is installed.
- 2 Install the .NET Framework on the destination machine on which you want to want to install the new VMware Horizon View Composer service.

### What to do next

Migrate the RSA key container to the destination machine. See [“Migrate the RSA Key Container to the New View Composer Service,”](#) on page 140.

## Migrate the RSA Key Container to the New View Composer Service

To use an existing View Composer database, you must migrate the RSA key container from the source physical or virtual machine on which the existing VMware Horizon View Composer service resides to the machine on which you want to install the new VMware Horizon View Composer service.

You must perform this procedure before you install the new VMware Horizon View Composer service.

### Prerequisites

Verify that the Microsoft .NET Framework and the ASP.NET IIS registration tool are installed on the source and destination machines. See [“Prepare a Microsoft .NET Framework for Migrating RSA Keys,”](#) on page 140.

### Procedure

- 1 On the source machine on which the existing VMware Horizon View Composer service resides, open a command prompt and navigate to the %windir%\Microsoft.NET\Framework\v2.0xxxxx directory.
- 2 Type the `aspnet_regiis -px "SviKeyContainer" "keys.xml" -pri`

```
aspnet_regiis -px "SviKeyContainer" "keys.xml" -pri
```

The ASP.NET IIS registration tool exports the RSA public-private key pair from the SviKeyContainer container to the keys.xml file and saves the file locally.
- 3 Copy the keys.xml file to the destination machine on which you want to install the new VMware Horizon View Composer service.
- 4 On the destination machine, open a command prompt and navigate to the %windir%\Microsoft.NET\Framework\v2.0xxxxx directory.

- 5 Type the `aspnet_regiis` command to migrate the RSA key pair data.

```
aspnet_regiis -pi "SviKeyContainer" "path\keys.xml" -exp
```

where *path* is the path to the exported file.

The `-exp` option creates an exportable key pair. If a future migration is required, the keys can be exported from this machine and imported to another machine. If you previously migrated the keys to this machine without using the `-exp` option, you can import the keys again using the `-exp` option so that you can export the keys in the future.

The registration tool imports the key pair data into the local key container.

### What to do next

Install the new VMware Horizon View Composer service on the destination machine. Provide the DSN and ODBC data source information that allows View Composer to connect to the same database information that was used by the original VMware Horizon View Composer service. For installation instructions, see "Installing View Composer" in the *View Installation* document.

Complete the steps to migrate View Composer to a new machine and use the same database. See ["Migrate View Composer with an Existing Database,"](#) on page 137.

## Update the Certificates on a View Connection Server Instance, Security Server, or View Composer

When you receive updated server SSL certificates or intermediate certificates, you import the certificates into the Windows local computer certificate store on each View Connection Server, security server, or View Composer host.

Typically, server certificates expire after 12 months. Root and intermediate certificates expire after 5 or 10 years.

For detailed information about importing server and intermediate certificates, see "Configure View Connection Server, Security Server, or View Composer to Use a New SSL Certificate" in the *View Installation* document.

### Prerequisites

- Obtain updated server and intermediate certificates from the CA before the currently valid certificates expire.
- Verify that the Certificate snap-in was added to MMC on the Windows Server on which the View Connection Server instance, security server, or VMware Horizon View Composer service was installed.

### Procedure

- 1 Import the signed SSL server certificate into the Windows local computer certificate store on the Windows Server host.
  - a In the Certificate snap-in, import the server certificate into the **Certificates (Local Computer) > Personal > Certificates** folder.
  - b Select **Mark this key as exportable**.
  - c Click **Next** and click **Finish**.
- 2 For View Connection Server or security server, delete the certificate Friendly name, **vdm**, from the old certificate that was issued to the View server.
  - a Right-click the old certificate and click **Properties**
  - b On the General tab, delete the Friendly name text, **vdm**.

- 3 For View Connection Server or security server, add the certificate Friendly name, **vdm**, to the new certificate that is replacing the previous certificate.
  - a Right-click the new certificate and click **Properties**
  - b On the General tab, in the Friendly name field, type **vdm**.
  - c Click **Apply** and click **OK**.
- 4 For a server certificate that is issued to View Composer, run the SviConfig ReplaceCertificate utility to bind the new certificate to the port used by View Composer.  
 This utility replaces the old certificate binding with the new certificate binding.
  - a Stop the VMware Horizon View Composer service.
  - b Open a Windows command prompt and navigate to the SviConfig executable file.  
 The file is located with the View Composer application. The default path is C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe.
  - c Type the SviConfig ReplaceCertificate command. For example:  

```
sviconfig -operation=ReplaceCertificate
          -delete=false
```

 The utility displays a numbered list of SSL certificates that are available in the Windows local computer certificate store.
  - d To select a certificate, type the number of the certificate and press Enter.
- 5 If intermediate certificates are issued to a View Connection Server, security server, or View Composer host, import the most recent update to the intermediate certificates into the **Certificates (Local Computer) > Intermediate Certification Authorities > Certificates** folder in the Windows certificate store.
- 6 Restart the VMware Horizon View Connection Server service, VMware Horizon View Security Server service, or VMware Horizon View Composer service to make your changes take effect.

## Information Collected by the Customer Experience Improvement Program

You can participate in a customer experience improvement program (CEIP). If you participate in the program, VMware collects anonymous data about your deployment in order to improve VMware's response to customer requirements. VMware uses this information to improve the quality, reliability, and performance of our products. No data that identifies your organization is collected.

Participation in this program is optional. You can choose not to participate by deselecting the option when you install View Connection Server with a new configuration. If you change your mind about participating at any time after the installation, you can either join or withdraw from the program by editing the Product Licensing and Usage page in View Administrator.

Before collecting the data, VMware makes anonymous all fields that contain information that is specific to your organization. The sanitized fields identify computers, data storage, networking features, applications, and users. For example, IP addresses and virtual machine customization specifications are made anonymous.

VMware sanitizes a field by generating a hash of the actual value. When a hash value is collected, VMware cannot identify the actual value but can detect changes in the value when you change your environment.

To help you determine whether to join the program, you can review the fields from which VMware gathers data. You can also examine all the sanitized fields. The fields are organized by View component. See [“Global View Data Collected by VMware,”](#) on page 144 and the related topics that follow.

## How VMware Ensures Your Privacy

VMware is committed to protecting your privacy and takes several steps to ensure that no data collected by the customer experience improvement program (CEIP) includes sensitive information that could uniquely identify a particular customer or user. The program does not collect any information that can be used to identify you or contact you. No data that identifies your organization or users is collected.

When the CEIP feature is enabled, View Connection Server gathers information from your deployment and performs the following actions on the data:

- 1 Data that could uniquely identify your deployment such as users, server names, IP addresses, and network server paths is made anonymous by executing a one-way hash function on the data. This approach allows VMware to gather useful information about how many unique servers, machines, and users are included in your deployment without collecting any specific server names, user names, or addresses.
- 2 The entire data set is encrypted using a public key. The private key that is required to decrypt the data set is available only to VMware.
- 3 The encrypted, anonymized information is transmitted to VMware using HTTPS.

You can review the complete list of fields from which data is collected, including which fields are made anonymous. See [“Global View Data Collected by VMware,”](#) on page 144 and the related topics that follow.

## Preview Data Collected by the Customer Experience Improvement Program

You can preview the data that VMware would receive before the data is encrypted and transmitted. When you enable this option, View Connection Server writes the data set to disk instead of encrypting and sending the data to VMware.

You configure the option to write CEIP data to disk instead of transmitting the data to VMware as a global option in the View LDAP directory. You use the ADSI Edit utility to modify View LDAP. The ADSI Edit utility is installed with View Connection Server. When you change View LDAP on a View Connection Server instance, the change is propagated to all replicated View Connection Server instances.

### Procedure

- 1 Start the ADSI Edit utility on your View Connection Server host.
- 2 In the Connection Settings dialog box, select or connect to **DC=vdi, DC=vmware, DC=int**.
- 3 In the Computer pane, select or type **localhost:389** or the fully qualified domain name (FQDN) of the View Connection Server host followed by port 389.

For example: localhost:389 or mycomputer.mydomain.com:389

- 4 On the object **CN=Common, OU=Global, OU=Properties**, set the **pae-ceipDumpOnly** attribute value to 1.
- 5 Restart View Connection Server.

The CEIP data files are written in plain-text JSON format to the %PROGRAMFILES%\VMware\VMware View\Server\broker\temp\spool directory on the View Connection Server instance.

### What to do next

To revert the setting and begin sending data to VMware, change **pae-ceipDumpOnly** attribute value to 0 and restart View Connection Server.

## Additional Information About the Customer Experience Improvement Program

After you choose to participate in the CEIP, data is collected on the first View Connection Server instance that starts in a View deployment. Configuration data is collected on a weekly basis. Performance and usage data is collected on an hourly basis. If your View Connection Server instance does not have access to the Internet, the information is saved on disk until the next time Internet connectivity is available.

If you choose to participate, you can opt out later. You can join or end your participation at any time by editing the **Send anonymous data to VMware** setting in the Product Licensing and Usage page in View Administrator. In order for the change to take effect, restart each View Connection Server instance in the environment.

Data collection by the CEIP does not have any negative performance or disk consumption impact on your View deployment. The information that is collected and sent to VMware is sent to the View Connection Server instance whether or not the CEIP feature is enabled. By default, enabling the feature can consume a maximum of 100MB of disk space on the View Connection Server instance to store data before it is sent to VMware. By default, unsent data that is more than eight days old is discarded.

If your View Connection Server instances are blocked by a firewall from accessing the Internet, you can still use the CEIP. When the CEIP is enabled, your View Connection Server instances periodically attempt to connect using HTTPS to the data collection URL at <https://ceip.vmware.com>. If the connection is blocked or inaccessible due to a proxy server or firewall restriction, View Connection Server caches your CEIP data until the records exceed the configured maximum age, eight days by default, or the total collected data exceeds the configured maximum spool size, 100MB by default.

You can change the location, maximum size, and maximum age of the CEIP data spool. The spool location and size are governed by the following settings in the View LDAP database:

<b>pae-ceipSpoolDirectory</b>	Directory where CEIP data is cached before being sent to VMware. Default: Program Files\VMware\VMware View\Server\broker\temp\spool
<b>pae-ceipMaxSpoolSize</b>	Maximum size, in bytes, of temporary spool data. Default: 100 MB
<b>pae-ceipMaxSpoolAge</b>	Maximum age of records in the temporary local spool. Default: 8 days

You will not be contacted or receive spam if you participate in the CEIP. The CEIP does not collect contact information such as your name, home address, email address, or phone number. The CEIP will not ask you to participate in surveys or to read junk e-mail, and you will not be contacted in any other way.

## Global View Data Collected by VMware

If you join the customer experience improvement program, VMware collects global data about the View environment. Fields containing sensitive information are made anonymous.

**Table 8-6.** Information About Global Configuration Settings

Description	Is This Field Made Anonymous?	Example Value
Maximum lifespan, in seconds, for a View Connection Server session	No	180,000
Amount of time, in seconds, before the View Connection Server forcibly disconnects users if no data is sent from the client	No	36,000

**Table 8-6.** Information About Global Configuration Settings (Continued)

Description	Is This Field Made Anonymous?	Example Value
Amount of time in seconds, that a user can be idle before View Connection Server locks the user's single sign-on (SSO) credentials	No	900
Amount of time, in minutes, before SSO credentials are cleared for desktop launches	No	-1 (which means never)
Amount of time, in minutes, before SSO credentials are cleared for application launches	No	-1 (which means never)
View Administrator console session timeout, in seconds	No	3,000
Show a pre-login message when users connect to View Connection Server instances in this pod	No	0 or 1
Remote desktop can run a server operating system	No	True or false
Mirage server is enabled	No	True or false
URL of the Mirage server, including port number	Yes	None
Is True SSO enabled?	Yes	None
Is there a primary enrollment server configured for True SSO?	Yes	None
Is there a secondary enrollment server configured for True SSO?	Yes	None

**Table 8-7.** Global Status Information

Description	Is This Field Made Anonymous?	Example Value
View servers can contact the domain controller.	No	True or false
The DNS of the Active Directory domain	Yes	None
The domain is an NT4-style domain.	No	True or false
The name of the domain	Yes	None
The status of the domain	No	OK
The type of trust relationship with the domain	No	Primary domain, two-way, two-way forest, and so on

## View Connection Server Data Collected by VMware

If you join the customer experience improvement program, VMware collects data from certain View Connection Server fields. Fields containing sensitive information are made anonymous.

**Table 8-8.** Configuration Information Collected from View Connection Server

Description	Is This Field Made Anonymous?	Example Value
The common name (CN) for the View Connection Server entry in View LDAP	Yes	None
View Connection Server is disabled	No	True or false
SecureID authentication is configured and active	No	True or false

**Table 8-8.** Configuration Information Collected from View Connection Server (Continued)

<b>Description</b>	<b>Is This Field Made Anonymous?</b>	<b>Example Value</b>
RADIUS authentication is configured and active	No	True or false
SAML server authentication is allowed, disabled, or required	No	0 = Disabled 1 = Allowed 2 = Required
Type of View Connection Server installation	No	0 = View Connection Server 1 = security server
Must the SecureID authentication name match the Active Directory name?	No	True = SecureID authentication name is mapped False = SecureID authentication name is not mapped
Are clients allowed to bypass the secure tunnel?	No	True or false
Are clients allowed to bypass the PCoIP Secure Gateway?	No	True or false
Configuration of smart card authentication	No	Off, Optional, or Required
Should users be automatically logged off when their smart card is removed?	No	True or false
Folder in which View LDAP backups are stored	Yes	None
Units of time for setting the View LDAP backup frequency	No	Hour, Day, or Week
Frequency of View LDAP backups	No	Integer
Time of View LDAP backup	No	Integer
Maximum number of View LDAP backups to store	No	Integer
Time of last View LDAP backup	No	Feb 21, 2014 12:00:10 AM
Status of the last View LDAP backup	No	OK
Pending immediate View LDAP backup	No	True or false
Tags associated with the View Connection Server instance	Yes	None
Whether the View Connection Server instance is paired with a security server	No	0 = Not paired 1 = Paired
The distinguished name (DN) of the View Connection Server instance in LDAP	Yes	None
Length of time the security server pairing password is valid	No	
The host/node name of the View Connection Server instance	Yes	None
The version number only of the View Connection Server instance	No	6.0.0
The full build and version of the View Connection Server instance	No	6.0.0-123455
Auto-reconnect to the secure gateway	No	True or false
Tunnel client protocol	No	
Protocol the View Connection Server instance or security server listens on	No	

**Table 8-9.** Status Information Collected from View Connection Server

<b>Description</b>	<b>Is This Field Made Anonymous?</b>	<b>Example Value</b>
The View Connection Server instance's build number	No	123456
Name of the View Connection Server replicated group, typically the first View Connection Server instance's node name	Yes	None
DNS name of the View Connection Server instance	Yes	None
IP address of the View Connection Server instance	Yes	None
NetBIOS host name of the View Connection Server instance	Yes	None
The current number of sessions on this View Connection Server instance	No	Integer
The maximum number of sessions on this View Connection Server instance	No	Integer
The current number of View Composer sessions on this View Connection Server instance	No	Integer
The maximum number of View Composer sessions on this View Connection Server instance	No	Integer
The version of the View Connection Server instance	No	6.0.0

**Table 8-10.** Dynamic Usage Data Collected from View Connection Server

<b>Description</b>	<b>Is This Field Made Anonymous?</b>	<b>Example Value</b>
Number of times individual PowerShell cmdlets have been invoked	No	List of integers
Number of times individual View API methods have been invoked in the previous minute	No	List of integers
Login rate, using passwords, over time	No	Float
Login rate, using the SSL server certificate, over time	No	Float
Login rate, using delegated authentication such as SAML, over time	No	Float
Average percent CPU utilization	No	Integer
Average percent memory utilization	No	Integer
Average logins with and without passwords available for SSO	No	Float
Number of times desktop connections have been launched with each type of display protocol (PCoIP, RDP, and VMware Blast)	No	List of integers
Number of times a new client connection has been made to a remote application, for each type of display protocol (PCoIP, RDP, and VMware Blast)	No	List of integers
Number of times launching a remote application results in a new connection, a reused connection, a new session connection, and a reused session connection	No	List of integers
Number of times desktop connections have been launched for a user who is entitled to <i>n</i> number of desktops	No	List of integers, such as a list of how many users are entitled to 1 desktop, 2 desktops, 3 desktops, and so on

**Table 8-10.** Dynamic Usage Data Collected from View Connection Server (Continued)

Description	Is This Field Made Anonymous?	Example Value
Number of times application connections have been launched for a user who is entitled to <i>n</i> number of applications	No	List of integers
Number of times <i>n</i> protocol (such as PCoIP) sessions have been in existence when a user launches another application. For example, a user launches a fifth application but because all the applications are in the same server farm, only one session is in existence.	No	List of integers, such as a list of how many users have one session, how many have two sessions, and so on

## Security Server Data Collected by VMware

If you join the customer experience improvement program, VMware collects data from security server fields. Fields containing sensitive information are made anonymous.

**Table 8-11.** Security Server Information

Description	Is This Field Made Anonymous?	Example Value
The number of PCoIP sessions that are running on the security server secure gateway	No	Integer
The number of sessions of any type that are running on the security server secure gateway	No	Integer
The security server build number	No	123456
The host name of the security server	Yes	None
IPsec is active	No	True or false
The secure gateway is down	No	True or false
The current number of sessions	No	Integer
The URL of the secure gateway	Yes	None
The security server version number	No	6.0.0

## Desktop Pool Data Collected by VMware

If you join the customer experience improvement program, VMware collects data from certain desktop pool fields. Fields containing sensitive information are made anonymous.

**Table 8-12.** Configuration Information Collected from Desktop Pools

Description	Is This Field Made Anonymous?	Example Value
The common name (CN) for the desktop pool entry in View LDAP	Yes	None
The descriptive, display name of the desktop pool	Yes	None
The desktop pool is disabled	No	True or false

**Table 8-12.** Configuration Information Collected from Desktop Pools (Continued)

<b>Description</b>	<b>Is This Field Made Anonymous?</b>	<b>Example Value</b>
Type of desktop pool	No	One of the following: IndividualVC, IndividualUnmanaged, Persistent, NonPersistent, SviPersistent, SviNonPersistent, ManualVCPersistent, Manual, ManualUnmanagedPersistent, ManualUnmanagedNonPersistent, TerminalService, OnRequestVcPersistent, OnRequestVcNonPersistent, OnRequestSviPersistent, OnRequestSviNonPersistent
The View Administrator folder under which this desktop pool is grouped	Yes	None
The list of virtual machine Distinguished Names (DNs) that belong to the desktop pool	No	An example list item: ["CN=8f11d7cf-b0ef-43ad-92ce-691aa929d3c4,0U=Servers,DC=vdi,DC=vmware,DC=int"]
Are multiple sessions allowed in the desktop pool?	No	True or false
Are users of this desktop pool allowed to reset their virtual machines?	No	Off, Optional, or Required
Time after which a forced logoff message is displayed	No	True or false
The Distinguished Name (DN) of the vCenter Server instance that manages the virtual machines in the pool	No	"CN=e7a718de-d0f7-444a-9452-156dce289028,0U=VirtualCenter,OU=Properties,DC=vdi,DC=vmware,DC=int"
Minimum number of virtual machines in the desktop pool	No	Integer
Maximum number of virtual machines in the desktop pool	No	Integer
Number of spare, provisioned virtual machines in the desktop pool	No	Integer
Deletion policy for the desktop pool	No	Default, DeleteOnUse, or RefreshOnUse
DNS suffix used in provisioning	Yes	None
The naming pattern (prefix) to use for auto-deployed virtual machine names	Yes	None
The template from which to clone virtual machines	Yes	None
The folder in vCenter Server in which deployed virtual machines are stored	Yes	None
The resource pool used for the virtual machines	Yes	None
A list of datastores	Yes	None
The customization specification used to deploy virtual machines	Yes	None
Enable auto-provisioning for the desktop pool	No	True or false
Errors encountered while provisioning	No	
Stop provisioning when an error is encountered	No	True or false

**Table 8-12.** Configuration Information Collected from Desktop Pools (Continued)

<b>Description</b>	<b>Is This Field Made Anonymous?</b>	<b>Example Value</b>
Start provisioning	No	True or false
Pool values have been calculated	No	True or false
The parent virtual machine used to provision linked clones	Yes	None
The snapshot name used for linked-clone provisioning	Yes	None
The snapshot ID used for linked-clone provisioning	No	"snapshot-38685"
Deployment group ID used by the VMware Horizon View Composer service	No	"7119316f-00a8-463d-bbba-c3000f105aeb"
View Composer persistent disk datastore path	Yes	None
Type of View Composer disk	No	"SystemDisposable", "UserProfile", and so on
Create the persistent disk as a sparse disk	No	True or false
The drive mount letter for the persistent disk or disposable data disk	No	"*", "C", and so on
Target size of the persistent disk	No	Integer
Type of refresh policy	No	Always, Never, or Conditional
Usage threshold for refresh operations	No	Integer
Time threshold for refresh operations	No	Integer
Level of overcommit for a datastore that stores linked clones	No	None, Conservative, Moderate, Aggressive
Datastore path for a datastore that stores linked clones	Yes	None
List of IDs this datastore is used for	No	List of GUIDs, such as the following: ["7119316f-00a8-463d-bbba-c3000f105aeb"]
Virtual machine state	No	Ready, Pre-provisioned, Cloning, Cloning Error, Customizing, Deleting, Maintenance, Error, or Logout
Assign a virtual machine to a user when the user first logs in	No	True or false
Flags for the desktop pool	No	
Multimonitor configuration settings	No	svga.maxWidth:int, svga.vramSize:int, svga.maxHeight:int, svga.enable3d:bool, svga.numDisplays:int
An individual virtual machine was converted to a manual pool	No	True or false
The linked-clone pool uses native snapshot cloning with VAAI	No	True or false
View Storage Accelerator (CBRC) is enabled	No	True or false
Frequency that the CBRC cache is refreshed	No	Integer
CBRC cache refresh blackout periods	No	List
The disk types that are cached for CBRC (OS disks, persistent disks)	No	List

**Table 8-12.** Configuration Information Collected from Desktop Pools (Continued)

Description	Is This Field Made Anonymous?	Example Value
Virtual machine disk space reclamation (SE Sparse format) is enabled	No	True or false
Disk space reclamation threshold, in bytes	No	
Minimum number of virtual machines that are ready during a refit operation	No	
The desktop pool uses a Virtual SAN datastore	No	True or false
Number of remote desktop entitlements for this server pool	No	0 or 1
Number of remote application entitlements for this pool	No	0 or 1
Default display protocol	No	PCoIP, RDP, or Blast
The user can chose the display protocol used	No	True or false
HTML Access is enabled	No	True or false
Flash quality level	No	None used, low, medium, high
Flash throttling level	No	None used, conservative, moderate, aggressive
Pool is disabled	No	True or false
Pool is marked for deletion	No	True or false
Tags associated with the View Connection Server instance	Yes	None
Use a different Mirage server than what is specified in the global settings	No	True or false
Mirage server is enabled	No	True or false
URL of the Mirage server, including port number	Yes	None
Number of clones per pool	No	Integer

## Machine Data Collected by VMware

If you join the customer experience improvement program, VMware collects data from View and vCenter Server fields that describe virtual machines. Fields containing sensitive information are made anonymous.

**Table 8-13.** Machine Data Collected from View

Description	Is This Field Made Anonymous?	Example Value
The machine was marked as dirty. The virtual machine was used when useonce=true, and therefore should not accept new sessions	No	True or false
Mapping of devices to change IDs	No	A set of IDs such as the following: 2000=01874583;01874583&2016=3910f513;3910f513
An identifier for the machine that is used to correlate data	No	vm-10
Sysprep customization is used for the guest operating system	No	True or false
Timeout value. The period of time before the machine is disconnected.	No	Time

**Table 8-13.** Machine Data Collected from View (Continued)

<b>Description</b>	<b>Is This Field Made Anonymous?</b>	<b>Example Value</b>
A random ID for View Agent or Horizon Agent for this machine	No	GUID
Miscellaneous configuration values	No	Integers and booleans (true or false)
View LDAP identifier for the previous View Composer persistent disk	No	LDAP entry
Thinapps that are entitled to the machine	Yes	None
Thinapps that are pending an uninstallation	Yes	None
Thinapps that are installed in the machine	Yes	None
The state of the machine	No	Undefined, Pre-provisioned, Cloning, Cloning error, Customizing, Ready, Deleting, Maintenance, Error, or Logout
Timestamp of when customization started	No	Integer
The machine is powered on for customization	No	Integer. The values are 0 or 1.
The machine is powered on	No	True or false
The machine is suspended	No	True or false
The machine state is in transition	No	True or false
The machine is configured	No	True or false
The path to the virtual machine in vCenter Server	Yes	None
Customization template used to customize the machine	Yes	None
View Composer linked clone ID for the machine	No	GUID of the linked clone
The virtual machine missing in vCenter Server	No	True or false
Number of times View tried to power off the machine	No	Integer
Status of CBRC (View Storage Accelerator)	No	Off, Current, Out of date, or Error
Time of the latest CBRC refresh	No	Date
Time of the latest CBRC error	No	Integer
Time of the latest incomplete attempt to configure CBRC	No	Integer
The version of View Agent or Horizon Agent installed on the machine	No	6.0.0-551711
View Persona Management is enabled on the machine	No	True or false
Last amount, in bytes, of machine disk space reclaimed (if using SE Sparse format)	No	
Time of last space reclamation	No	Timestamp

**Table 8-14.** Virtual Machine Data Collected from vCenter Server

<b>Description</b>	<b>Is This Field Made Anonymous?</b>	<b>Example Value</b>
The virtual machine hardware version	No	v8
The amount of RAM that is allocated to the virtual machine	No	1024

**Table 8-14.** Virtual Machine Data Collected from vCenter Server (Continued)

Description	Is This Field Made Anonymous?	Example Value
The number of virtual CPUs that are configured in the virtual machine	No	Integer
The operating system installed on the virtual machine	No	Microsoft Windows 7 (32-bit), Microsoft Windows 8 (32-bit), Microsoft Windows Server 2008 R2 (64-bit), Microsoft Windows Server 2012 R2 (64-bit), and so on

## vCenter Server Data Collected by VMware

If you join the customer experience improvement program, VMware collects data from certain vCenter Server fields. Fields containing sensitive information are made anonymous.

**Table 8-15.** Host System Information Collected from vCenter Server

Description	Is This Field Made Anonymous?	Example Value
The time that View last communicated with this vCenter Server host	No	Integer
The URL of the vCenter Server instance	Yes	None
The API version of the vCenter Server instance	No	5.0
The build number of the vCenter Server instance	No	456789
The version number of the vCenter Server instance	No	5.0.0

**Table 8-16.** Host Status Information Collected from vCenter Server

Description	Is This Field Made Anonymous?	Example Value
The internal status code of the connection status between vCenter Server and View Connection Server	No	Status_Up
Description of the connection status code	No	Connected
The vCenter Server SSL certificate is valid	No	True or false
The reason that the SSL certificate is not valid	No	Name mismatch, not trusted, cannot check revocation, and so on

**Table 8-17.** Datastore Data Collected from vCenter Server

Description	Is This Field Made Anonymous?	Example Value
Disk capacity of this datastore	No	Integer
Free disk space on this datastore	No	Integer
The type of storage	No	NFS, VMFS
Multiple hosts can access this datastore concurrently.	No	True or false

**Table 8-18.** ESX Node Information

Description	Is This Field Made Anonymous?	Example Value
Identifier of the vCenter Server that manages a particular ESXi host, along with an identifier for the ESXi host	No	1234-ADEE-BECF-41AA-4950BCDA-host-14

**Table 8-19.** Information About Direct-Attached Storage for an ESXi Host

Description	Is This Field Made Anonymous?	Example Value
Hardware vendor of the physical disk	No	SEAGATE
Model of the physical disk	No	ST9300653SS
SSD	No	True or false
Capacity, in bytes	No	
Identifier for the ESXi host	No	host-123
Identifier of the vCenter Server that manages a particular ESXi host	No	1234-ADEE-BECF-41AA-4950BCDA

## ThinApp Data Collected by VMware

If you join the customer experience improvement program, VMware collects data from certain ThinApp fields. Fields containing sensitive information are made anonymous.

**Table 8-20.** ThinApp Information

Description	Is This Field Made Anonymous?	Value Type
Display name of the ThinApp package	No	
Number of MSI packages associated with ThinApp	No	Integer
Assignment count for full installation	No	Integer
List of pools set to use full installation	Yes	List with hash of CN (common name)
Remote desktops set to use full installation	No	List with CN (GUID) of desktops
Assignment count for streaming the ThinApp	No	Integer
List of pools set to stream ThinApp	Yes	List with hash of CN (common name)
Remote desktops set to stream the ThinApp	No	List with CN (GUID) of desktops
ThinApps in a group for pools set to use full installation	No	List with ID of ThinApps

## Cloud Pod Architecture Information Collected by VMware

If you join the customer experience improvement program, VMware collects data from certain Cloud Pod Architecture fields. Fields containing sensitive information are made anonymous.

**Table 8-21.** Information Collected About Cloud Pod Architecture

Description	Is This Field Made Anonymous?	Example or type
The Cloud Pod Architecture feature is enabled	No	True or false
Local pod ID	No	
Frequency, in seconds, that the system will perform a cross-pod health check	No	Integer
Maximum allowed time difference between the pods, in seconds	No	Integer
Common name of the site that the pod belongs to	No	
List of global entitlement IDs (for example, a pod has desktop pools that support the global entitlements)	No	List of strings
Common name of the pod endpoint, which is a View Connection Server instance	Yes	
Common name of the pod that contains this endpoint	No	
The pod endpoint is disabled	No	True or false
Weighting to apply when randomly selecting endpoints (View Connection Server instances) for remote sessions	No	Integer
The global entitlement is disabled	No	True or false
Desktop lookup starts from the user's home site (If set to false, the lookup starts from the local pod)	No	True or false
Global entitlement is for a dedicate desktop	No	0 = No 1 = Yes
Scope for which the existing session lookup is to be done	No	ANY, SITE, or LOCAL
Scope for which the new session placement is to be done	No	ANY, SITE, or LOCAL
User's home site is required for this global entitlement	No	True or false
Automatic session cleanup is enabled	No	True or false

## Horizon Client Data Collected by VMware

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

Although the information is encrypted while in transit to 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.

**Table 8-22.** Data Collected from Horizon Clients for the Customer Experience Improvement Program

<b>Description</b>	<b>Is This Field Made Anonymous ?</b>	<b>Example Value</b>
Company that produced the Horizon Client application	No	VMware
Product name	No	VMware Horizon Client
Client product version	No	(The format is <i>x.x.x-yyyyyy</i> , where <i>x.x.x</i> is the client version number and <i>yyyyyy</i> is the build number.)
Client binary architecture	No	Examples include the following: <ul style="list-style-type: none"> <li>■ i386</li> <li>■ x86_64</li> <li>■ arm</li> </ul>
Client build name	No	Examples include the following: <ul style="list-style-type: none"> <li>■ VMware-Horizon-Client-Win32-Windows</li> <li>■ VMware-Horizon-Client-Linux</li> <li>■ VMware-Horizon-Client-iOS</li> <li>■ VMware-Horizon-Client-Mac</li> <li>■ VMware-Horizon-Client-Android</li> <li>■ VMware-Horizon-Client-WinStore</li> </ul>
Host operating system	No	Examples include the following: <ul style="list-style-type: none"> <li>■ Windows 8.1</li> <li>■ Windows 7, 64-bit Service Pack 1 (Build 7601 )</li> <li>■ iPhone OS 5.1.1 (9B206)</li> <li>■ Ubuntu 12.04.4 LTS</li> <li>■ Mac OS X 10.8.5 (12F45)</li> </ul>
Host operating system kernel	No	Examples include the following: <ul style="list-style-type: none"> <li>■ Windows 6.1.7601 SP1</li> <li>■ Darwin Kernel Version 11.0.0: Sun Apr 8 21:52:26 PDT 2012; root:xnu-1878.11.10~1/RELEASE_ARM_S5L8945X</li> <li>■ Darwin 11.4.2</li> <li>■ Linux 2.6.32-44-generic #98-Ubuntu SMP Mon Sep 24 17:27:10 UTC 2012</li> <li>■ unknown (for Windows Store)</li> </ul>
Host operating system architecture	No	Examples include the following: <ul style="list-style-type: none"> <li>■ x86_64</li> <li>■ i386</li> <li>■ armv71</li> <li>■ ARM</li> </ul>
Host system model	No	Examples include the following: <ul style="list-style-type: none"> <li>■ Dell Inc. OptiPlex 960</li> <li>■ iPad3,3</li> <li>■ MacBookPro8,2</li> <li>■ Dell Inc. Precision WorkStation T3400 (A04 03/21/2008)</li> </ul>
Host system CPU	No	Examples include the following: <ul style="list-style-type: none"> <li>■ Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GH</li> <li>■ Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GH</li> <li>■ unknown (for iPad)</li> </ul>
Number of cores in the host system's processor	No	For example: 4

**Table 8-22.** Data Collected from Horizon Clients for the Customer Experience Improvement Program (Continued)

Description	Is This Field Made Anonymous ?	Example Value
MB of memory on the host system	No	Examples include the following: <ul style="list-style-type: none"> <li>■ 4096</li> <li>■ unknown (for Windows Store)</li> </ul>
Number of USB devices connected	No	2 (USB device redirection is supported only for Linux, Windows, and Mac clients.)
Maximum concurrent USB device connections	No	2
USB device vendor ID	No	Examples include the following: <ul style="list-style-type: none"> <li>■ Kingston</li> <li>■ NEC</li> <li>■ Nokia</li> <li>■ Wacom</li> </ul>
USB device product ID	No	Examples include the following: <ul style="list-style-type: none"> <li>■ DataTraveler</li> <li>■ Gamepad</li> <li>■ Storage Drive</li> <li>■ Wireless Mouse</li> </ul>
USB device family	No	Examples include the following: <ul style="list-style-type: none"> <li>■ Security</li> <li>■ Human Interface Device</li> <li>■ Imaging</li> </ul>
USB device usage count	No	(Number of times the device was shared)

## Data Collected by VMware

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

**Table 8-23.** Client Data Collected for the Customer Experience Improvement Program

Description	Field name	Is This Field Made Anonymous ?	Example Value
Company that produced the application	<client-vendor>	No	VMware
Product name	<client-product>	No	
Client product version	<client-version>	No	4.4.0-build_number
Client binary architecture	<client-arch>	No	Examples include the following values: <ul style="list-style-type: none"> <li>■ browser</li> <li>■ arm</li> </ul>

**Table 8-23.** Client Data Collected for the Customer Experience Improvement Program (Continued)

<b>Description</b>	<b>Field name</b>	<b>Is This Field Made Anonymous ?</b>	<b>Example Value</b>
Native architecture of the browser	<browser-arch>	No	Examples include the following values: <ul style="list-style-type: none"> <li>■ Win32</li> <li>■ Win64</li> <li>■ MacIntel</li> <li>■ iPad</li> </ul>
Browser user agent string	<browser-user-agent>	No	Examples include the following values: <ul style="list-style-type: none"> <li>■ Mozilla/5.0 (Windows NT 6.1; WOW64)</li> <li>■ AppleWebKit/703.00 (KHTML, like Gecko)</li> <li>■ Chrome/3.0.1750</li> <li>■ Safari/703.00</li> <li>■ Edge/13.10586</li> </ul>
Browser's internal version string	<browser-version>	No	Examples include the following values: <ul style="list-style-type: none"> <li>■ 7.0.3 (for Safari),</li> <li>■ 44.0 (for Firefox)</li> <li>■ 13.10586 (for Edge)</li> </ul>
Browser's core implementation	<browser-core>	No	Examples include the following values: <ul style="list-style-type: none"> <li>■ Chrome</li> <li>■ Safari</li> <li>■ Firefox</li> <li>■ Internet Explorer</li> <li>■ Edge</li> </ul>
Whether the browser is running on a handheld device	<browser-is-handheld>	No	true

# Managing View Composer Linked-Clone Desktop Virtual Machines

# 9

You can update View Composer linked-clone desktop machines, reduce the size of their operating system data, and rebalance the machines among datastores. You also can manage the persistent disks associated with linked clones.

This chapter includes the following topics:

- [“Reduce Linked-Clone Size with Machine Refresh,”](#) on page 159
- [“Update Linked-Clone Desktops,”](#) on page 161
- [“Rebalance Linked-Clone Virtual Machines,”](#) on page 165
- [“Manage View Composer Persistent Disks,”](#) on page 168

## Reduce Linked-Clone Size with Machine Refresh

A machine refresh operation restores the operating system disk of each linked clone to its original state and size, reducing storage costs.

If possible, schedule refresh operations during off-peak hours.

For guidelines, see [“Machine Refresh Operations,”](#) on page 160.

### Prerequisites

- Decide when to schedule the refresh operation. By default, View Composer starts the operation immediately.

You can schedule only one refresh operation at a time for a given set of linked clones. You can schedule multiple refresh operations if they affect different linked clones.

- Decide whether to force all users to log off as soon as the operation begins or wait for each user to log off before refreshing that user's linked-clone desktop.

If you force users to log off, View notifies users before they are disconnected and allows them to close their applications and log off.

If you force users to log off, the maximum number of concurrent refresh operations on remote desktops that require logoffs is half the value of the **Max concurrent View Composer maintenance operations** setting. For example, if this setting is configured as 24 and you force users to log off, the maximum number of concurrent refresh operations on remote desktops that require logoffs is 12.

- If your deployment includes replicated View Connection Server instances, verify that all instances are the same version.

### Procedure

- 1 In View Administrator, select **Catalog > Desktop Pools**.

- 2 Select the desktop pool to refresh by double-clicking the pool ID in the left column.
- 3 Choose whether to refresh multiple virtual machines or a single virtual machine.

Option	Action
<b>To refresh all virtual machines in the desktop pool</b>	a In View Administrator, select <b>Catalog &gt; Desktop Pools</b> .
	b Select the desktop pool to refresh by double-clicking the pool ID in the left column.
	c On the <b>Inventory</b> tab, click <b>Machines</b> .
	d Use the Ctrl or Shift key to select all the machine IDs in the left column.
	e Select <b>Refresh</b> from the <b>View Composer</b> drop-down menu.
<b>To refresh a single virtual machine</b>	a In View Administrator, select <b>Resources &gt; Machines</b> .
	b Select the machine to refresh by double-clicking the machine ID in the left column.
	c On the <b>Summary</b> tab, select <b>Refresh</b> from the <b>View Composer</b> drop-down menu.

- 4 Follow the wizard instructions.

The OS disks are reduced to their original size.

In vCenter Server, you can monitor the progress of the refresh operation on the linked-clone virtual machines.

In View Administrator, you can monitor the operation by selecting **Catalog > Desktop Pools**, double-clicking the pool ID, and clicking the **Tasks** tab. You can click **Cancel task**, **Pause task**, or **Resume task** to terminate a task, suspend a task, or resume a suspended task.

## Machine Refresh Operations

As users interact with linked clones, the clones' OS disks grow. A machine refresh operation restores the OS disks to their original state and size, reducing storage costs.

A refresh operation does not affect View Composer persistent disks.

A linked clone uses less storage space than the parent virtual machine, which contains the complete OS data. However, a clone's OS disk expands each time data is written to it from within the guest operating system.

When View Composer creates a linked clone, it takes a snapshot of the clone's OS disk. The snapshot uniquely identifies the linked-clone virtual machine. A refresh operation reverts the OS disk to the snapshot.

View Composer can refresh a linked clone in as little as half the time it takes to delete and recreate the clone.

Apply these guidelines to refresh operations:

- You can refresh a desktop pool on demand, as a scheduled event, or when the OS data reaches a specified size.

You can schedule only one refresh operation at a time for a given set of linked clones. If you start a refresh operation immediately, the operation overwrites any previously scheduled task.

You can schedule multiple refresh operations if they affect different linked clones.

Before you schedule a new refresh operation, you must cancel any previously scheduled task.

- You can refresh dedicated-assignment and floating-assignment pools.
- A refresh can only occur when users are disconnected from their linked-clone desktops.

- A refresh preserves the unique computer information set up by QuickPrep or Sysprep. You do not need to rerun Sysprep after a refresh to restore the SID or the GUIDs of third-party software installed in the system drive.
- After you recompose a linked clone, Horizon 7 takes a new snapshot of the linked clone's OS disk. Future refresh operations restore the OS data to that snapshot, not the one originally taken when the linked clone was first created.

If you use native NFS snapshot (VAAI) technology to generate linked clones, certain vendors' NAS devices take snapshots of the replica disk when they refresh the linked clones' OS disks. These NAS devices do not support taking direct snapshots of each clone's OS disk.

- You can set a minimum number of ready, provisioned desktops that remain available for users to connect to during the refresh operation. See "Keeping Linked-Clone Desktops Provisioned and Ready During View Composer Operations" in the *Setting Up Virtual Desktops in Horizon 7* document.

---

**NOTE** You can slow the growth of linked clones by redirecting their paging files and system temp files to a temporary disk. When a linked clone is powered off, Horizon 7 replaces the temporary disk with a copy of the original temporary disk that View Composer created with the linked-clone pool. This operation shrinks the temporary disk to its original size.

You can configure this option when you create a linked-clone desktop pool.

---

## Update Linked-Clone Desktops

You can update linked-clone virtual machines by creating a new base image on the parent virtual machine and using the recompose feature to distribute the updated image to the linked clones.

- [Prepare a Parent Virtual Machine to Recompose Linked Clones](#) on page 161  
Before you recompose a linked-clone desktop pool, you must update the parent virtual machine that you used as a base image for the linked clones.
- [Recompose Linked-Clone Virtual Machines](#) on page 162  
Machine recomposition simultaneously updates all the linked-clone virtual machines anchored to a parent virtual machine.
- [Updating Linked Clones with Recomposition](#) on page 163  
In a recomposition, you can provide operating system patches, install or update applications, or modify the virtual machine hardware settings in all the linked clones in a desktop pool.
- [Correcting an Unsuccessful Recomposition](#) on page 164  
You can correct a recomposition that failed. You can also take action if you accidentally recompose linked clones using a different base image than the one you intended to use.

## Prepare a Parent Virtual Machine to Recompose Linked Clones

Before you recompose a linked-clone desktop pool, you must update the parent virtual machine that you used as a base image for the linked clones.

View Composer does not support recomposing linked clones that use one operating system to a parent virtual machine that uses a different operating system. For example, you cannot use a snapshot of a Windows 8 parent virtual machine to recompose a Windows 7 linked clone.

### Procedure

- 1 In vCenter Server, update the parent virtual machine for the recomposition.
  - Install OS patches or service packs, new applications, application updates, or make other changes in the parent virtual machine.
  - Alternatively, prepare another virtual machine to be selected as the new parent during the recomposition.
- 2 In vCenter Server, power off the updated or new parent virtual machine.
- 3 In vCenter Server, take a snapshot of the parent virtual machine.

### What to do next

Recompose the linked-clone desktop pool.

## Recompose Linked-Clone Virtual Machines

Machine recomposition simultaneously updates all the linked-clone virtual machines anchored to a parent virtual machine.

If possible, schedule recompositions during off-peak hours.

### Prerequisites

- Verify that you have a snapshot of the parent virtual machine. See [“Prepare a Parent Virtual Machine to Recompose Linked Clones,”](#) on page 161.
- Familiarize yourself with the recomposition guidelines. See [“Updating Linked Clones with Recomposition,”](#) on page 163.
- Decide when to schedule the recomposition. By default, View Composer starts the recomposition immediately.

You can schedule only one recomposition at a time for a given set of linked clones. You can schedule multiple recompositions if they affect different linked clones.

- Decide whether to force all users to log off as soon as the recomposition begins or wait for each user to log off before recomposing that user's linked-clone desktop.

If you force users to log off, Horizon 7 notifies users before they are disconnected and allows them to close their applications and log off.

- Decide whether to stop provisioning at first error. If you select this option and an error occurs when View Composer provisions a linked clone, provisioning stops for all clones in the desktop pool. You can select this option to ensure that resources such as storage are not consumed unnecessarily.

Selecting the **Stop at first error** option does not affect customization. If a customization error occurs on a linked clone, other clones continue to be provisioned and customized.

- Verify that provisioning for the desktop pool is enabled. When desktop pool provisioning is disabled, Horizon 7 stops the desktops from being customized after they are recomposed.
- If your deployment includes replicated Horizon Connection Server instances, verify that all instances are the same version.

## Procedure

- 1 Choose whether to recompose the whole desktop pool or a single machine.

Option	Action
<b>To recompose all virtual machines in the desktop pool</b>	<ol style="list-style-type: none"> <li>a In Horizon Administrator, select <b>Catalog &gt; Desktop Pools</b>.</li> <li>b Select the desktop pool to recompose by double-clicking the pool ID in the left column.</li> <li>c On the <b>Inventory</b> tab, click <b>Machines</b>.</li> <li>d Use the Ctrl or Shift keys to select all the machine IDs in the left column.</li> <li>e Select <b>Recompose</b> from the <b>View Composer</b> drop-down menu.</li> </ol>
<b>To recompose selected virtual machines</b>	<ol style="list-style-type: none"> <li>a In Horizon Administrator, select <b>Resources &gt; Machines</b>.</li> <li>b Select the machine to recompose by double-clicking the machine ID in the left column.</li> <li>c On the <b>Summary</b> tab, select <b>Recompose</b> from the <b>View Composer</b> drop-down menu.</li> </ol>

- 2 Follow the wizard instructions.

You can select a new virtual machine to be used as the parent virtual machine for the desktop pool.

On the Ready to Complete page, you can click **Show Details** to display the linked-clone desktops that will be recomposed.

The linked-clone virtual machines are refreshed and updated. The OS disks are reduced to their original size.

In a dedicated-assignment pool, unassigned linked clones are deleted and recreated. The specified number of spare virtual machines is maintained.

In a floating-assignment pool, all selected linked clones are recomposed.

In vCenter Server, you can monitor the progress of the recomposition on the linked-clone virtual machines.

In Horizon Administrator, you can monitor the operation by clicking **Catalog > Desktop Pools**, double-clicking the pool ID, and clicking the **Tasks** tab. You can click **Cancel task**, **Pause task**, or **Resume task** to terminate a task, suspend a task, or resume a suspended task.

**NOTE** If you used a Sysprep customization specification to customize the linked clones when you created the desktop pool, new SIDs might be generated for the recomposed virtual machines. For details, see "Recomposing Linked Clones Customized with Sysprep" in the *Setting Up Virtual Desktops in Horizon 7* document.

## Updating Linked Clones with Recomposition

In a recomposition, you can provide operating system patches, install or update applications, or modify the virtual machine hardware settings in all the linked clones in a desktop pool.

To recompose linked-clone virtual machines, you update the parent virtual machine in vCenter Server or select a different virtual machine to become the new parent. Next, you take a snapshot of the new parent virtual machine configuration.

You can change the parent virtual machine without affecting the linked clones because they are linked to the replica, not directly to the parent.

You then initiate the recomposition, selecting the snapshot to be used as the new base image for the desktop pool. View Composer creates a new replica, copies the reconfigured OS disk to the linked clones, and anchors the linked clones to the new replica.

The recomposition also refreshes the linked clones, reducing the size of their OS disks.

Desktop recompositions do not affect View Composer persistent disks.

Apply these guidelines to recompositions:

- You can recompose dedicated-assignment and floating-assignment desktop pools.
- You can recompose a desktop pool on demand or as a scheduled event.

You can schedule only one recomposition at a time for a given set of linked clones. Before you can schedule a new recomposition, you must cancel any previously scheduled task or wait until the previous operation is completed. Before you can start a new recomposition immediately, you must cancel any previously scheduled task.

You can schedule multiple recompositions if they affect different linked clones.

- You can recompose selected linked clones or all linked clones in a desktop pool.
- When different linked clones in a desktop pool are derived from different snapshots of the base image or from different base images, the desktop pool includes more than one replica.
- A recomposition can only occur when users are logged off of their linked-clone desktops.
- You cannot recompose linked clones that use one operating system to a new or updated parent virtual machine that uses a different operating system.
- You cannot recompose linked clones to a lower hardware version than their current version. For example, you cannot recompose hardware version 8 clones to a parent virtual machine that is hardware version 7.
- You can set a minimum number of ready, provisioned desktops that remain available for users to connect to during the recompose operation. See "Keeping Linked-Clone Desktops Provisioned and Ready During View Composer Operations" in the *Setting Up Virtual Desktops in Horizon 7* document.

---

**Note** If you used a Sysprep customization specification to customize the linked clones when you created the desktop pool, new SIDs might be generated for the recomposed virtual machines. For details, see "Recomposing Linked Clones Customized with Sysprep" in the *Setting Up Virtual Desktops in Horizon 7* document.

---

## Correcting an Unsuccessful Recomposition

You can correct a recomposition that failed. You can also take action if you accidentally recompose linked clones using a different base image than the one you intended to use.

### Problem

The virtual machines are in an erroneous or outdated state as a result of an unsuccessful recomposition.

### Cause

A system failure or problem might have occurred on the vCenter Server host, in vCenter Server, or on a datastore during the recomposition.

Alternatively, the recomposition might have used a virtual-machine snapshot with a different operating system than the operating system of the original parent virtual machine. For example, you might have used a Windows 8 snapshot to recompose Windows 7 linked clones.

### Solution

- 1 Select the snapshot that was used in the last successful recomposition.

You can also select a new snapshot to update the linked clones to a new state.

The snapshot must use the same operating system as the original parent virtual machine's snapshot.

- 2 Recompose the desktop pool again.

View Composer creates a base image from the snapshot and recreates the linked-clone OS disks.

View Composer persistent disks that contain user data and settings are preserved during the recomposition.

Depending on the conditions of the incorrect recomposition, you might refresh or rebalance the linked clones instead of or in addition to recomposing them.

---

**NOTE** If you do not configure View Composer persistent disks, all recompositions delete user-generated changes in the linked-clone virtual machines.

---

## Rebalance Linked-Clone Virtual Machines

A rebalance operation evenly redistributes linked-clone virtual machines among available datastores.

You can also use the rebalance operation to migrate linked-clone virtual machines to another datastore. Do not use vSphere Client or vCenter Server to migrate or manage linked-clone virtual machines. See [“Migrate Linked-Clone Virtual Machines to Another Datastore,”](#) on page 167.

If possible, schedule rebalance operations during off-peak hours.

For guidelines, see [“Rebalancing Linked Clones Among Logical Drives,”](#) on page 166.

### Prerequisites

- Familiarize yourself with the rebalance operation. See [“Rebalancing Linked Clones Among Logical Drives,”](#) on page 166.

- Decide when to schedule the rebalance operation. By default, View Composer starts the operation immediately.

You can schedule only one rebalance operation at a time for a given set of linked clones. You can schedule multiple rebalance operations if they affect different linked clones.

- Decide whether to force all users to log off as soon as the operation begins or wait for each user to log off before rebalancing that user's linked-clone desktop.

If you force users to log off, View notifies users before they are disconnected and allows them to close their applications and log off.

If you force users to log off, the maximum number of concurrent rebalance operations on remote desktops that require logoffs is half the value of the **Max concurrent View Composer maintenance operations** setting. For example, if this setting is configured as 24 and you force users to log off, the maximum number of concurrent rebalance operations on remote desktops that require logoffs is 12.

- Verify that provisioning for the desktop pool is enabled. When pool provisioning is disabled, View stops the virtual machines from being customized after they are rebalanced.
- If your deployment includes replicated View Connection Server instances, verify that all instances are the same version.

## Procedure

- 1 Choose whether to rebalance the whole pool or a single virtual machine.

Option	Action
<b>To rebalance all virtual machines in the pool</b>	a In View Administrator, select <b>Catalog &gt; Desktop Pools</b> .
	b Select the pool to rebalance by double-clicking the pool ID in the left column.
	c On the <b>Inventory</b> tab, click <b>Machines</b> .
	d Use the Ctrl or Shift keys to select multiple all the machine IDs in the left column.
	e Select <b>Rebalance</b> from the <b>View Composer</b> drop-down menu.
<b>To rebalance a single virtual machine</b>	a In View Administrator, select <b>Resources &gt; Machines</b> .
	b Select the machine to rebalance by double-clicking the machine ID in the left column.
	c On the <b>Summary</b> tab, select <b>Rebalance</b> from the View Composer drop-down menu.

- 2 Follow the wizard instructions.

The linked-clone virtual machines are refreshed and rebalanced. The OS disks are reduced to their original size.

In View Administrator, you can monitor the operation by selecting **Catalog > Desktop Pools**, double-clicking the pool ID, and clicking the **Tasks** tab. You can click **Cancel task**, **Pause task**, or **Resume task** to terminate a task, suspend a task, or resume a suspended task.

## Rebalancing Linked Clones Among Logical Drives

A rebalance operation evenly redistributes linked-clone virtual machines among available logical drives. It saves storage space on overloaded drives and ensures that no drives are underused.

When you create large linked-clone desktop pools and use multiple Logical Unit Numbers (LUNs), the space might not be used efficiently if the initial sizing was inaccurate. If you set an aggressive storage overcommit level, the linked clones can grow quickly and consume all the free space on the datastore.

When the virtual machines use 95% of the space on the datastore, Horizon 7 generates a warning log entry.

The rebalance also refreshes the linked clones, reducing the size of their OS disks. It does not affect View Composer persistent disks.

Apply these guidelines to rebalances:

- You can rebalance dedicated-assignment and floating-assignment desktop pools.
- You can rebalance selected linked clones or all clones in a pool.
- You can rebalance a desktop pool on demand or as a scheduled event.

You can schedule only one rebalance operation at a time for a given set of linked clones. If you start a rebalance operation immediately, the operation overwrites any previously scheduled task.

You can schedule multiple rebalance operations if they affect different linked clones.

Before you schedule a new rebalance operation, you must cancel any previously scheduled task.

- You can only rebalance virtual machines in the Available, Error, or Customizing state with no schedules or pending cancellations.
- As a best practice, do not mix linked-clone virtual machines with other types of virtual machines on the same datastore. This way View Composer can rebalance all the virtual machines on the datastore.

- If you edit a pool and change the host or cluster and the datastores on which linked clones are stored, you can only rebalance the linked clones if the newly selected host or cluster has full access to both the original and the new datastores. All hosts in the new cluster must have access to the original and new datastores.

For example, you might create a linked-clone desktop pool on a standalone host and select a local datastore to store the clones. If you edit the desktop pool and select a cluster and a shared datastore, a rebalance operation will fail because the hosts in the cluster cannot access the original, local datastore.

- You can set a minimum number of ready, provisioned virtual machines that remain available for users to connect to during the rebalance operation. See "Keeping Linked-Clone Desktops Provisioned and Ready During View Composer Operations" in the *Setting Up Virtual Desktops in Horizon 7* document.

---

**IMPORTANT** If you use a Virtual SAN datastore, you can use the rebalance operation only to migrate all the virtual machines in a desktop pool from a Virtual SAN datastore to some other type of datastore, or the reverse. If a desktop pool uses a Virtual SAN datastore, Virtual SAN provides the load balancing functionality and optimizes the use of resources across the ESXi cluster.

---

## Migrate Linked-Clone Virtual Machines to Another Datastore

To migrate linked-clone virtual machines from one set of datastores to another, use the rebalance operation.

When you use rebalance, View Composer manages the movement of the linked clones between datastores. View Composer ensures that the linked clones' access to the replica is maintained during and after the rebalance operation. If necessary, View Composer creates an instance of the replica on the destination datastore.

---

**NOTE** Do not use vSphere Client or vCenter Server to migrate or manage linked-clone virtual machines. Do not use Storage vMotion to migrate linked-clone virtual machines to other datastores.

---

### Prerequisites

Familiarize yourself with the rebalance operation. See "[Rebalance Linked-Clone Virtual Machines](#)," on page 165 and "[Rebalancing Linked Clones Among Logical Drives](#)," on page 166.

### Procedure

- 1 In View Administrator, select **Catalog > Desktop Pools**, select the desktop pool that you want to migrate, and click **Edit**.
- 2 On the **vCenter Settings** tab, scroll down to **Datastores** and click **Browse**.
- 3 On the Select Linked Clone Datastores page, deselect the datastores that currently store the linked clones, select the destination datastores, and click **OK**.
- 4 In the Edit window, click **OK**.
- 5 On the Desktop Pools page, select the pool by double-clicking the pool ID in the left column.
- 6 Select **Rebalance** from the **View Composer** drop-down menu and follow the wizard instructions to rebalance the linked-clone virtual machines.

The linked-clone virtual machines are refreshed and migrated to the destination datastores.

## Filenames of Linked-Clone Disks After a Rebalance Operation

When you rebalance linked-clone virtual machines, vCenter Server changes the filenames of View Composer persistent disks and disposable-data disks in linked clones that are moved to a new datastore.

The original filenames identify the disk type. The renamed disks do not include the identifying labels.

An original persistent disk has a filename with a user-disk label: `desktop_name-vdm-user-disk-D-ID.vmdk`.

An original disposable-data disk has a filename with a disposable label: *desktop\_name-vdm-disposable-ID.vmdk*.

After a rebalance operation moves a linked clone to a new datastore, vCenter Server uses a common filename syntax for both types of disks: *desktop\_name\_n.vmdk*.

## Manage View Composer Persistent Disks

You can detach a View Composer persistent disk from a linked-clone virtual machine and attach it to another linked clone. This feature lets you manage user information separately from linked-clone virtual machines.

### View Composer Persistent Disks

With View Composer, you can configure OS data and user information on separate disks in linked-clone virtual machines. View Composer preserves the user information on the persistent disk when the OS data is updated, refreshed, or rebalanced.

A View Composer persistent disk contains user settings and other user-generated data. You create persistent disks when you create a linked-clone desktop pool. See "Worksheet for Creating a Linked-Clone Desktop Pool" in the *Setting Up Virtual Desktops in Horizon 7* document.

You can detach a persistent disk from its linked-clone virtual machine and store the disk on its original datastore or another datastore. After you detach the disk, the linked-clone virtual machine is deleted. A detached persistent disk is no longer associated with any virtual machine.

You can use several methods to attach a detached persistent disk to another linked-clone virtual machine. This flexibility has several uses:

- When a linked clone is deleted, you can preserve the user data.
- When an employee leaves the company, another employee can access the departing employee's user data.
- A user who has multiple remote desktops can consolidate the user data on a single remote desktop.
- If a virtual machine becomes inaccessible in vCenter Server, but the persistent disk is intact, you can import the persistent disk and create a new linked clone using the disk.

---

**NOTE** Persistent disks must be reconnected to the operating system that was used when they were created. For example, you cannot detach a persistent disk from a Windows 7 linked clone and recreate or attach the persistent disk to a Windows 8 linked clone.

Horizon 7 can manage persistent disks from linked-clone pools that were created in View 4.5 or later. Persistent disks that were created in earlier versions of Horizon 7 cannot be managed and do not appear on the Persistent Disks page in Horizon Administrator.

---

### Detach a View Composer Persistent Disk

When you detach a View Composer persistent disk from a linked-clone virtual machine, the disk is stored and the linked clone is deleted. By detaching a persistent disk, you can store and reuse user-specific information with another virtual machine.

#### Procedure

- 1 In View Administrator, select **Resources > Persistent Disks**.
- 2 Select the persistent disk to detach and click **Detach**.

- 3 Choose where to store the persistent disk.

Option	Description
<b>Use current datastore</b>	Store the persistent disk on the datastore where it is currently located.
<b>Use the following datastore</b>	<p>Select a new datastore on which to store the persistent disk. Click <b>Browse</b>, click the down arrow, and select a new datastore from the <b>Choose a Datastore</b> menu.</p> <p>You cannot select a local datastore to store a detached persistent disk. You must use a shared datastore or Virtual SAN datastore.</p> <p>If the persistent disk was originally stored on a Virtual SAN datastore, you can select a Virtual SAN or non-Virtual SAN datastore to store the detached persistent disk. Similarly, if the persistent disk was stored on non-Virtual SAN, you can detach the disk on a non-Virtual SAN or Virtual SAN datastore.</p>

The View Composer persistent disk is saved on the datastore. The linked-clone virtual machine is deleted and does not appear in View Administrator.

## Attach a View Composer Persistent Disk to Another Linked Clone

You can attach a detached persistent disk to another linked-clone virtual machine. Attaching a persistent disk makes the user settings and information in the disk available to the user of the other virtual machine.

You attach a detached persistent disk as a secondary disk on the selected linked-clone virtual machine. The new user of the linked clone has access to the secondary disk and to the existing user information and settings.

You cannot attach a persistent disk that is stored on a non-Virtual SAN datastore to a virtual machine that is stored on a Virtual SAN datastore. Similarly, you cannot attach a disk that is stored on Virtual SAN to a virtual machine that is stored on non-Virtual SAN. View Administrator prevents you from selecting virtual machines that span Virtual SAN and non-Virtual SAN datastores.

To move a detached persistent disk from non-Virtual SAN to Virtual SAN, you can recreate the disk on a virtual machine that is stored on a non-Virtual SAN datastore and rebalance the virtual machine's desktop pool to a Virtual SAN datastore. See [“Recreate a Linked Clone With a Detached Persistent Disk,”](#) on page 170.

### Prerequisites

- Verify that the selected virtual machine uses the same operating system as the linked clone in which the persistent disk was created.

### Procedure

- 1 In View Administrator, select **Resources > Persistent Disks**.
- 2 On the **Detached** tab, select the persistent disk and click **Attach**.
- 3 Select a linked-clone virtual machine to which to attach the persistent disk.
- 4 Select **Attach as a secondary disk**.
- 5 Click **Finish**.

### What to do next

Make sure that the user of the linked clone has sufficient privileges to use the attached secondary disk. For example, if the original user had certain access permissions on the persistent disk, and the persistent disk is attached as drive D on the new linked clone, the new user of the linked clone must have the original user's access permissions on drive D.

Log in to the linked clone's guest operating system as an administrator and assign appropriate privileges to the new user.

## Edit a View Composer Persistent Disk's Pool or User

You can assign a detached View Composer persistent disk to a new desktop pool or user if the original desktop pool or user was deleted from View.

A detached persistent disk is still associated with its original desktop pool and user. If the desktop pool or user is deleted from View, you cannot use the persistent disk to recreate a linked-clone virtual machine.

By editing the desktop pool and user, you can use the detached persistent disk to recreate a virtual machine in the new desktop pool. The virtual machine is assigned to the new user.

You can select a new desktop pool, a new user, or both.

### Prerequisites

- Verify that the persistent disk's desktop pool or user was deleted from View.
- Verify that the new desktop pool uses the same operating system as the desktop pool in which persistent disk was created.

### Procedure

- 1 In View Administrator, select **Resources > Persistent Disks**
- 2 Select the persistent disk for which the user or desktop pool has been deleted and click **Edit**.
- 3 (Optional) Select a linked-cloned desktop pool from the list.
- 4 (Optional) Select a user for the persistent disk.

You can browse your Active Directory for the domain and username.

### What to do next

Recreate a linked-clone virtual machine with the detached persistent disk.

## Recreate a Linked Clone With a Detached Persistent Disk

When you detach a View Composer persistent disk, the linked clone is deleted. You can give the original user access to the detached user settings and information by recreating the linked-clone virtual machine from the detached disk.

---

**NOTE** If you recreate a linked-clone virtual machine in a desktop pool that has reached its maximum size, the recreated virtual machine is still added to the desktop pool. The desktop pool grows larger than the specified maximum size.

---

If a persistent disk's original desktop pool or user was deleted from View, you can assign a new one to the persistent disk. See [“Edit a View Composer Persistent Disk's Pool or User,”](#) on page 170.

View does not support recreating a virtual machine with a persistent disk that is stored on a non-Virtual SAN datastore if the new virtual machine is stored on a Virtual SAN datastore. Similarly, if the persistent disk is stored on Virtual SAN, View does not support recreating a virtual machine on non-Virtual SAN.

To move a detached persistent disk from non-Virtual SAN to Virtual SAN, you can recreate the disk on a virtual machine that is stored on a non-Virtual SAN datastore and rebalance the virtual machine's desktop pool to a Virtual SAN datastore.

#### Procedure

- 1 In View Administrator, select **Resources > Persistent Disks**.
- 2 On the **Detached** tab, select the persistent disk and click **Recreate Machine**.  
You can select multiple persistent disks to recreate a linked-clone virtual machine for each disk.
- 3 Click **OK**.

View creates a linked-clone virtual machine for each persistent disk you select and adds the virtual machine to the original desktop pool.

The persistent disks remain on the datastore where they were stored.

## Restore a Linked Clone by Importing a Persistent Disk from vSphere

If a linked-clone virtual machine becomes inaccessible in View, you can restore the virtual machine if it was configured with a View Composer persistent disk. You can import the persistent disk from a vSphere datastore into View.

You import the persistent disk file as a detached persistent disk in View. You can either attach the detached disk to an existing virtual machine or recreate the original linked clone in View.

#### Procedure

- 1 In View Administrator, select **Resources > Persistent Disks**.
- 2 On the **Detached** tab, click **Import from vCenter**.
- 3 Select a vCenter Server instance.
- 4 Select the datacenter where the disk file is located.
- 5 Select a linked-clone desktop pool in which to create a new linked clone virtual machine with the persistent disk.
- 6 In the **Persistent Disk File** text box, click **Browse**, click the down arrow, and select a datastore from the **Choose a Datastore** menu.  
You cannot import a persistent disk from a local datastore. Only shared datastores are available.
- 7 Click the datastore name to display its disk storage files and virtual-machine files.
- 8 Select the persistent-disk file you want to import.
- 9 In the **User** text box, click **Browse**, select a user to assign to the virtual machine, and click **OK**.

The disk file is imported into View as a detached persistent disk.

#### What to do next

To restore the linked-clone virtual machine, you can recreate the original virtual machine or attach the detached persistent disk to another virtual machine.

For details, see [“Recreate a Linked Clone With a Detached Persistent Disk,”](#) on page 170 and [“Attach a View Composer Persistent Disk to Another Linked Clone,”](#) on page 169.

## Delete a Detached View Composer Persistent Disk

When you delete a detached persistent disk, you can remove the disk from View and leave it on the datastore or delete the disk from View and the datastore.

### Procedure

- 1 In View Administrator, select **Resources > Persistent Disks**.
- 2 On the **Detached** tab, select the persistent disk and click **Delete**.
- 3 Choose whether to delete the disk from the datastore or let it remain on the datastore after it is removed from View.

Option	Description
<b>Delete from disk</b>	After the deletion, the persistent disk no longer exists.
<b>Delete from View only</b>	After the deletion, the persistent disk is no longer accessible in View but remains on the datastore.

- 4 Click **OK**.

# Managing Desktop Pools, Machines, and Sessions

---

# 10

In View Administrator, you can manage desktop pools, virtual machine-based desktops, physical machine-based desktops, desktop sessions, and application sessions.

This chapter includes the following topics:

- [“Managing Instant-Clone Desktop Pools,”](#) on page 173
- [“Managing Desktop Pools,”](#) on page 174
- [“Managing Virtual Machine-Based Desktops,”](#) on page 183
- [“Managing Unmanaged Machines,”](#) on page 188
- [“Manage Published Desktop and Application Sessions,”](#) on page 191
- [“Export View Information to External Files,”](#) on page 191

## Managing Instant-Clone Desktop Pools

In View Administrator you can perform administrative tasks on a instant-clone desktop pool such as scheduling a push-image operation.

### Change the Image of an Instant-Clone Desktop Pool

You can change the image of an instant-clone desktop pool to push out changes or to revert to a previous image. You can select any snapshot from any virtual machine to be the new image.

#### Procedure

- 1 In Horizon Administrator, select **Catalog > Desktop Pools**
- 2 Double-click the pool ID.
- 3 Select **Push Image > Schedule**.

The Schedule Push Image window opens.

- 4 Follow the prompts.

You can schedule the task to start immediately or sometime in the future. For clones with user sessions, you can specify whether to force the users to log out or to wait. When the users log out, Horizon 7 recreates the clones.

- 5 On the Ready to Complete page, click **Show Details** to see the list of desktops in the pool.

After you initiate this operation, publishing of the new image starts immediately. For more information about publishing, see "Instant-Clone Desktop Pools" in the *Setting Up Virtual Desktops in Horizon 7* document. Recreating the clones starts at the time that you specify in the Schedule Push Image wizard.

## Monitor a Push-Image Operation

You can monitor the progress of a push-image operation on an instant-clone desktop pool in View Administrator.

### Procedure

- 1 In View Administrator, select **Catalog > Desktop Pools**.

- 2 Double-click the pool ID.

The **Summary** tab shows the current image and pending image information.

- 3 Click the **Tasks** tab.

The list of tasks that are associated with the push-image operation appears.

## Reschedule or Cancel a Push-Image Operation

You can reschedule or cancel a push-image operation on an instant-clone desktop pool in View Administrator.

### Procedure

- 1 In View Administrator, select **Catalog > Desktop Pools**.

- 2 Double-click the pool ID.

The **Summary** tab shows the current image and pending image information.

- 3 Select **Push Image > Reschedule** or **Push Image > Cancel**.

- 4 Follow the prompts.

If you cancel the push-image operation while clone creation is in progress, the clones that have the new image remain in the pool and the pool has a mix of clones, some with the new image and the others with the old image. To ensure that all the clones have the same image, you can remove all the clones. View recreates the clones with the same image.

## Managing Desktop Pools

In View Administrator you can perform administrative tasks on a desktop pool such as editing its properties, enabling, disabling, or deleting the pool.

### Edit a Desktop Pool

You can edit an existing desktop pool to configure settings such as the number of spare machines, datastores, and customization specifications.

#### Prerequisites

Familiarize yourself with the desktop pool settings that you can and cannot change after a desktop pool is created. See [“Modifying Settings in an Existing Desktop Pool,”](#) on page 175 and [“Fixed Settings in an Existing Desktop Pool,”](#) on page 177.

#### Procedure

- 1 In View Administrator, select **Catalog > Desktop Pools**.

- 2 Select a desktop pool and click **Edit**.

- 3 Click a tab in the Edit dialog box and reconfigure desktop pool options.

#### 4 Click **OK**.

If you change the image of an instant-clone desktop pool, the image publishing operation starts immediately. In View Administrator, the summary page for the desktop pool shows the state for the pending image as **Publishing – Infrastructure Change**.

If you change the cluster of an instant-clone desktop pool, new replica and parent VMs are created in the new cluster. You can initiate a push image using the same image to have new clones created in the new cluster. However, the template VM, which is used in the cloning process, remains in the old cluster. You can put the ESXi host that the template VM is on in maintenance mode but you cannot migrate the template VM. To completely remove all infrastructure VMs, including the template VM, from the old cluster, you can initiate a push image using a new image.

## Modifying Settings in an Existing Desktop Pool

After you create a desktop pool, you can change certain configuration settings.

**Table 10-1.** Editable Settings in an Existing Desktop Pool

Configuration Tab	Description
<b>General</b>	<p>Edit desktop pool-naming options and storage policy management settings. Storage policy management settings determine whether to use a Virtual SAN datastore. If you do not use Virtual SAN, you can select separate datastores for replica and OS disks.</p> <p><b>NOTE</b> For View Composer linked clones, if you change to using Virtual SAN, you must use a rebalance operation to migrate all virtual machines in the desktop pool to the Virtual SAN datastore.</p>
<b>Desktop Pool Settings</b>	<p>Edit machine settings such as the power policy, display protocol, and Adobe Flash settings. In Horizon 7.0, power policy is not supported for instant clones.</p>
<b>Provisioning Settings</b>	<p>Edit desktop pool provisioning options and add machines to the desktop pool.</p> <p>This tab is available for automated desktop pools only.</p>
<b>vCenter Settings</b>	<p>Edit the virtual machine template or default base image. Add or change the vCenter Server instance, ESXi host or cluster, datastores, and other vCenter features.</p> <p>The new values only affect virtual machines that are created after the settings are changed. The new settings do not affect existing virtual machines.</p> <p>This tab is available for automated desktop pools only.</p>
<b>Guest Customization</b>	<p>If Sysprep was selected, you can change the customization specification. In Horizon 7.0, Sysprep is not available to instant clones.</p> <p>If QuickPrep was selected, you can change the Active Directory domain and container and specify the power-off and post-synchronization scripts.</p> <p>If ClonePrep was selected, you can change the Active Directory container and specify the power-off and post-synchronization scripts. You cannot change the domain.</p> <p><b>NOTE</b> For instant clones, if you change the power-off or post-synchronization script name, or their parameters, and the new script exists in the current image, the new script is executed and the new parameters are used when a new clone is created. If the new script does not exist in the current image, you must select or create an image that has the new script and do a push image.</p> <p>For View Composer linked clones, if you change the power-off or post-synchronization script name, the change applies at the next recompose operation. However, changes to the power-off script parameters or the post-synchronization script parameters do apply to the clones that are created with the current snapshot.</p> <p>This tab is available for automated desktop pools only.</p>

**Table 10-1.** Editable Settings in an Existing Desktop Pool (Continued)

Configuration Tab	Description
<b>Advanced Storage &gt; Use View Storage Accelerator</b>	<p>If you select or deselect <b>Use View Storage Accelerator</b>, or reschedule when the View Storage Accelerator digest files are regenerated, the settings do affect existing virtual machines. If you modify View Storage Accelerator settings for an existing desktop pool, the changes do not take effect until the virtual machines in the desktop pool are powered off. See "Configure View Storage Accelerator for View Composer Linked Clones" in the <i>Setting Up Virtual Desktops in Horizon 7</i> document.</p> <p><b>NOTE</b> If you select <b>Use View Storage Accelerator</b> on an existing linked-clone desktop pool, and the replica was not previously enabled for View Storage Accelerator, this feature might not take effect right away. View Storage Accelerator cannot be enabled while the replica is in use. You can force View Storage Accelerator to be enabled by recomposing the desktop pool to a new parent virtual machine.</p> <p>This option is automatically enabled on instant clones.</p>
<b>Advanced Storage &gt; Reclaim VM disk space</b>	<p>If you select or deselect <b>Reclaim VM disk space</b>, or reschedule when the virtual machine disk space reclamation occurs, the new settings do affect existing virtual machines if they were created with space-efficient disks. See "Reclaim Disk Space on Linked-Clone Virtual Machines" in the <i>Setting Up Virtual Desktops in Horizon 7</i> document.</p> <p>This option does not apply to instant clones.</p>
<b>Advanced Storage &gt; Use native NFS snapshots (VAAD)</b>	<p>If you select or deselect <b>Use native NFS snapshots (VAAD)</b>, the new setting only affects virtual machines that are created after the settings are changed. You can change existing virtual machines to become native NFS snapshot clones by recomposing and, if needed, rebalancing the desktop pool. See "Using View Composer Array Integration with Native NFS Snapshot Technology" in the <i>Setting Up Virtual Desktops in Horizon 7</i> document.</p> <p>This option is not supported for instant clones.</p>
<b>Advanced Storage &gt; Transparent Page Sharing Scope</b>	<p>If you change the <b>Transparent Page Sharing Scope</b> setting, the new setting takes effect the next time the virtual machine is powered on.</p> <p>Select the level at which to allow transparent page sharing (TPS). The choices are <b>Virtual Machine</b> (the default), <b>Pool</b>, <b>Pod</b>, or <b>Global</b>. If you turn on TPS for all the machines in the pool, pod, or globally, the ESXi host eliminates redundant copies of memory pages that result if the machines use the same guest operating system or applications.</p> <p>Page sharing happens on the ESXi host. For example, if you enable TPS at the pool level but the pool is spread across multiple ESXi hosts, only virtual machines on the same host and within the same pool will share pages. At the global level, all machines managed by Horizon 7 on the same ESXi host can share memory pages, regardless of which pool the machines reside in.</p> <p><b>NOTE</b> The default setting is not to share memory pages among machines because TPS can pose a security risk. Research indicates that TPS could possibly be abused to gain unauthorized access to data in very limited configuration scenarios.</p> <p>This option is automatically enabled on instant clones.</p>

If you edit a instant-clone desktop pool to add or remove datastores, rebalancing of the VMs happens automatically when a new clone must be created, for example, when a user logs off or when you increase the size of the pool. If you want rebalancing to happen faster, take the following actions:

- If you remove a datastore, manually remove the desktops on that datastore so that the new desktops will be created on the remaining datastores.
- If you add a datastore, manually remove some desktops from the original datastores so that the new desktops will be created on the new datastore. You can also remove all desktops so that when they are recreated, they will be evenly distributed across the datastores.

## Fixed Settings in an Existing Desktop Pool

After you create a desktop pool, you cannot change certain configuration settings.

**Table 10-2.** Fixed Settings in an Existing Desktop Pool

Setting	Description
Pool type	After you create an automated, manual, or RDS desktop pool, you cannot change the pool type.
User assignment	You cannot switch between dedicated assignments and floating assignments.
Type of virtual machine	You cannot switch between full virtual machines and linked-clone virtual machines.
Pool ID	You cannot change the pool ID.
Machine-naming and provisioning method	To add virtual machines to a desktop pool, you must use the provisioning method that was used to create the pool. You cannot switch between specifying machine names manually and using a naming pattern. If you specify names manually, you can add names to the list of machine names. If you use a naming pattern, you can increase the maximum number of machines.
vCenter settings	You cannot change vCenter settings for existing virtual machines. You can change vCenter settings in the Edit dialog box, but the values affect only new virtual machines that are created after the settings are changed.
View Composer persistent disks	You cannot configure persistent disks after a linked-clone desktop pool is created without persistent disks.
View Composer customization method	After you customize a linked-clone desktop pool with QuickPrep or Sysprep, you cannot switch to the other customization method when you create or recompose virtual machines in the pool.

## Change the Size of an Automated Pool Provisioned by a Naming Pattern

When you provision an automated desktop pool by using a naming pattern, you can increase or decrease the size of the pool by changing the maximum number of machines.

### Prerequisites

- Verify that you provisioned the desktop pool by using a naming pattern. If you specify machine names manually, see [“Add Machines to an Automated Pool Provisioned by a List of Names,”](#) on page 178.
- Verify that the desktop pool is automated.

### Procedure

- 1 In View Administrator, select **Catalog > Desktop Pools**.
- 2 Select the desktop pool and click **Edit**.
- 3 On the **Provisioning Settings** tab, type the new number of machines in the desktop pool in the **Max number of machines** text box.

If you increase the desktop pool size, new machines can be added to the pool up to the maximum number.

If you decrease the size of a floating-assignment pool, unused machines are deleted. If more users are logged into the pool than the new maximum, the pool size decreases after users log off.

If you decrease the size of a dedicated-assignment pool, unassigned machines are deleted. If more users are assigned to machines than the new maximum, the pool size decreases after you unassign users.

---

**NOTE** When you decrease the size of a desktop pool, the actual number of machines might be larger than **Max number of machines** if more users are currently logged in or assigned to machines than the value that is specified in **Max number of machines**.

---

## Add Machines to an Automated Pool Provisioned by a List of Names

To add machines to an automated desktop pool provisioned by manually specifying machine names, you provide another list of new machine names. This feature lets you expand a desktop pool and continue to use your company's naming conventions.

In Horizon 7.0, this feature is not supported for instant clones.

Follow these guidelines for manually adding machine names:

- Type each machine name on a separate line.
- A machine name can have up to 15 alphanumeric characters.
- You can add a user name to each machine entry. Use a comma to separate the user name from the machine name.

In this example, two machines are added. The second machine is associated with a user:

```
Desktop-001
Desktop-002,abccorp.com/jdoe
```

---

**NOTE** In a floating-assignment pool, you cannot associate user names with machine names. The machines are not dedicated to the associated users. In a floating-assignment pool, all machines that are not currently in use remain accessible to any user who logs in.

---

### Prerequisites

Verify that you created the desktop pool by manually specifying machine names. You cannot add machines by providing new machine names if you created the pool by providing a naming pattern.

### Procedure

- 1 Create a text file that contains the list of additional machine names.  
If you intend to add only a few machines, you can type the machine names directly in the Add Desktop Pool wizard. You do not have to create a separate text file.
- 2 In View Administrator, select **Catalog > Desktop Pools**.
- 3 Select the desktop pool to be expanded.
- 4 Click **Edit**.
- 5 Click the **Provisioning Settings** tab.
- 6 Click **Add Machines**.
- 7 Copy your list of machine names in the Enter Machine Names page and click **Next**.  
The Enter Machine Names wizard displays the machine list and indicates validation errors with a red **X**.

- 8 Correct invalid machine names.
  - a Place your cursor over an invalid name to display the related error message at the bottom of the page.
  - b Click **Back**.
  - c Edit the incorrect names and click **Next**.
- 9 Click **Finish**.
- 10 Click **OK**.

In vCenter Server, you can monitor the creation of the new virtual machines.

In View Administrator, you can view the machines as they are added to the desktop pool by selecting **Catalog > Desktop Pools**.

## Disable or Enable a Desktop Pool

When you disable a desktop pool, the pool is no longer presented to users and pool provisioning is stopped. Users have no access to the pool. After you disable a pool, you can enable it again.

You can disable a desktop pool to prevent users from accessing their remote desktops while you prepare the desktops for use. If a desktop pool is no longer needed, you can use the disable feature to withdraw the pool from active use without having to delete the desktop pool definition from View.

### Procedure

- 1 In View Administrator, select **Catalog > Desktop Pools**.
- 2 Select a desktop pool and change the status of the pool.

Option	Action
<b>Disable the pool</b>	Select <b>Disable Desktop Pool</b> from the <b>Status</b> drop-down menu.
<b>Enable the pool</b>	Select <b>Enable Desktop Pool</b> from the <b>Status</b> drop-down menu.

- 3 Click **OK**.

## Disable or Enable Provisioning in an Automated Desktop Pool

When you disable provisioning in an automated desktop pool, View stops provisioning new virtual machines for the pool. After you disable provisioning, you can enable provisioning again.

Before you change a desktop pool's configuration, you can disable provisioning to ensure that no new machines are created with the old configuration. You also can disable provisioning to prevent View from using additional storage when a pool is close to filling up the available space.

When provisioning is disabled in a linked-clone pool, View stops new machines from being provisioned and stops machines from being customized after they are recomposed or rebalanced.

### Procedure

- 1 In View Administrator, select **Catalog > Desktop Pools**.
- 2 Select a desktop pool and change the status of the pool.

Option	Action
<b>Disable provisioning</b>	Select <b>Disable Provisioning</b> from the <b>Status</b> drop-down menu.
<b>Enable provisioning</b>	Select <b>Enable Provisioning</b> from the <b>Status</b> drop-down menu.

- 3 Click **OK**.

## Configure Adobe Flash Quality and Throttling

You can set Adobe Flash quality and throttling modes to reduce the amount of bandwidth that is used by Adobe Flash content in remote desktops. This reduction can improve the overall browsing experience and make other applications that run in the remote desktop more responsive.

### Prerequisites

Familiarize yourself with Adobe Flash quality and throttling settings. See [“Adobe Flash Quality and Throttling,”](#) on page 180.

### Procedure

- 1 In View Administrator, select **Catalog > Desktop Pools**.
- 2 Select a desktop pool and click **Edit**.
- 3 On the **Desktop Pool Settings** tab, select a quality mode from the **Adobe Flash quality** menu and a throttling mode from the **Adobe Flash throttling** menu.
- 4 Click **OK**.

---

**NOTE** Adobe Flash bandwidth-reduction settings do not take effect until Horizon Client reconnects with the remote desktop.

---

## Adobe Flash Quality and Throttling

You can specify a maximum allowable level of quality for Adobe Flash content that overrides Web page settings. If Adobe Flash quality for a Web page is higher than the maximum level allowed, quality is reduced to the specified maximum. Lower quality results in more bandwidth savings.

To make use of Adobe Flash bandwidth-reduction settings, Adobe Flash must not be running in full screen mode.

[Table 10-3](#) shows the available Adobe Flash render-quality settings.

**Table 10-3.** Adobe Flash Quality Settings

Quality Setting	Description
<b>Do not control</b>	Quality is determined by Web page settings.
<b>Low</b>	This setting results in the most bandwidth savings.
<b>Medium</b>	This setting results in moderate bandwidth savings.
<b>High</b>	This setting results in the least bandwidth savings.

If no maximum level of quality is specified, the system defaults to a value of **Low**.

Adobe Flash uses timer services to update what is shown on the screen at a given time. A typical Adobe Flash timer interval value is between 4 and 50 milliseconds. By throttling, or prolonging, the interval, you can reduce the frame rate and thereby reduce bandwidth.

[Table 10-4](#) shows the available Adobe Flash throttling settings.

**Table 10-4.** Adobe Flash Throttling Settings

Throttling Setting	Description
Disabled	No throttling is performed. The timer interval is not modified.
Conservative	Timer interval is 100 milliseconds. This setting results in the lowest number of dropped frames.
Moderate	Timer interval is 500 milliseconds.
Aggressive	Timer interval is 2500 milliseconds. This setting results in the highest number of dropped frames.

Audio speed remains constant regardless of which throttling setting you select.

## Delete a Desktop Pool

When you delete a desktop pool, users can no longer launch new remote desktops in the pool.

Depending on the type of desktop pool, you have various options regarding how View handles persistent disks, vCenter Server full virtual machines, and users' active sessions.

By default, you can delete a desktop pool even if desktop machines exist in the pool. View does not give you a warning. You can configure View to not allow the deletion of a pool that contains desktop machines. For details, see [“Configure View to Disallow the Deletion of a Desktop Pool That Contains Desktop Machines,”](#) on page 182. If you configure the setting, you must delete all the machines in a desktop pool before you can delete the pool.

With an automated desktop pool of instant clones or View Composer linked clones, View always deletes the virtual machines from disk.

---

**IMPORTANT** Do not delete the virtual machines in vCenter Server before you delete a desktop pool with View Administrator. This action could put View components into an inconsistent state.

---

### Procedure

- 1 In View Administrator, select **Catalog > Desktop Pools**.
- 2 Select a desktop pool and click **Delete**.
- 3 Choose how to delete the desktop pool.

Pool	Options
<b>Automated desktop pool of instant clones or linked clones without persistent disks.</b>	No available options. View deletes all virtual machines from disk. Users' sessions to their remote desktops are terminated.
<b>Automated desktop pool of linked clones with persistent disks.</b>	<p>Choose whether to detach or delete the persistent disks when the linked-clone virtual machines are deleted.</p> <p>In both cases, View deletes all virtual machines from disk, and users' sessions to their remote desktops are terminated.</p> <p>If you detach a persistent disk, the linked-clone virtual machine that contained the persistent disk can be recreated, or the persistent disk can be attached to another virtual machine. You can store detached persistent disks in the same datastore or a different one. If you select a different datastore, you cannot store detached persistent disks on a local datastore. You must use a shared datastore.</p> <p>You can only detach persistent disks that were created in View 4.5 or later releases.</p>

Pool	Options
<b>Automated desktop pool of full virtual machines.</b>	Choose whether to keep or delete the virtual machines in vCenter Server.
<b>Manual desktop pool of vCenter Server virtual machines.</b>	
<b>RDS desktop pool.</b>	If there are users who are connected to their remote desktops, choose whether to keep users' sessions active or terminate them. Note that View Connection Server does not keep track of sessions that are kept active.
<b>Automated desktop pool of full virtual machines.</b>	
<b>Manual desktop pool.</b>	

When you delete a desktop pool, linked-clone virtual machines' computer accounts are removed from Active Directory. Full virtual machines' computer accounts remain in Active Directory. To remove these accounts, you must manually delete them from Active Directory.

If you delete an instant-clone desktop pool, it can take some time for View to delete the internal VMs from vCenter Server. Do not remove vCenter Server from View Administrator until you verify that all the internal VMs are deleted.

## Configure View to Disallow the Deletion of a Desktop Pool That Contains Desktop Machines

You can configure View to disallow the deletion of a desktop pool that contains desktop machines. By default, View allows the deletion of such a pool.

If you configure this setting, you must delete all the machines in a desktop pool before you can delete the pool.

### Prerequisites

See the Microsoft TechNet Web site for information on how to use the ADSI Edit utility on your Windows server.

### Procedure

- 1 Start the ADSI Edit utility on the View Connection Server host.
- 2 In the Connection Settings dialog box, select or connect to **DC=vdi,DC=vmware,DC=int**.
- 3 In the Computer pane, select or type **localhost:389** or the fully qualified domain name (FQDN) of the View Connection Server host followed by port 389.

For example: **localhost:389** or **mycomputer.mydomain.com:389**

- 4 On the object **CN=Common, OU=Global, OU=Properties**, edit the **pae-NameValuePair** attribute and add the value **cs-disableNonEmptyPoolDelete=1**.

The new setting takes effect immediately. You do not need to restart the View Connection Server service.

## Managing Virtual Machine-Based Desktops

A virtual machine-based desktop is a desktop that is from an automated desktop pool or a manual desktop pool that contains vCenter Server virtual machines.

### Assign a Machine to a User

In a dedicated-assignment pool, you can assign a user to be the owner of the virtual machine that hosts a remote desktop. Only the assigned user can log in and connect to the remote desktop.

View assigns machines to users in these situations.

- When you create a desktop pool and select the **Enable automatic assignment** setting.

---

**NOTE** If you select the **Enable automatic assignment** setting, you can still manually assign machines to users.

---

- When you create an automated pool, select the **Specify names manually** setting, and provide user names with the machine names.

If you do not select either setting in a dedicated-assignment pool, users do not have access to remote desktops. You must manually assign a machine to each user.

You can also use the `vdmdadmin` command to assign machines to users. See [“Assigning Dedicated Machines Using the -L Option,”](#) on page 260.

#### Prerequisites

- Verify that the remote desktop virtual machine belongs to a dedicated-assignment pool. In View Administrator, the desktop pool assignment appears in the Desktop Pool column the Machines page.

#### Procedure

- 1 In View Administrator, select **Resources > Machines**, or select **Catalog > Desktop Pools**, double-click a pool ID, and click the **Inventory** tab.
- 2 Select the machine.
- 3 Select **Assign User** from the **More Commands** drop-down menu.
- 4 Choose whether to find users or groups, select a domain, and type a search string in the **Name** or **Description** text box.
- 5 Select the user or group name and click **OK**.

### Unassign a User from a Dedicated Machine

In a dedicated-assignment pool, you can remove a machine assignment to a user.

You can also use the `vdmdadmin` command to remove a machine assignment to a user. See [“Assigning Dedicated Machines Using the -L Option,”](#) on page 260.

#### Procedure

- 1 In View Administrator, select **Resources > Machines** or select **Catalog > Desktop Pools**, double-click a pool ID, and click the **Inventory** tab.
- 2 Select the machine.
- 3 Select **Unassign User** from the **More Commands** drop-down menu.
- 4 Click **OK**.

The machine is available and can be assigned to another user.

## Customize Existing Machines in Maintenance Mode

After a desktop pool is created, you can customize, modify, or test individual machines by placing them in maintenance mode. When a machine is in maintenance mode, users cannot access the virtual-machine desktop.

You place existing machines in maintenance mode one at a time. You can remove multiple machines from maintenance mode in one operation.

When you create a desktop pool, you can start all the machines in the pool in maintenance mode if you specify machine names manually. For details, see "Customizing Desktops in Maintenance Mode" in the *Setting Up Virtual Desktops in Horizon 7* document.

In Horizon 7.0, this feature is not supported for instant clones.

### Procedure

- 1 In Horizon Administrator, select **Resources > Machines** or select **Catalog > Desktop Pools**, double-click a pool ID, and select the **Inventory** tab.
- 2 Select a machine.
- 3 Select **Enter Maintenance Mode** from the **More Commands** drop-down menu.
- 4 Customize, modify, or test the virtual-machine desktop.
- 5 Repeat [Step 2](#) through [Step 4](#) for all virtual machines that you want to customize.
- 6 Select the customized machines and select **Exit Maintenance Mode** from the **More Commands** drop-down menu.

The modified virtual-machine desktops are available to users.

## Monitor Virtual-Machine Desktop Status

You can quickly survey the status of virtual-machine desktops in your View deployment by using the View Administrator dashboard. For example, you can display all disconnected virtual machines or virtual machines that are in maintenance mode.

### Prerequisites

Familiarize yourself with the virtual machine states. See [“Status of vCenter Server Virtual Machines,”](#) on page 185.

### Procedure

- 1 In View Administrator, click **Dashboard**.
- 2 In the Machine Status pane, expand a status folder.

Option	Description
<b>Preparing</b>	Lists the machine states while the virtual machine is being provisioned, deleted, or in maintenance mode.
<b>Problem Machines</b>	Lists the machine error states.
<b>Prepared for use</b>	Lists the machine states when the virtual machine is ready for use.

- 3 Locate the machine status and click the hyperlinked number next to it.

The Machines page displays all virtual machines with the selected status.

## What to do next

You can click a machine name to see details about the virtual machine or click the View Administrator back arrow to return to the dashboard page.

## Status of vCenter Server Virtual Machines

Virtual machines that are managed by vCenter Server can be in various states of operation and availability. In Horizon Administrator, you can track the status of machines in the right-hand column of the Machines page.

Table 10-5 shows the operational state of virtual-machine desktops that are displayed in Horizon Administrator. A desktop can be in only one state at a time.

**Table 10-5.** Status of Virtual Machines That Are Managed by vCenter Server

Status	Description
Provisioning	The virtual machine is being provisioned.
Customizing	The virtual machine in an automated pool is being customized.
Deleting	The virtual machine is marked for deletion. Horizon 7 will delete the virtual machine soon.
Waiting for Agent	Horizon Connection Server is waiting to establish communication with View Agent or Horizon Agent on a virtual machine in a manual pool.
Maintenance mode	The virtual machine is in maintenance mode. Users cannot log in or use the virtual machine.
Startup	View Agent or Horizon Agent has started on the virtual machine, but other required services such as the display protocol are still starting. For example, View Agent cannot establish an RDP connection with client computers until RDP has finished starting. The agent startup period allows other processes such as protocol services to start up as well.
Agent disabled	This state can occur in two cases. First, in a desktop pool with the <b>Delete or refresh machine on logoff</b> or <b>Delete machine after logoff</b> setting enabled, a desktop session is logged out, but the virtual machine is not yet refreshed or deleted. Second, View Connection Server disables View Agent or Horizon Agent just before sending a request to power off the virtual machine. This state ensures that a new desktop session cannot be started on the virtual machine.
Agent unreachable	Horizon Connection Server cannot establish communication with View Agent or Horizon Agent on a virtual machine.
Invalid IP	The subnet mask registry setting is configured on the virtual machine, and no active network adapters have an IP address within the configured range.
Agent needs reboot	An Horizon 7 component was upgraded, and the virtual machine must be restarted to allow View Agent or Horizon Agent to operate with the upgraded component.
Protocol failure	A display protocol did not start before the View Agent or Horizon Agent startup period expired. <b>NOTE</b> View Administrator can display machines in a <b>Protocol failure</b> state when one protocol failed but other protocols started successfully. For example, the <b>Protocol failure</b> state might be displayed when HTML Access failed but PCoIP and RDP are working. In this case, the machines are available and Horizon Client devices can access them through PCoIP or RDP.
Domain failure	The virtual machine encountered a problem reaching the domain. The domain server was not accessible, or the domain authentication failed.

**Table 10-5.** Status of Virtual Machines That Are Managed by vCenter Server (Continued)

Status	Description
Already used	In a desktop pool with the <b>Delete or refresh machine on logoff</b> or <b>Delete machine after logoff</b> setting enabled, there is no session on the virtual machine, but the session was not logged off. This condition might occur if a virtual machine shuts down unexpectedly or the user resets the machine during a session. By default, when a virtual machine is in this state, Horizon 7 prevents any other Horizon Client devices from accessing the desktop.
Configuration error	The display protocol such as RDP or PCoIP is not enabled.
Provisioning error	An error occurred during provisioning.
Error	An unknown error occurred in the virtual machine.
Unassigned user connected	A user other than the assigned user is logged in to a virtual machine in a dedicated pool. For example, this state can occur if an administrator starts vSphere Client, opens a console on the virtual machine, and logs in.
Unassigned user disconnected	A user other than the assigned user is logged in and disconnected from a virtual machine in a dedicated-assignment pool.
Unknown	The virtual machine is in an unknown state.
Provisioned	The virtual machine is powered off or suspended.
Available	The virtual machine is powered on and ready for a connection. In a dedicated pool, the virtual machine is assigned to a user and will start when the user logs in.
Connected	The virtual machine is in a session and has a remote connection to the Horizon Client device.
Disconnected	The virtual machine is in a session, but it is disconnected from the Horizon Client device.
In progress	The virtual machine is in a transitional state during a maintenance operation.

While a machine is in a particular state, it can be subject to further conditions. Horizon Administrator displays these conditions as suffixes to the machine state. For example, Horizon Administrator might display the Customizing (missing) state.

[Table 10-6](#) shows these additional conditions.

**Table 10-6.** Machine Status Conditions

Condition	Description
Missing	The virtual machine is missing in vCenter Server. Typically, the virtual machine was deleted in vCenter Server, but the Horizon LDAP configuration still has a record of the machine.
Task halted	An instant clone task such as push image or a View Composer operation such as refresh, recompose, or rebalance was stopped. For details about troubleshooting a recompose operation, see <a href="#">“Correcting an Unsuccessful Recomposition,”</a> on page 164. For details about View Composer error states, see “View Composer Provisioning Errors” in the <i>Setting Up Virtual Desktops in Horizon 7</i> document. The Task halted condition applies to all virtual machines that were selected for the operation, but on which the operation has not yet started. Virtual machines in the pool that are not selected for the operation are not placed in the Task halted condition.

A machine state can be subject to both conditions, (missing, task halted), if a View Composer task was stopped and the virtual machine is missing in vCenter Server.

## Delete Virtual-Machine Desktops

When you delete a virtual-machine desktop, users can no longer access the desktop. A virtual-machine desktop is either a vCenter Server virtual machine or an unmanaged virtual machine.

Users in currently active sessions can continue to use full virtual-machine desktops if you keep the virtual machines in vCenter Server. After the users log off, they cannot access the deleted virtual-machine desktops.

With instant clones and linked-clone virtual machines, vCenter Server always deletes the virtual machines from disk.

---

**Note** Do not delete the virtual machines in vCenter Server before you delete virtual-machine desktops with View Administrator. This action could put View components into an inconsistent state.

---

### Procedure

- 1 In View Administrator, select **Resources > Machines**.
- 2 Select the **vCenter VMs** tab or the **Others** tab.
- 3 Select one or more machines and click **Remove**.
- 4 Choose how to delete the virtual-machine desktop.

Option	Description
<b>Pool that contains full virtual-machine desktops</b>	Choose whether to keep or delete the virtual machines in vCenter Server. If you delete the virtual machines from disk, users in active sessions are disconnected from their desktops. If you keep the virtual machines in vCenter Server, choose whether to let users in active sessions stay connected to their desktops or disconnect them.
<b>View Composer linked-clone pool with persistent disks</b>	Choose whether to detach or delete the persistent disks when the virtual-machine desktops are deleted. In both cases, vCenter Server deletes the linked-clone virtual machines from disk. Users in currently active sessions are disconnected from their remote desktops. If you detach a persistent disk, the linked-clone virtual machine that contained the persistent disk can be recreated, or the persistent disk can be attached to another virtual machine. You can store detached persistent disks in the same datastore or a different one. If you select a different datastore, you cannot store detached persistent disks on a local datastore. You must use a shared datastore. You can only detach persistent disks that were created in View 4.5 or later releases.
<b>Instant-clone pool and View Composer linked-clone pool without persistent disks</b>	vCenter Server deletes the linked-clone virtual machines from disk. Users in currently active sessions are disconnected from their remote desktops.

When you delete virtual-machine desktops, linked-clone virtual machine computer accounts are removed from Active Directory. Full virtual machine accounts remain in Active Directory. To remove these accounts, you must manually delete them from Active Directory.

## Recover Instant-Clone Desktops

When an instant-clone desktop is in an error state, you have the option to recover it. The desktop is recreated from the current base image.

### Procedure

- 1 In View Administrator, select **Catalog > Desktop Pools**, double-click a pool's ID, and click the **Inventory** tab.
- 2 Select one or more machines and click **Recover**.

## Managing Unmanaged Machines

In View Administrator, you can add and remove unmanaged machines from manual desktop pools and remove registered machines from View. Unmanaged machines include physical computers and virtual machines that are not managed by vCenter Server.

For information about deleting a desktop pool that contains unmanaged machines, see [“Delete a Desktop Pool,”](#) on page 181.

When you reconfigure a setting that affects an unmanaged machine, it can take up to 10 minutes for the new setting to take effect. For example, if you change the Message security mode in Global Settings or change the **Automatically logoff after disconnect** setting for a pool, View might take up to 10 minutes to reconfigure the affected unmanaged machines.

---

**NOTE** RDS hosts are also unmanaged machines, since they are not generated from a parent virtual machine or template and managed by vCenter Server. RDS hosts support session-based desktops and applications and are treated as a separate category. See [“Managing RDS Hosts,”](#) on page 199.

---

## Add an Unmanaged Machine to a Manual Pool

You can increase the size of a manual desktop pool by adding unmanaged machines to the pool.

### Prerequisites

Verify that Horizon Agent is installed on the unmanaged machine. For information about preparing an unmanaged machine, see "Install Horizon Agent on an Unmanaged Machine" in the *Setting Up Virtual Desktops in Horizon 7* document.

### Procedure

- 1 In Horizon Administrator, select **Catalog > Desktop Pools**.
- 2 Double-click the pool ID of the manual pool.
- 3 In the **Inventory** tab, click **Add**.
- 4 Select unmanaged machines from the Add Desktops window and click **OK**.

The unmanaged machines are added to the pool.

## Remove an Unmanaged Machine from a Manual Desktop Pool

You can reduce the size of a manual desktop pool by removing unmanaged machines from the pool.

### Procedure

- 1 In View Administrator, select **Catalog > Desktop Pools**.
- 2 Double-click the pool ID of the manual pool.

- 3 Select the **Inventory** tab.
- 4 Select the unmanaged machines to remove.
- 5 Click **Remove**.
- 6 If users are logged in to the unmanaged machine-based desktops, choose whether to terminate the sessions or let the sessions remain active.

Option	Description
<b>Leave active</b>	Active sessions remain until the user logs off. View Connection Server does not keep track of these sessions.
<b>Terminate</b>	Active sessions end immediately.

- 7 Click **OK**.

The unmanaged machines are removed from the pool.

## Remove Registered Machines from View

If you do not plan to use a registered machine again, you can remove it from View.

There are two types of registered machines in View: RDS Hosts and Others. Unmanaged machines are in the Others category. Unmanaged machines include physical computers and virtual machines that are not managed by vCenter Server. They are used to form manual desktop pools that do not contain vCenter Server virtual machines.

After you remove a registered machine, it becomes unavailable in View. To make the machine available again, you must reinstall Horizon Agent.

### Prerequisites

Verify that the registered machines that you want to remove are not being used in any desktop pool.

### Procedure

- 1 In View Administrator, select **View Configuration > Registered Machines**.
- 2 Click the **Others** tab.
- 3 Select one or more machines and click **Remove**.  
You can select only machines that are not being used by a desktop pool.
- 4 Click **OK** to confirm.

## Status of Unmanaged Machines

Unmanaged machines, which are physical computers or virtual machines that are not managed by vCenter Server, can be in various states of operation and availability. In View Administrator, you can track the status of unmanaged machines in the right-hand column of the Machines page under the **Others** tab.

[Table 10-7](#) shows the operational state of unmanaged machines that are displayed in View Administrator. A machine can be in only one state at a time.

**Table 10-7.** Status of Unmanaged Machines

Status	Description
Startup	View Agent or Horizon Agent has started on the machine, but other required services such as the display protocol are still starting. The agent startup period allows other processes such as protocol services to start up as well.
Validating	This state occurs after View Connection Server first becomes aware of the machine, typically after View Connection Server is started or restarted, and before the first successful communication with View Agent or Horizon Agent on the machine. Typically, this state is transient. It is not the same as the Agent unreachable state, which indicates a communication problem.
Agent disabled	This state can occur if View Connection Server disables View Agent or Horizon Agent. This state ensures that a new desktop session cannot be started on the machine.
Agent unreachable	View Connection Server cannot establish communication with View Agent or Horizon Agent on the machine. The machine might be powered off.
Invalid IP	The subnet mask registry setting is configured on the machine, and no active network adapters have an IP address within the configured range.
Agent needs reboot	A View component was upgraded, and the machine must be restarted to allow View Agent or Horizon Agent to operate with the upgraded component.
Protocol failure	<p>A display protocol did not start before the View Agent or Horizon Agent startup period expired.</p> <p><b>NOTE</b> View Administrator can display machines in a <b>Protocol failure</b> state when one protocol failed but other protocols started successfully. For example, the <b>Protocol failure</b> state might be displayed when HTML Access failed but PCoIP and RDP are working. In this case, the machines are available and Horizon Client devices can access them through PCoIP or RDP.</p>
Domain failure	The machine encountered a problem reaching the domain. The domain server was not accessible, or the domain authentication failed.
Configuration error	The display protocol such as RDP or another protocol is not enabled.
Unassigned user connected	<p>A user other than the assigned user is logged in to a machine in a dedicated-assignment pool.</p> <p>For example, this state can occur if an administrator logs in to the unmanaged machine without using Horizon Client.</p>
Unassigned user disconnected	A user other than the assigned user is logged in and disconnected from a machine in a dedicated-assignment pool.
Unknown	The machine is in an unknown state.
Available	The desktop-source computer is powered on and the desktop is ready for a connection. In a dedicated pool, the desktop is assigned to a user. The desktop starts when the user logs in.
Connected	The desktop is in a session and has a remote connection to a Horizon Client device.
Disconnected	The desktop is in a session, but it is disconnected from the Horizon Client device.

## Manage Published Desktop and Application Sessions

When a user launches a published desktop or application, a session is created. You can disconnect and log off sessions, send messages to clients, reset, and restart virtual machines.

### Procedure

- 1 In Horizon Administrator, navigate to where session information is displayed.

Session Type	Navigation
Remote desktop sessions	Select <b>Catalog &gt; Desktop Pools</b> , double-click a pool's ID, and click the <b>Sessions</b> tab.
Remote desktop and application sessions	Select <b>Monitoring &gt; Sessions</b> .
Sessions associated with a user or user group	<ul style="list-style-type: none"> <li>■ Select <b>Users and Groups</b>.</li> <li>■ Double-click a user's name or a user group's name.</li> <li>■ Click on the <b>Sessions</b> tab.</li> </ul>

- 2 Select a session.

To send a message to users, you can select multiple sessions. You can perform the other operations on only one session at a time.

- 3 Choose whether to disconnect, log off, or send a message, or reset a virtual machine.

Option	Description
<b>Disconnect Session</b>	Disconnects the user from the session.
<b>Logoff Session</b>	Logs the user off the session. Data that is not saved is lost.
<b>Send Message</b>	Send a message to Horizon Client. You can label the message as <b>Info</b> , <b>Warning</b> , or <b>Error</b> .

- 4 Click **OK**.

## Export View Information to External Files

In View Administrator, you can export View table information to external files. You can export the tables that list users and groups, pools, machines, View Composer persistent disks, ThinApp applications, events, and VDI sessions. You can view and manage the information in a spreadsheet or another tool.

For example, you might collect information about machines that are managed by more than one View Connection Server instance or group of replicated View Connection Server instances. You can export the Machines table from each View Administrator interface and view it in a spreadsheet.

When you export a View Administrator table, it is saved as a comma-separated value (CSV) file. This feature exports the entire table, not individual pages.

### Procedure

- 1 In View Administrator, display the table you want to export.

For example, click **Resources > Machines** to display the machines table.

- 2 Click the export icon in the upper right corner of the table.

When you point to the icon, the **Export table contents** tooltip appears.

- 3 Type a filename for the CSV file in the Select location for download dialog box.

The default filename is `global_table_data_export.csv`.

- 4 Browse to a location to store the file.
- 5 Click **Save**.

**What to do next**

Open a spreadsheet or another tool to view the CSV file.

# Managing Application Pools, Farms, and RDS Hosts

---

# 11

In Horizon Administrator, you can perform management operations such as configuring or deleting desktop pools, farms, or RDS hosts.

This chapter includes the following topics:

- [“Managing Application Pools,”](#) on page 193
- [“Managing Farms,”](#) on page 194
- [“Managing RDS Hosts,”](#) on page 199
- [“Configuring Load Balancing for RDS Hosts,”](#) on page 203
- [“Configure an Anti-Affinity Rule for an Application Pool,”](#) on page 209

## Managing Application Pools

You can add, edit, delete, or entitle application pools in Horizon Administrator.

To add an application pool, see “Creating Application Pools” in the *Setting Up Published Desktops and Applications in Horizon 7* document. To entitle an application pool, see “Entitling Users and Groups” in the *Setting Up Published Desktops and Applications in Horizon 7* document.

### Edit an Application Pool

You can edit an existing application pool to configure settings such as display name, version, publisher, path, start folder, parameters, and description. You cannot change the ID or access group of an application pool.

If you need to ensure that View Connection Server launches the application only on RDS hosts that have sufficient resources to run the application, see [“Configure an Anti-Affinity Rule for an Application Pool,”](#) on page 209.

#### Prerequisites

Familiarize yourself with the settings of an application pool. See “Creating Application Pools” in the *Setting Up Published Desktops and Applications in Horizon 7* document.

#### Procedure

- 1 In Horizon Administrator, select **Catalog > Application Pools**.
- 2 Select a pool and click **Edit**.
- 3 Make changes to the pool settings.
- 4 Click **OK**.

## Delete an Application Pool

When you delete an application pool, users can no longer launch the application in the pool.

You can delete an application pool even if users are currently accessing the application. After the users close the application, they can no longer access the application.

### Procedure

- 1 In Horizon Administrator, select **Catalog > Application Pools**.
- 2 Select one or more application pools and click **Delete**.
- 3 Click **OK** to confirm.

## Managing Farms

In Horizon Administrator, you can add, edit, delete, enable, and disable farms.

To add a farm, see "Creating Farms" in the *Setting Up Published Desktops and Applications in Horizon 7* document. For information on access groups, see [Chapter 6, "Configuring Role-Based Delegated Administration,"](#) on page 95.

After you create a farm, you can add or remove RDS hosts to support more or fewer users.

## Edit a Farm

For an existing farm, you can make changes to the configuration settings.

### Prerequisites

Familiarize yourself with the settings of a farm. See "Creating Farms" in the *Setting Up Published Desktops and Applications in Horizon 7* document.

### Procedure

- 1 In Horizon Administrator, select **Resources > Farms**.
- 2 Select a farm and click **Edit**.
- 3 Make changes to the farm settings.
- 4 Click **OK**.

## Delete a Farm

You can delete a farm if you no longer need it or if you want to create a new one with different RDS hosts. You can only delete a farm that is not associated with an RDS desktop pool or an application pool.

### Prerequisites

Verify that the farm is not associated with any RDS desktop pool or application pool.

### Procedure

- 1 In Horizon Administrator, select **Resources > Farms**.
- 2 Select one or more farms and click **Delete**.
- 3 Click **OK** to confirm.

## Disable or Enable a Farm

When you disable a farm, users can no longer launch RDS desktops or applications from the RDS desktop pools and the application pools that are associated with the farm. Users can continue to use RDS desktops and applications that are currently open.

You can disable a farm if you plan to do maintenance on the RDS hosts in the farm or on the RDS desktop and application pools that are associated with the farm. After you disable a farm, some users might still be using RDS desktops or applications that they opened before you disable the farm.

### Procedure

- 1 In Horizon Administrator, select **Resources > Farms**.
- 2 Select one or more farms and click **More Commands**.
- 3 Click **Enable** or **Disable**.
- 4 Click **OK** to confirm.

The status of the RDS desktop pools and application pools that are associated with the farm are now Unavailable. You can view the status of the pools by selecting **Catalog > Desktop Pools** or **Catalog > Application Pools**.

## Recompose an Automated Linked-Clone Farm

With the View Composer recompose operation, you can update the machine image of all the RDS hosts in an automated linked-clone farm. You can update the hardware settings or the software of the parent virtual machine and run the recompose operation to have the changes propagated to all the RDS hosts in the farm.

You can make changes to the parent virtual machine without affecting the RDS host linked clones because the clones are linked to a replica of the parent. The recompose operation deletes the old replica and creates a new one for the clones to link to. The recompose creates new linked clones, which typically use less storage because the disk files of linked clones usually grow in size over time.

You can recompose an automated farm but not individual RDS hosts in the farm. You cannot recompose linked clones to a lower hardware version than their current hardware version.

If possible, schedule recompose operations during off-peak hours because the operation can be time consuming.

### Prerequisites

- Verify that you have a snapshot of a parent virtual machine. You must specify a snapshot when you recompose. The snapshot can be on the current parent virtual machine or a different one.
- Decide when to schedule the recompose operation. By default, View Composer starts the operation immediately.

You can schedule only one recompose operation at a time for a farm. You can recompose multiple farms concurrently.

- Decide whether to force all users to log off as soon as the recompose operation begins or wait for each user to log off before recomposing that user's machine.

If you force users to log off, Horizon 7 notifies users before they are disconnected and allows them to close their applications and log off.

- Decide whether to stop provisioning at first error. If you select this option and an error occurs when View Composer provisions a linked clone, provisioning stops. You can select this option to ensure that resources such as storage are not consumed unnecessarily.

Selecting the **Stop at first error** option does not affect customization. If a customization error occurs on a linked clone, other clones continue to be provisioned and customized.

- Verify that provisioning is enabled. When provisioning is disabled, Horizon 7 stops the machines from being customized after they are recomposed.
- If your deployment includes replicated Connection Server instances, verify that all instances are the same version.

### Procedure

- 1 In Horizon Administrator, select **Resources > Farms**.
- 2 Double-click the pool ID of the farm that you want to recompose.
- 3 Click **Recompose**.
- 4 (Optional) Click **Change** to change the parent virtual machine.  
The new parent virtual machine must run the same version of the operating system as the current parent virtual machine.
- 5 Select a snapshot.
- 6 (Optional) Click Snapshot Details to display details about the snapshot.
- 7 Click **Next**.
- 8 (Optional) Schedule a start time.  
The current time is filled in by default.
- 9 (Optional) Specify whether to force users to log off or wait for users to log off.  
The option to force users to log off is selected by default.
- 10 (Optional) Specify whether to stop provisioning at first error.  
This option is selected by default.
- 11 Click **Next**.  
The Ready to Complete page is displayed.
- 12 (Optional) Click **Show Details** to display details of the recompose operation.
- 13 Click **Finish**.

In vCenter Server, you can monitor the progress of the recompose operation on the linked-clone virtual machines.

---

**NOTE** During the recompose operation, View Composer runs Sysprep again on the linked clones. New SIDs and third-party GUIDs might be generated for the recomposed virtual machines. For details, see "Recomposing Linked Clones Customized with Sysprep" in the *Setting Up Virtual Desktops in Horizon 7* document.

---

## Schedule Maintenance for an Automated Instant-Clone Farm

With the maintenance operation, you can schedule recurring or immediate maintenance of all the RDS hosts in an automated instant-clone farm. During each maintenance cycle, all the RDS hosts are refreshed from the parent virtual machine.

You can make changes to the parent virtual machine without affecting the RDS host instant clones because the snapshot of the current parent VM is used for maintenance. The instant clones created in the automated farm use the information in the parent VM for their system configuration.

You can schedule maintenance on an automated farm but not on individual RDS hosts in the farm.

If possible, schedule maintenance operations during off-peak hours to ensure all that RDS hosts have finished maintenance and are available during peak hours.

### Prerequisites

- Decide when to schedule the maintenance operation. By default, Connection Server starts the operation immediately.

You can schedule an immediate maintenance or recurring maintenance or both for a farm. You can schedule maintenance operations on multiple farms concurrently.

- Decide whether to force all users to log off when the maintenance operation begins or wait for each user to log off before refreshing that user's machine.

If you force users to log off, Horizon 7 notifies users before they are disconnected and allows them to close their applications and log off.

- Decide the minimum farm size. The minimum farm size is the number of RDS hosts that are kept available at all times to allow users to continue to use the farm. For example, if the farm size is ten and the minimum farm size is two, then maintenance will be performed on eight RDS hosts. As each RDS host becomes available again then the remaining hosts will go through maintenance. All RDS hosts are managed individually, so as one host becomes available then one of the remaining hosts will be put into maintenance.

However, if you schedule immediate maintenance, then all the RDS hosts in the farm will be put into maintenance.

All RDS hosts will also be subject to policy and will wait for logoff or force users to logoff depending upon what policy is configured.

- Decide whether to stop provisioning at first error. If you select this option and an error occurs when Connection Server provisions an instant-clone, provisioning stops. You can select this option to ensure that resources such as storage are not consumed unnecessarily.

Selecting the **Stop at first error** option does not affect customization. If a customization error occurs on an instant-clone, other clones continue to be provisioned and customized.

- Verify that provisioning is enabled. When provisioning is disabled, Horizon 7 stops the machines from being customized after they are refreshed.
- If your deployment includes replicated Connection Server instances, verify that all instances are the same version.

### Procedure

- 1 In Horizon Administrator, select **Resources > Farms**.
- 2 Double-click the pool ID of the farm for which you want to schedule a maintenance.
- 3 Click **Maintenance > Schedule**.

- 4 In the Schedule Recurring Maintenance wizard, choose a maintenance mode.

◆ Option	Action
<b>Recurring</b>	<p>Schedules periodic maintenance of all the RDS host servers in a farm.</p> <ul style="list-style-type: none"> <li>■ Select a date and time from which the maintenance is effective.</li> <li>■ Select a maintenance period. You can select daily, monthly, or weekly maintenance periods.</li> <li>■ Select a repeat interval in days for the maintenance operation to recur.</li> </ul> <p>If an immediate maintenance is scheduled on a farm, then the immediate maintenance date becomes the effective date for any recurring maintenance. If you cancel the immediate maintenance, then the current date becomes the effective date for recurring maintenance.</p>
<b>Immediate</b>	<p>Schedules immediate maintenance of all the RDS host servers in a farm. Immediate maintenance creates a one-time maintenance schedule for immediate or near future maintenance. Use immediate maintenance to refresh the farm from a new parent VM image or snapshot when you want to apply urgent security patches.</p> <p>Select an immediate maintenance configuration.</p> <ul style="list-style-type: none"> <li>■ Select <b>Start Now</b> to start the maintenance operation instantly.</li> <li>■ Select <b>Start at</b> to start the maintenance operation at a near future date and time. Enter the date and Web browser local time.</li> </ul> <p><b>Note</b> Recurring maintenance will be put on hold until immediate maintenance is complete.</p>

- 5 Click **Next**.

- 6 (Optional) Click **Change** to change the parent virtual machine.

- 7 Select a snapshot.

You cannot select a different snapshot unless you clear the **Use current parent VM image** checkbox.

- 8 (Optional) Click **Snapshot Details** to display details about the snapshot.

- 9 Click **Next**.

- 10 (Optional) Specify whether to force users to log off or wait for users to log off.

The option to force users to log off is selected by default.

- 11 (Optional) Specify whether to stop provisioning at first error.

This option is selected by default.

- 12 Click **Next**.

The Ready to Complete page is displayed.

- 13 Click **Finish**.

## Managing RDS Hosts

You can manage RDS hosts that you set up manually and RDS hosts that are created automatically when you add an automated farm.

When you manually set up an RDS host, it automatically registers with Horizon Connection Server. You cannot manually register an RDS host with Connection Server. See "Setting Up Remote Desktop Session Hosts" in the *Setting Up Published Desktops and Applications in Horizon 7* document. For an RDS host that you set up manually, you can perform the following management tasks:

- Edit the RDS host.
- Add the RDS host to a manual farm.
- Remove the RDS host from a farm.
- Enable the RDS host.
- Disable the RDS host.

For an RDS host that is created automatically when you add an automated farm, you can perform the following management tasks:

- Remove the RDS host from a farm.
- Enable the RDS host.
- Disable the RDS host.

### Edit an RDS Host

You can change the number of connections that an RDS host can support. This setting is the only one that you can change. The default value is 150. You can set it to any positive number, or to unlimited.

You can only edit an RDS host that you set up manually, but not an RDS host that is in an automated farm.

#### Procedure

- 1 In View Administrator, select **View Configuration > Registered Machines**.
- 2 Select an RDS host and click **Edit**.
- 3 Specify a value for the setting **Number of connections**.
- 4 Click **OK**.

### Add an RDS Host to a Manual Farm

You can add an RDS host that you set up manually to a manual farm to increase the scale of the farm or for other reasons. You can only add RDS hosts to a manual farm.

#### Procedure

- 1 In View Administrator, select **Resources > Farms**.
- 2 Double-click the pool ID of the farm.
- 3 Select the **RDS Hosts** tab.
- 4 Select one or more RDS hosts.
- 5 Click **OK**.

## Remove an RDS Host from a Farm

You can remove an RDS host from a manual farm to reduce the scale of the farm, to perform maintenance on the RDS host, or for other reasons. As a best practice, disable the RDS host and ensure that users are logged off from active sessions before you remove a host from a farm.

If users have application or desktop sessions on hosts that you remove, the sessions remain active, but View no longer keeps track of them. A user who disconnects from a session will be unable to reconnect to it, and any unsaved data might be lost.

You can also remove an RDS host from an automated farm. One possible reason might be that the RDS host is in an unrecoverable error state. View Composer automatically creates a new RDS host to replace the one that you remove.

### Procedure

- 1 In View Administrator, select **Resources > Farms**.
- 2 Double-click the pool ID.
- 3 Select the **RDS Hosts** tab.
- 4 Select one or more RDS hosts.
- 5 Click **Remove from farm**.
- 6 Click **OK**.

## Remove an RDS Host from Horizon 7

You can remove from Horizon 7 an RDS host that you set up manually and that you no longer plan to use. The RDS host must not currently be in a manual farm.

### Prerequisites

Verify that the RDS host does not belong to a farm.

### Procedure

- 1 In Horizon Administrator, select **View Configuration > Registered Machines**.
- 2 Select an RDS host and click **Remove**.
- 3 Click **OK**.

After you remove an RDS host, to use it again, you must reinstall Horizon Agent. See “Setting Up Remote Desktop Session Hosts” in the *Setting Up Published Desktops and Applications in Horizon 7* document.

## Disable or Enable an RDS Host

When you disable an RDS host, View no longer uses it to host new RDS desktops or applications. Users can continue to use RDS desktops and applications that are currently open.

### Procedure

- 1 In View Administrator, select **Resources > Farms**.
- 2 Double-click the pool ID of a farm.
- 3 Select the **RDS Hosts** tab.
- 4 Select an RDS host and click **More Commands**.
- 5 Click **Enable** or **Disable**.

6 Click **OK**.

If you enable the RDS host, a check mark appears in the Enabled column, and Available appears in the Status column. If you disable the RDS host, the Enabled column is empty and Disabled appears in the Status column.

## Monitor RDS Hosts

You can monitor the status and view the properties of RDS hosts in View Administrator.

### Procedure

- ◆ In View Administrator, navigate to the page that displays the properties that you want to view.

Properties	Action
<b>RDS Host, Farm, Desktop Pool, Agent Version, Sessions, Status</b>	<ul style="list-style-type: none"> <li>■ In View Administrator, select <b>Resources &gt; Machines</b>.</li> <li>■ Click the <b>RDS Hosts</b> tab. Both linked-clone RDS hosts and RDS hosts that are set up manually are displayed.</li> </ul>
<b>DNS Name, Type, RDS Farm, Max Number of Connections, Agent Version, Enabled, Status</b>	<ul style="list-style-type: none"> <li>■ In View Administrator, select <b>View Configuration &gt; Registered Machines</b>.</li> <li>■ Click the <b>RDS Hosts</b> tab. Only RDS hosts that are set up manually are displayed.</li> </ul>

The properties are displayed and have the following meanings:

Property	Description
RDS Host	Name of the RDS host.
Farm	Farm to which the RDS host belongs.
Desktop Pool	RDS desktop pool associated with the farm.
Agent Version	Version of View Agent or Horizon Agent that runs on the RDS host.
Sessions	Number of client sessions.
DNS Name	DNS name of the RDS host.
Type	Version of Windows Server that runs on the RDS host.
RDS Farm	Farm to which the RDS host belongs.
Max Number of Connections	Maximum number of connections that the RDS host can support.
Enabled	Whether the RDS host is enabled.
Status	State of the RDS host. See <a href="#">“Status of RDS Hosts,”</a> on page 201 for a description of the possible states.

## Status of RDS Hosts

An RDS host can be in various states from the time that it is initialized. As a best practice, check that RDS hosts are in the state that you expect them to be in before and after you perform tasks or operations on them.

**Table 11-1.** Status of an RDS Host

Status	Description
Startup	View Agent or Horizon Agent has started on the RDS host, but other required services such as the display protocol are still starting. The agent startup period also allows other processes such as protocol services to start up.
Disable in progress	RDS host is in the process of being disabled while sessions are still running on the host. When the sessions end, the status changes to Disabled.

**Table 11-1.** Status of an RDS Host (Continued)

Status	Description
Disabled	Process of disabling the RDS host is complete.
Validating	Occurs after View Connection Server first becomes aware of the RDS host, typically after View Connection Server is started or restarted, and before the first successful communication with View Agent or Horizon Agent on the RDS host. Typically, this state is transient. This state is not the same as the Agent unreachable state, which indicates a communication problem.
Agent disabled	Occurs if View Connection Server disables View Agent or Horizon Agent. This state ensures that a new desktop or application session cannot be started on the RDS host.
Agent unreachable	View Connection Server cannot establish communication with View Agent or Horizon Agent on an RDS host.
Invalid IP	Subnet mask registry setting is configured on the RDS host, and no active network adapters have an IP address within the configured range.
Agent needs reboot	View component was upgraded, and the RDS host must be restarted to allow View Agent or Horizon Agent to operate with the upgraded component.
Protocol failure	The RDP display protocol is not running correctly. If RDP is not running and PCoIP is running, clients cannot connect using either RDP or PCoIP. However, if RDP is running and PCoIP is not running, clients can connect using RDP.
Domain failure	RDS host encountered a problem reaching the domain. The domain server was not accessible, or the domain authentication failed.
Configuration error	RDS role is not enabled on the server.
Unknown	RDS host is in an unknown state.
Available	RDS host is available. If the host is in a farm, and the farm is associated with an RDS or application pool, it will be used to deliver RDS desktops or applications to users.
Provisioning	(For linked-clone RDS hosts only) Provisioning of the virtual machine is in progress.
Customizing	(For linked-clone RDS hosts only) Customization of the virtual machine is in progress.
Deleting	(For linked-clone RDS hosts only) Deletion of the virtual machine is in progress.
Waiting for Agent	(For linked-clone RDS hosts only) View Connection Server is waiting to establish communication with View Agent or Horizon Agent.
Maintenance Mode	(For linked-clone RDS hosts only) The virtual machine is in maintenance mode and is not available to users.
Provisioned	(For linked-clone RDS hosts only) Provisioning of the virtual machine is complete.
Provisioning Error	(For linked-clone RDS hosts only) An error occurred during provisioning.
Error	(For linked-clone RDS hosts only) An unknown error occurred in the virtual machine.

## Configure Adobe Flash Throttling with Internet Explorer in RDS Desktops

To ensure that Adobe Flash throttling works with Internet Explorer in RDS desktops, users must enable third-party browser extensions.

### Procedure

- 1 Start Horizon Client and log in to a user's remote desktop.
- 2 In Internet Explorer, click **Tools > Internet Options**.
- 3 Click the **Advanced** tab, select **Enable third-party browser extensions**, and click **OK**.
- 4 Restart Internet Explorer.

## Configuring Load Balancing for RDS Hosts

By default, View Connection Server uses the current session count and limit to balance the placement of new application sessions on RDS hosts. You can override this default behavior and control the placement of new application sessions by writing and configuring load balancing scripts.

A load balancing script returns a load value. The load value can be based on any host metric, such as CPU utilization or memory utilization. Horizon Agent maps the load value to a load preference, and reports the load preference to View Connection Server. View Connection Server uses reported load preferences to determine where to place new application sessions.

You can write your own load balancing scripts, or you can use one of the sample load balancing scripts provided with Horizon Agent.

Configuring load balancing scripts involves enabling the VMware Horizon View Script Host service and setting a registry key on each RDS host in a farm.

### Load Values and Mapped Load Preferences

Horizon Agent maps the load value that a load balancing script returns to a load preference. View Connection server uses reported load preferences to determine where to place new application sessions.

The following table lists the valid load values that a load balancing script can return and describes the associated load preferences.

**Table 11-2.** Valid Load Values and Mapped Load Preferences

Valid Load Value	Load Preference Reported by Horizon Agent	Description
0	BLOCK	Do not choose this RDS host.
1	LOW	Low preference/high load.
2	MED	Medium preference/normal load.
3	HIGH	High preference/light load.

### Load Balancing Feature Constraints

The RDS host load balancing feature has certain constraints.

- Anti-infinity rules can prevent an application from being placed on an RDS host, regardless of the reported load preference. For more information, see [“Configure an Anti-Affinity Rule for an Application Pool,”](#) on page 209.
- Load balancing affects new application sessions only. An RDS host that contains sessions in which a user has previously run an application is always reused for the same application. This behavior overrides reported load preferences and anti-affinity rules.
- Applications are launched on an RDS host where a user already has an existing session, even if the RDS host reports a BLOCK load preference.
- RDS session limits prevent application sessions from being created, regardless of the reported load preference.

## Writing a Load Balancing Script for an RDS Host

You can write a load balancing script to generate a load value based on any RDS host metric that you want to use for load balancing. You can also write a simple load balancing script that returns a fixed load value.

Your load balancing script must return a single number from 0 to 3. For descriptions of the valid load values, see [“Load Values and Mapped Load Preferences,”](#) on page 203.

If at least one RDS host in the farm returns a valid load value, View Connection Server assumes a load value of 2 (mapped load preference of MED) for the other RDS hosts in farm until their load balancing scripts return valid values. If no RDS host in the farm returns a valid load value, the load balancing feature is disabled for the farm.

If your load balancing script returns an invalid load value or does not finish running within 10 seconds, Horizon Agent sets the load preference to BLOCK and the RDS host state to configuration error. These values effectively remove the RDS host from the list of RDS hosts available for new sessions.

Copy your load balancing script to the Horizon Agent scripts directory (C:\Program Files\VMware\VMware View\Agent\scripts) on each RDS host in the farm. You must copy the same script to every RDS host in the farm.

For an example how to write a load balancing script, see the sample scripts in the Horizon Agent scripts directory. For more information, see [“Sample Load Balancing Scripts for RDS Hosts,”](#) on page 204.

### Sample Load Balancing Scripts for RDS Hosts

When you install Horizon Agent on an RDS host, the installer places sample load balancing scripts in the Horizon Agent scripts directory (C:\Program Files\VMware\VMware View\Agent\scripts).

**Table 11-3.** Sample Load Balancing Scripts

Name	Description
cpuutilisation.vbs	<p>Reads the percentage of CPU that has been utilized from the registry and returns the following load values:</p> <ul style="list-style-type: none"> <li>■ 0, if CPU utilization is greater than 90 percent</li> <li>■ 1, if CPU utilization is greater than 75 percent</li> <li>■ 2, if CPU utilization is greater than 25 percent</li> <li>■ 3, if CPU utilization is less or equal to 25 percent</li> </ul>
memoryutilisation.vbs	<p>Calculates the percentage of memory that has been utilized and returns the following load values:</p> <ul style="list-style-type: none"> <li>■ 0, if memory utilization is greater than 90 percent</li> <li>■ 1, if memory utilization is greater than 75 percent</li> <li>■ 2, if memory utilization is greater than 25 percent</li> <li>■ 3, if memory utilization is less or equal to 25 percent</li> </ul>

**NOTE** Because the `cpuutilisation.vbs` script uses rolling average data that is sampled every five minutes, short-term high-utilization events might not be reflected in reported load preferences. You can reduce the sampling period to a minimum of two minutes, but performance might be affected on the RDS host. The sampling interval is controlled by the registry entry `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Performance Stats\SamplingIntervalSeconds`. The default is 300 seconds.

## Enable the VMware Horizon View Script Host Service on an RDS Host

You must enable the VMware Horizon View Script Host service on an RDS host before you configure a load balancing script. The VMware Horizon View Script Host service is disabled by default.

### Procedure

- 1 Log in to the RDS host as an administrator.
- 2 Start Server Manager.
- 3 Select **Tools > Services** and navigate to the VMware Horizon View Script Host service.
- 4 Right-click **VMware Horizon View Script Host** and select **Properties**.
- 5 In the Properties dialog box, select **Automatic** from the **Startup type** drop-down menu and click **OK** to save your changes.
- 6 Right-click **VMware Horizon View Script Host** and select **Start** to start the VMware Horizon View Script Host service.

The VMware Horizon View Script Host service restarts automatically each time the RDS host starts.

### What to do next

Configure your load balancing script on each RDS host in the farm. See [“Configure a Load Balancing Script on an RDS Host,”](#) on page 205.

## Configure a Load Balancing Script on an RDS Host

You must configure the same load balancing script on every RDS host in the farm. Configuring a load balancing script involves setting a registry key on the RDS host.

If you are using an automated farm, you perform this procedure on the parent virtual machine for the automated farm.

---

**IMPORTANT** You must configure the load balancing script on all of the RDS hosts in a farm or on none of the RDS hosts in a farm. If you configure a load balancing script on only some of the RDS hosts in a farm, View Administrator sets the health of the farm to yellow.

---

### Prerequisites

- Write a load balancing script and copy the same script to the Horizon Agent scripts directory on each RDS host in the farm. See [“Writing a Load Balancing Script for an RDS Host,”](#) on page 204.
- Enable the VMware Horizon View Script Host service on the RDS host. See [“Enable the VMware Horizon View Script Host Service on an RDS Host,”](#) on page 205

### Procedure

- 1 Log in to the RDS host as an administrator.
- 2 Start Server Manager.
- 3 Select **Tools > System Configuration**, click the **Tools** tab, and launch the Registry Editor.
- 4 In the registry, navigate to HKEY\_LOCAL\_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\ScriptEvents.
- 5 In the navigation area, select the **RdshLoad** key.

The values for the **RdshLoad** key, if any, appear in the topic area (the right pane).

- 6 Right-click in the topic area for the **RdshLoad** key, select **New > String Value**, and create a new string value.  
  
As a best practice, use a name that represents the load balancing script to be run, for example, **cpuutilisationScript** for the `cpuutilisation.vbs` script.
- 7 Right-click the entry for the new string value you created and select **Modify**.
- 8 In the **Value data** text box, type the command line that invokes your load balancing script and click **OK**.  
  
Type the full path to your load balancing script.  
  
For example: `cscript.exe "C:\Program Files\VMware\VMware View Agent\scripts\cpuutilisation.vbs"`
- 9 Restart the Horizon Agent service on the RDS host to make your changes take effect.

Your load balancing script begins to run on the RDS host.

### What to do next

Repeat this procedure on each RDS host in the farm. If you performed this procedure on the parent virtual machine for an automated farm, provision the automated farm.

To verify that your load balancing script is working correctly, see [“Verify a Load Balancing Script,”](#) on page 206.

## Verify a Load Balancing Script

You can verify that your load balancing script is working correctly by viewing RDS farm and RDS host information in View Administrator.

### Procedure

- 1 In View Administrator, click **Dashboard** and expand **RDS Farms** in the System Health pane.
- 2 View the health of the farm that contains the RDS hosts.  
  
The health of the farm should be green. If a load balancing script is configured on only some of the RDS hosts in a farm, View Administrator sets the health of the farm to yellow. You must configure the load balancing script on all of the RDS hosts in a farm or on none of the RDS hosts in a farm.
- 3 Expand the farm and click the name of each RDS host to view its load preference.  
  
The Server load field in the details dialog box shows the load preference reported by Horizon Agent, for example, `Light load, new sessions okay`. If Horizon Agent did not report a load preference, the Server load field shows `Load not reported`.

### What to do next

If load balancing is not working as you expected, verify the content of your load balancing script. If the script is written correctly, verify that the VMware Horizon View Script Host service is running and that the same load balancing script is configured on each RDS host in the farm.

## Load Balancing Session Placement Examples

These examples illustrate two load balancing session placement scenarios.

### Example 1: No Existing User Session

This example illustrates how session placement might occur for a farm that contains six RDS hosts when a user session does not currently exist on any of the RDS hosts.

- 1 Horizon Agent reports the following load preferences for each RDS host in the farm.

RDS Host	Load Preference
1	HIGH
2	LOW
3	HIGH
4	MED
5	BLOCK
6	LOW

- 2 View sorts the RDS hosts into three buckets according to load preference. View discards RDS host 5 because Horizon Agent reported a load preference of BLOCK.

Bucket	Load Preference	RDS Host
1	HIGH	1
	HIGH	3
2	MED	4
3	LOW	2
	LOW	6

- 3 Because bucket 2 has only one RDS host, View combines bucket 2 and bucket 3

Bucket	Load Preference	RDS Host
1	HIGH	1
	HIGH	3
	MED	4
2	LOW	2
	LOW	6

- 4 View randomizes the bucket order.

Bucket	Load Preference	RDS Host
1	MED	4
	HIGH	3
	MED	1
2	LOW	6
	LOW	2

- 5 View Connection Server attempts to place a new application session on RDS host 4 first, followed by RDS host 3, and so on.

RDS Host Session Placement Order
4
3
1
6
2

**NOTE** Anti-infinity rules can prevent an application from being placed on an RDS host, regardless of the reported load preference. For more information, see [“Configure an Anti-Affinity Rule for an Application Pool,”](#) on page 209.

## Example 2: Existing User Session

This example illustrates how session placement might occur for a farm that contains six RDS hosts when a user session currently exists on one of the RDS hosts. An RDS host that contains a session in which a user has previously run an application is always reused for the same application.

- 1 A user session already exists on RDS host 3. RDS host 3 has a load preference of MED. The remaining RDS in the hosts in the farm (the spare list) have the following load preferences.

RDS Host	Load Preference
1	MED
2	LOW
4	HIGH
5	LOW
6	BLOCK

- 2 View sorts the RDS hosts in the spare list into two buckets according to load preference. View discards RDS host 6 because Horizon Agent reported a load preference of BLOCK.

Bucket	Load Preference	RDS Host
1	HIGH	4
	MED	1
2	LOW	2
	LOW	5

- 3 View randomizes the bucket order.

Bucket	Load Preference	RDS Host
1	HIGH	4
	MED	1
2	LOW	5
	LOW	2

- 4 View adds the RDS host that contains the existing session to the top of the new bucket ordered list.

RDS Host Session Placement Order
3
4
1
5
2

## Configure an Anti-Affinity Rule for an Application Pool

When you configure an anti-affinity rule for an application pool, Horizon Connection Server attempts to launch the application only on RDS hosts that have sufficient resources to run the application. This feature can be useful for controlling applications that consume large amounts of CPU or memory resources.

An anti-affinity rule consists of an application matching pattern and a maximum count. For example, the application matching pattern might be `autocad.exe` and the maximum count might be 2.

Connection Server sends the anti-affinity rule to Horizon Agent on an RDS host. If any applications running on the RDS host have process names that match the application matching pattern, Horizon Agent counts the current number of instances of those applications and compares the number to the maximum count. If the maximum count is exceeded, Connection Server skips that RDS host when it selects an RDS host to run new sessions of the application.

### Prerequisites

- Create the application pool. See "Creating Application Pools" section in the *Setting Up Published Desktops and Applications in Horizon 7* document.
- Become familiar with the constraints of the anti-affinity feature. See ["Anti-Affinity Feature Constraints,"](#) on page 210.

### Procedure

- 1 In Horizon Administrator, select **Catalog > Application Pools**.
- 2 Select the pool to modify and click **Edit**.
- 3 In the **Anti-Affinity Patterns** text box, type a comma-separated list of patterns to match against the process names of other applications running on RDS hosts.

The pattern string can include the asterisk (\*) and question mark (?) wildcard characters. An asterisk matches zero or more characters and a question mark matches any single character.

For example, `*pad.exe,*notepad.???` matches `wordpad.exe`, `notepad.exe`, and `notepad.bat`, but it does not match `wordpad.bat` or `notepad.script`.

---

**NOTE** Horizon 7 counts multiple patterns that match for an application in a single session as a single match.

---

- 4 In the **Anti-Affinity Count** text box, type the maximum number of other applications that can be running on the RDS host before the RDS host is rejected for new application sessions.

The maximum count can be an integer from 1 to 20.

- 5 Click **OK** to save your changes.

## Anti-Affinity Feature Constraints

The anti-affinity feature has certain constraints.

- Anti-affinity rules affect new application sessions only. An RDS host that contains sessions in which a user has previously run an application is always reused for the same application. This behavior overrides reported load preferences and anti-affinity rules.
- Anti-affinity rules do not affect application launches from within an RDS desktop session.
- RDS session limits prevent application sessions from being created, regardless of anti-affinity rules.
- In certain circumstances, the instances of applications on the RDS host might not be restricted to the maximum count that you specify. For example, View cannot determine the exact instance count if other applications for other pending sessions are in the process of being launched.
- Inter-application anti-affinity rules are not supported. For example, large application classes, such as Autocad and Visual Studio instances, cannot be counted in a single rule.
- Do not use anti-affinity rules in environments where end-users use Horizon Client on mobile clients. Anti-affinity rules can result in multiple sessions in the same farm for an end user. Reconnecting to multiple sessions on mobile clients can result in indeterminate behavior.

# Managing ThinApp Applications in View Administrator

# 12

You can use View Administrator to distribute and manage applications packaged with VMware ThinApp. Managing ThinApp applications in View Administrator involves capturing and storing application packages, adding ThinApp applications to View Administrator, and assigning ThinApp applications to machines and desktop pools.

You must have a license to use the ThinApp management feature in View Administrator.

---

**IMPORTANT** If, instead of distributing ThinApps by assigning them to machines and desktop pools, you would rather assign ThinApps to Active Directory users and groups, you can use VMware Identity Manager.

---

This chapter includes the following topics:

- [“View Requirements for ThinApp Applications,”](#) on page 211
- [“Capturing and Storing Application Packages,”](#) on page 212
- [“Assigning ThinApp Applications to Machines and Desktop Pools,”](#) on page 215
- [“Maintaining ThinApp Applications in View Administrator,”](#) on page 221
- [“Monitoring and Troubleshooting ThinApp Applications in View Administrator,”](#) on page 224
- [“ThinApp Configuration Example,”](#) on page 227

## View Requirements for ThinApp Applications

When capturing and storing ThinApp applications that will be distributed to remote desktops in View Administrator, you must meet certain requirements.

- You must package your applications as Microsoft Installation (MSI) packages.
- You must use ThinApp version 4.6 or later to create or repackage the MSI packages.
- You must store the MSI packages on a Windows network share that resides in an Active Directory domain that is accessible to your View Connection Server host and remote desktops. The file server must support authentication and file permissions that are based on computer accounts.
- You must configure the file and sharing permissions on the network share that hosts the MSI packages to give Read access to the built-in Active Directory group Domain Computers. If you plan to distribute ThinApp applications to domain controllers, you must also give Read access to the built-in Active Directory group Domain Controllers.
- To allow users access to streaming ThinApp application packages, you must set the NTFS permission of the network share that hosts the ThinApp packages to Read&Execute for users.

- Make sure that a disjoint namespace does not prevent domain member computers from accessing the network share that hosts the MSI packages. A disjoint namespace occurs when an Active Directory domain name is different from the DNS namespace that is used by machines in that domain. See VMware Knowledge Base (KB) article 1023309 for more information.
- To run streamed ThinApp applications on remote desktops, users must have access to the network share that hosts the MSI packages.

## Capturing and Storing Application Packages

ThinApp provides application virtualization by decoupling an application from the underlying operating system and its libraries and framework and bundling the application into a single executable file called an application package.

To manage ThinApp applications in View Administrator, you must use the ThinApp Setup Capture wizard to capture and package your applications in MSI format and store the MSI packages in an application repository.

An application repository is a Windows network share. You use View Administrator to register the network share as an application repository. You can register multiple application repositories.

---

**NOTE** If you have multiple application repositories, you can use third-party solutions to manage load balancing and availability. View does not include load balancing or availability solutions.

---

See the *Introduction to VMware ThinApp* and the *ThinApp User's Guide* for complete information on ThinApp features and how to use the ThinApp Setup Capture wizard.

- 1 [Package Your Applications](#) on page 212  
You use the ThinApp Setup Capture wizard to capture and package your applications.
- 2 [Create a Windows Network Share](#) on page 213  
You must create a Windows network share to host the MSI packages that are distributed to remote desktops and pools in View Administrator.
- 3 [Register an Application Repository](#) on page 213  
You must register the Windows network share that hosts your MSI packages as an application repository in View Administrator.
- 4 [Add ThinApp Applications to View Administrator](#) on page 214  
You add ThinApp applications to View Administrator by scanning an application repository and selecting ThinApp applications. After you add a ThinApp application to View Administrator, you can assign it to machines and desktop pools.
- 5 [Create a ThinApp Template](#) on page 214  
You can create a template in View Administrator to specify a group of ThinApp applications. You can use templates to group applications together by function, vendor, or any other logical grouping that makes sense in your organization.

## Package Your Applications

You use the ThinApp Setup Capture wizard to capture and package your applications.

### Prerequisites

- Download the ThinApp software from <http://www.vmware.com/products/thinapp> and install it on a clean computer. View supports ThinApp version 4.6 and later.
- Familiarize yourself with the ThinApp software requirements and application packaging instructions in the *ThinApp User's Guide*.

**Procedure**

- 1 Start the ThinApp Setup Capture wizard and follow the prompts in the wizard.
- 2 When the ThinApp Setup Capture wizard prompts you for a project location, select **Build MSI package**.
- 3 If you plan to stream the application to remote desktops, set the MSISstreaming property to 1 in the package.ini file.

```
MSISstreaming=1
```

The ThinApp Setup Capture wizard encapsulates the application, all of the necessary components to run the application, and the application itself into an MSI package.

**What to do next**

Create a Windows network share to store the MSI packages.

**Create a Windows Network Share**

You must create a Windows network share to host the MSI packages that are distributed to remote desktops and pools in View Administrator.

**Prerequisites**

- Use the ThinApp Setup Capture wizard to package the applications.
- Verify that the network share meets View requirements for storing ThinApp applications. See [“View Requirements for ThinApp Applications,”](#) on page 211 for more information.

**Procedure**

- 1 Create a shared folder on a computer in an Active Directory domain that is accessible to both your View Connection Server host and remote desktops.
- 2 Configure the file and sharing permissions on the shared folder to give Read access to the built-in Active Directory group Domain Computers.
- 3 If you plan to assign ThinApp applications to domain controllers, give Read access to the built-in Active Directory group Domain Controllers.
- 4 If you plan to use streaming ThinApp application packages, set the NTFS permission of the network share that hosts the ThinApp packages to Read&Execute for users.
- 5 Copy your MSI packages to the shared folder.

**What to do next**

Register the Windows network share as an application repository in View Administrator.

**Register an Application Repository**

You must register the Windows network share that hosts your MSI packages as an application repository in View Administrator.

You can register multiple application repositories.

**Prerequisites**

Create a Windows network share.

### Procedure

- 1 In View Administrator, select **View Configuration > ThinApp Configuration** and click **Add Repository**.
- 2 Type a display name for the application repository in the **Display name** text box.
- 3 Type the path to the Windows network share that hosts your application packages in the **Share path** text box.

The network share path must be in the form `\\ServerComputerName\ShareName` where *ServerComputerName* is the DNS name of the server computer. Do not specify an IP address.

For example: `\\server.domain.com\MSIPackages`

- 4 Click **Save** to register the application repository with View Administrator.

## Add ThinApp Applications to View Administrator

You add ThinApp applications to View Administrator by scanning an application repository and selecting ThinApp applications. After you add a ThinApp application to View Administrator, you can assign it to machines and desktop pools.

### Prerequisites

Register an application repository with View Administrator.

### Procedure

- 1 In View Administrator, select **Catalog > ThinApps**.
- 2 On the **Summary** tab, click **Scan New ThinApps**.
- 3 Select an application repository and a folder to scan and click **Next**.  
If the application repository contains subfolders, you can expand the root folder and select a subfolder.
- 4 Select the ThinApp applications that you want to add to View Administrator.  
You can press Ctrl+click or Shift+click to select multiple ThinApp applications.
- 5 Click **Scan** to begin scanning the MSI packages that you selected.  
You can click **Stop Scan** if you need to stop the scan.  
View Administrator reports the status of each scanning operation and the number of ThinApp applications that were added to View Administrator. If you select an application that is already in View Administrator, it is not added again.
- 6 Click **Finish**.

The new ThinApp applications appear on the **Summary** tab.

### What to do next

(Optional) Create ThinApp templates.

## Create a ThinApp Template

You can create a template in View Administrator to specify a group of ThinApp applications. You can use templates to group applications together by function, vendor, or any other logical grouping that makes sense in your organization.

With ThinApp templates, you can streamline the distribution of multiple applications. When you assign a ThinApp template to a machine or desktop pool, View Administrator installs all of the applications that are currently in the template.

Creating ThinApp templates is optional.

---

**NOTE** If you add an application to a ThinApp template after assigning the template to a machine or desktop pool, View Administrator does not automatically assign the new application to the machine or desktop pool. If you remove an application from a ThinApp template that was previously assigned to a machine or desktop pool, the application remains assigned to the machine or desktop pool.

---

### Prerequisites

Add selected ThinApp applications to View Administrator.

### Procedure

- 1 In View Administrator, select **Catalog > ThinApps** and click **New Template**.
- 2 Type a name for the template and click **Add**.  
All of the available ThinApp applications appear in the table.
- 3 To find a particular ThinApp application, type the name of the application in the **Find** text box and click **Find**.
- 4 Select the ThinApp applications that you want to include in the template and click **Add**.  
You can press Ctrl+click or Shift+click to select multiple applications.
- 5 Click **OK** to save the template.

## Assigning ThinApp Applications to Machines and Desktop Pools

To install a ThinApp application on a remote desktop, you use View Administrator to assign the ThinApp application to a machine or desktop pool.

When you assign a ThinApp application to a machine, View Administrator begins installing the application on the virtual machine a few minutes later. When you assign a ThinApp application to a desktop pool, View Administrator begins installing the application the first time a user logs in to a remote desktop in the pool.

<b>Streaming</b>	View Administrator installs a shortcut to the ThinApp application on the remote desktop. The shortcut points to the ThinApp application on the network share that hosts the repository. Users must have access to the network share to run streamed ThinApp applications.
<b>Full</b>	View Administrator installs the full ThinApp application on the local file system.

The amount of time it takes to install a ThinApp application depends on the size of the application.

---

**IMPORTANT** You can assign ThinApp applications to virtual machine-based desktops and automated desktop pools or manual pools that contains vCenter Server virtual machines. You cannot assign ThinApp applications to RDS desktops or traditional PCs.

---

- [Best Practices for Assigning ThinApp Applications](#) on page 216  
Follow best practices when you assign ThinApp applications to machines and desktop pools.
- [Assign a ThinApp Application to Multiple Machines](#) on page 216  
You can assign a particular ThinApp to one or more machines.
- [Assign Multiple ThinApp Applications to a Machine](#) on page 217  
You can assign one or more ThinApp applications to a particular machine.

- [Assign a ThinApp Application to Multiple Desktop Pools](#) on page 218  
You can assign a particular ThinApp application to one or more desktop pools.
- [Assign Multiple ThinApp Applications to a Desktop Pool](#) on page 218  
You can assign one more ThinApp applications to a particular desktop pool.
- [Assign a ThinApp Template to a Machine or Desktop Pool](#) on page 219  
You can streamline the distribution of multiple ThinApp applications by assigning a ThinApp template to a machine or desktop pool.
- [Review ThinApp Application Assignments](#) on page 220  
You can review all of the machines and desktop pools that a particular ThinApp application is currently assigned to. You can also review all of the ThinApp applications that are assigned to a particular machine or desktop pool.
- [Display MSI Package Information](#) on page 221  
After you add a ThinApp application to View Administrator, you can display information about its MSI package.

## Best Practices for Assigning ThinApp Applications

Follow best practices when you assign ThinApp applications to machines and desktop pools.

- To install a ThinApp application on a particular remote desktop, assign the application to the virtual machine that hosts the desktop. If you use a common naming convention for your machines, you can use machine assignments to quickly distribute applications to all of the machines that use that naming convention.
- To install a ThinApp application on all of the machines in a desktop pool, assign the application to the desktop pool. If you organize your desktop pools by department or user type, you can use desktop pool assignments to quickly distribute applications to specific departments or users. For example, if you have a desktop pool for your accounting department users, you can distribute the same application to all of the users in your accounting department by assigning the application to the accounting pool.
- To streamline the distribution of multiple ThinApp applications, include the applications in a ThinApp template. When you assign a ThinApp template to a machine or desktop pool, View Administrator installs all of the applications currently in the template.
- Do not assign a ThinApp template to a machine or desktop pool if the template contains a ThinApp application that is already assigned to that machine or desktop pool. Also, do not assign a ThinApp template to the same machine or desktop pool more than once with a different installation type. View Administrator will return ThinApp assignment errors in both of these situations.

## Assign a ThinApp Application to Multiple Machines

You can assign a particular ThinApp to one or more machines.

### Prerequisites

Scan an application repository and add selected ThinApp applications to View Administrator. See [“Add ThinApp Applications to View Administrator,”](#) on page 214.

### Procedure

- 1 In View Administrator, select **Catalog > ThinApps** and select the ThinApp application.

- 2 Select **Assign Machines** from the **Add Assignment** drop-down menu.

The machines that the ThinApp application is not already assigned to appear in the table.

Option	Action
<b>Find a specific machine</b>	Type the name of the machine in the <b>Find</b> text box and click <b>Find</b> .
<b>Find all of the machines that follow the same naming convention</b>	Type a partial machine name in the <b>Find</b> text box and click <b>Find</b> .

- 3 Select the machines that you want to assign the ThinApp application to and click **Add**.

You can press Ctrl+click or Shift+click to select multiple machines.

- 4 Select an installation type and click **OK**.

Option	Action
<b>Streaming</b>	Installs a shortcut to the application on the machine. The shortcut points to the application on the network share that hosts the repository. Users must have access to the network share to run the application.
<b>Full</b>	Installs the full application on the machine's local file system.

Some ThinApp applications do not support both installation types. How the application package was created determines which installation types are available.

View Administrator begins installing the ThinApp application a few minutes later. After the installation is finished, the application is available to all of the users of the remote desktops hosted by the virtual machines.

## Assign Multiple ThinApp Applications to a Machine

You can assign one or more ThinApp applications to a particular machine.

### Prerequisites

Scan an application repository and add selected ThinApp applications to View Administrator. See [“Add ThinApp Applications to View Administrator,”](#) on page 214.

### Procedure

- 1 In View Administrator, select **Resources > Machines** and double-click the name of the machine in the Machine column.
- 2 On the **Summary** tab, click **Add Assignment** in the ThinApps pane.  
The ThinApp applications that are not already assigned to the machine appear in the table.
- 3 To find a particular application, type the name of the application in the **Find** text box and click **Find**.
- 4 Select a ThinApp application to assign to the machine and click **Add**.  
Repeat this step to add multiple applications.
- 5 Select an installation type and click **OK**.

Option	Action
<b>Streaming</b>	Installs a shortcut to the application on the machine. The shortcut points to the application on the network share that hosts the repository. Users must have access to the network share to run the application.
<b>Full</b>	Installs the full application on the machine's local file system.

Some ThinApp applications do not support both installation types. How the application package was created determines which installation types are available.

View Administrator begins installing the ThinApp applications a few minutes later. After the installation is finished, the applications are available to all of the users of the remote desktop that is hosted by the virtual machine.

## Assign a ThinApp Application to Multiple Desktop Pools

You can assign a particular ThinApp application to one or more desktop pools.

If you assign a ThinApp application to a linked-clone pool and later refresh, recompose, or rebalance the pool, View Administrator reinstalls the application for you. You do not have to manually reinstall the application.

### Prerequisites

Scan an application repository and add selected ThinApp applications to View Administrator. See [“Add ThinApp Applications to View Administrator,”](#) on page 214.

### Procedure

- 1 In View Administrator, select **Catalog > ThinApps** and select the ThinApp application.
- 2 Select **Assign Desktop Pools** from the **Add Assignment** drop-down menu.

The desktop pools that the ThinApp application is not already assigned to appear in the table.

Option	Action
<b>Find a specific desktop pool</b>	Type the name of the desktop pool in the <b>Find</b> text box and click <b>Find</b> .
<b>Find all of the desktop pools that follow the same naming convention</b>	Type a partial desktop pool name in the <b>Find</b> text box and click <b>Find</b> .

- 3 Select the desktop pools that you want to assign the ThinApp application to and click **Add**.  
You can press Ctrl+click or Shift+click to select multiple desktop pools.
- 4 Select an installation type and click **OK**.

Option	Action
<b>Streaming</b>	Installs a shortcut to the application on the machine. The shortcut points to the application on the network share that hosts the repository. Users must have access to the network share to run the application.
<b>Full</b>	Installs the full application on the machine's local file system.

Some ThinApp applications do not support both installation types. How the application package was created determines which installation types are available.

View Administrator begins installing the ThinApp application the first time a user logs in to a desktop in the pool. After the installation is finished, the application is available to all of the users of the desktop pool.

## Assign Multiple ThinApp Applications to a Desktop Pool

You can assign one more ThinApp applications to a particular desktop pool.

If you assign a ThinApp application to a linked-clone pool and later refresh, recompose, or rebalance the pool, View Administrator reinstalls the application for you. You do not have to manually reinstall the application.

### Prerequisites

Scan an application repository and add selected ThinApp applications to View Administrator. See [“Add ThinApp Applications to View Administrator,”](#) on page 214.

**Procedure**

- 1 In View Administrator, select **Catalog > Desktop Pools** and double-click the pool ID.
- 2 On the **Inventory** tab, click **ThinApps** and then click **Add Assignment**.  
The ThinApp applications that are not already assigned to the pool appear in the table.
- 3 To find a particular application, type the name of the ThinApp application in the **Find** text box and click **Find**.
- 4 Select a ThinApp application to assign to the pool and click **Add**.  
Repeat this step to select multiple applications.
- 5 Select an installation type and click **OK**.

Option	Action
<b>Streaming</b>	Installs a shortcut to the application on the machine. The shortcut points to the application on the network share that hosts the repository. Users must have access to the network share to run the application.
<b>Full</b>	Installs the full application on the machine's local file system.

Some ThinApp applications do not support both installation types. How the application package was created determines which installation types are available.

View Administrator begins installing the ThinApp applications the first time a user logs in to a desktop in the pool. After the installation is finished, the applications are available to all of the users of the desktop pool.

## Assign a ThinApp Template to a Machine or Desktop Pool

You can streamline the distribution of multiple ThinApp applications by assigning a ThinApp template to a machine or desktop pool.

When you assign a ThinApp template to a machine or desktop pool, View Administrator installs the ThinApp applications currently in the template.

**Prerequisites**

Create a ThinApp template. See [“Create a ThinApp Template,”](#) on page 214.

**Procedure**

- 1 In View Administrator, select **Catalog > ThinApps**.
- 2 Select the ThinApp template.
- 3 Select **Assign Machines** or **Assign Desktop Pools** from the **Add Assignment** drop-down menu.

All machines or desktop pools appear in the table.

Option	Action
<b>Find a specific machine or desktop pool</b>	Type the name of the machine or desktop pool in the <b>Find</b> text box and click <b>Find</b> .
<b>Find all of the machines or desktop pools that follow the same naming convention</b>	Type a partial machine or desktop pool name in the <b>Find</b> text box and click <b>Find</b> .

- 4 Select the machines or desktop pools that you want to assign the ThinApp template to and click **Add**.  
Repeat this step to select multiple machines or desktop pools.

- 5 Select an installation type and click **OK**.

Option	Action
<b>Streaming</b>	Installs a shortcut to the application on the machine. The shortcut points to the application on the network share that hosts the repository. Users must have access to the network share to run the application.
<b>Full</b>	Installs the full application on the machine's local file system.

Some ThinApp applications do not support both installation types. How the application package was created determines which installation types are available.

When you assign a ThinApp template to a machine, View Administrator begins installing the applications in the template a few minutes later. When you assign a ThinApp template to a desktop pool, View Administrator begins installing the applications in the template the first time a user logs in to a remote desktop in the desktop pool. After the installation is finished, the applications are available to all of the users of the machine or desktop pool.

View Administrator returns an application assignment error if a ThinApp template contains an application that is already assigned to the machine or desktop pool.

## Review ThinApp Application Assignments

You can review all of the machines and desktop pools that a particular ThinApp application is currently assigned to. You can also review all of the ThinApp applications that are assigned to a particular machine or desktop pool.

### Prerequisites

Familiarize yourself with the ThinApp installation status values in [“ThinApp Application Installation Status Values,”](#) on page 220.

### Procedure

- ◆ Select the ThinApp application assignments that you want to review.

Option	Action
<b>Review all of the machines and desktop pools that a particular ThinApp application is assigned to</b>	<p>Select <b>Catalog &gt; ThinApps</b> and double-click the name of the ThinApp application.</p> <p>The <b>Assignments</b> tab shows the machines and desktop pools that the application is currently assigned to, including the installation type.</p> <p>The <b>Machines</b> tab shows the machines that are currently associated with the application, including installation status information.</p> <p><b>NOTE</b> When you assign a ThinApp application to a pool, machines in the pool appear on the <b>Machines</b> tab only after the application is installed.</p>
<b>Review all of the ThinApp applications that are assigned to a particular machine</b>	<p>Select <b>Resources &gt; Machines</b> and double-click the name of the machine in Machine column.</p> <p>The ThinApps pane on <b>Summary</b> tab shows each application that is currently assigned to the machine, including the installation status.</p>
<b>Review all of the ThinApp applications that are assigned to a particular desktop pool</b>	<p>Select <b>Catalog &gt; Desktop Pools</b>, double-click the pool ID, select the <b>Inventory</b> tab, and click <b>ThinApps</b>.</p> <p>The ThinApp Assignments pane shows each application that is currently assigned to the desktop pool.</p>

## ThinApp Application Installation Status Values

After you assign a ThinApp application to a machine or pool, View Administrator indicates the status of the installation.

[Table 12-1](#) describes each status value.

**Table 12-1.** ThinApp Application Installation Status

Status	Description
Assigned	The ThinApp application is assigned to the machine.
Install Error	An error occurred when View Administrator attempted to install the ThinApp application.
Uninstall Error	An error occurred when View Administrator attempted to uninstall the ThinApp application.
Installed	The ThinApp application is installed.
Pending Install	View Administrator is attempting to install the ThinApp application. You cannot unassign an application that has this status. <b>NOTE</b> This value does not appear for machines in desktop pools.
Pending Uninstall	View Administrator is attempting to uninstall the ThinApp application.

## Display MSI Package Information

After you add a ThinApp application to View Administrator, you can display information about its MSI package.

### Procedure

- 1 In View Administrator, select **Catalog > ThinApps**.  
The **Summary** tab lists the applications that are currently available and shows the number of full and streaming assignments.
- 2 Double-click the name of the application in the ThinApp column.
- 3 Select the **Summary** tab to see general information about the MSI package.
- 4 Click **Package Info** to see detailed information about the MSI package.

## Maintaining ThinApp Applications in View Administrator

Maintaining ThinApp applications in View Administrator involves tasks such as removing ThinApp application assignments, removing ThinApp applications and application repositories, and modifying and deleting ThinApp templates.

**NOTE** To upgrade a ThinApp application, you must unassign and remove the older version of the application and add and assign the newer version.

- [Remove a ThinApp Application Assignment from Multiple Machines](#) on page 222  
You can remove an assignment to a particular ThinApp application from one or more machines.
- [Remove Multiple ThinApp Application Assignments from a Machine](#) on page 222  
You can remove assignments to one or more ThinApp applications from a particular machine.
- [Remove a ThinApp Application Assignment from Multiple Desktop Pools](#) on page 223  
You can remove an assignment to a particular ThinApp application from one or more desktop pools.
- [Remove Multiple ThinApp Application Assignments from a Desktop Pool](#) on page 223  
You can remove one or more ThinApp application assignments from a particular desktop pool.
- [Remove a ThinApp Application from View Administrator](#) on page 223  
When you remove a ThinApp application from View Administrator, you can no longer assign the application to machines and desktop pools.

- [Modify or Delete a ThinApp Template](#) on page 224  
You can add and remove applications from a ThinApp template. You can also delete a ThinApp template.
- [Remove an Application Repository](#) on page 224  
You can remove an application repository from View Administrator.

## Remove a ThinApp Application Assignment from Multiple Machines

You can remove an assignment to a particular ThinApp application from one or more machines.

### Prerequisites

Notify the users of the remote desktops that are hosted by the machines that you intend to remove the application.

### Procedure

- 1 In View Administrator, select **Catalog > ThinApps** and double-click the name of the ThinApp application.
- 2 On the **Assignments** tab, select a machine and click **Remove Assignment**.

You can press Ctrl+click or Shift+click to select multiple machines.

View Administrator uninstalls the ThinApp application a few minutes later.

---

**IMPORTANT** If an end user is using the ThinApp application at the time when View Administrator attempts to uninstall the application, the uninstallation fails and the application status changes to Uninstall Error. When this error occurs, you must first manually uninstall the ThinApp application files from the machine and then click **Remove App Status for Desktop** in View Administrator.

---

## Remove Multiple ThinApp Application Assignments from a Machine

You can remove assignments to one or more ThinApp applications from a particular machine.

### Prerequisites

Notify the users of the remote desktop that is hosted by the machine that you intend to remove the applications.

### Procedure

- 1 In View Administrator, select **Resources > Machines** and double-click the name of the machine in the Machine column.
- 2 On the **Summary** tab, select the ThinApp application and click **Remove Assignment** in the ThinApps pane.

Repeat this step to remove another application assignment.

View Administrator uninstalls the ThinApp application a few minutes later.

---

**IMPORTANT** If an end user is using the ThinApp application at the time when View Administrator attempts to uninstall the application, the uninstallation fails and the application status changes to Uninstall Error. When this error occurs, you must first manually uninstall the ThinApp application files from the machine and then click **Remove App Status For Desktop** in View Administrator.

---

## Remove a ThinApp Application Assignment from Multiple Desktop Pools

You can remove an assignment to a particular ThinApp application from one or more desktop pools.

### Prerequisites

Notify the users of the remote desktops in the pools that you intend to remove the application.

### Procedure

- 1 In View Administrator, select **Catalog > ThinApps** and double-click the name of the ThinApp application.
- 2 On the **Assignments** tab, select a desktop pool and click **Remove Assignment**.

You can press Ctrl+click or Shift+click to select multiple desktop pools.

View Administrator uninstalls the ThinApp application the first time a user logs in to a remote desktop in the pool.

## Remove Multiple ThinApp Application Assignments from a Desktop Pool

You can remove one or more ThinApp application assignments from a particular desktop pool.

### Prerequisites

Notify the users of the remote desktops in the pool that you intend to remove the applications.

### Procedure

- 1 In View Administrator, select **Catalog > Desktop Pools** and double-click the pool ID.
- 2 On the **Inventory** tab, click **ThinApps**, select the ThinApp application, and click **Remove Assignment**.  
Repeat this step to remove multiple applications.

View Administrator uninstalls the ThinApp applications the first time a user logs in to a remote desktop in the pool.

## Remove a ThinApp Application from View Administrator

When you remove a ThinApp application from View Administrator, you can no longer assign the application to machines and desktop pools.

You might need to remove a ThinApp application if your organization decides to replace it with a different vendor's application.

---

**NOTE** You cannot remove a ThinApp application if it is already assigned to a machine or desktop pool or if it is in the Pending Uninstall state.

---

### Prerequisites

If a ThinApp application is currently assigned to a machine or desktop pool, remove the assignment from the machine or desktop pool.

### Procedure

- 1 In View Administrator, select **Catalog > ThinApps** and select the ThinApp application.
- 2 Click **Remove ThinApp**.
- 3 Click **OK**.

## Modify or Delete a ThinApp Template

You can add and remove applications from a ThinApp template. You can also delete a ThinApp template.

If you add an application to a ThinApp template after assigning the template to a machine or desktop pool, View Administrator does not automatically assign the new application to the machine or desktop pool. If you remove an application from a ThinApp template that was previously assigned to a machine or desktop pool, the application remains assigned to the machine or desktop pool.

### Procedure

- ◆ In View Administrator, select **Catalog > ThinApps** and select the ThinApp template.

Option	Action
<b>Add or remove ThinApp applications from the template</b>	Click <b>Edit Template</b> .
<b>Delete the template</b>	Click <b>Remove Template</b> .

## Remove an Application Repository

You can remove an application repository from View Administrator.

You might need to remove an application repository if you no longer need the MSI packages that it contains, or if you need to move the MSI packages to a different network share. You cannot edit the share path of an application repository in View Administrator.

### Procedure

- 1 In View Administrator, select **View Configuration > ThinApp Configuration** and select the application repository.
- 2 Click **Remove Repository**.

## Monitoring and Troubleshooting ThinApp Applications in View Administrator

View Administrator logs events that are related to ThinApp application management to the Events and Reporting database. You can view these events on the **Events** page in View Administrator.

An event appears on the **Events** page when the following situations occur.

- A ThinApp application is assigned or an application assignment is removed
- A ThinApp application is installed or uninstalled on a machine
- A ThinApp application cannot be installed or uninstalled
- A ThinApp application repository is registered, modified, or removed from View Administrator
- A ThinApp application is added to View Administrator

Troubleshooting tips are available for common ThinApp application management problems.

## Cannot Register an Application Repository

You cannot register an application repository in View Administrator.

### Problem

You receive an error message when you attempt to register an application repository in View Administrator.

**Cause**

The View Connection Server host cannot access the network share that hosts the application repository. The network share path that you typed in the **Share path** text box might be incorrect, the network share that hosts the application repository is in a domain that is not accessible from the View Connection Server host, or the network share permissions have not been set up properly.

**Solution**

- If the network share path is incorrect, type the correct network share path. Network share paths that contain IP addresses are not supported.
- If the network share is not in an accessible domain, copy your application packages to a network share in a domain that is accessible from the View Connection Server host.
- Verify that the file and sharing permissions on the shared folder give Read access to the built-in Active Directory group Domain Computers. If you plan to assign ThinApps to domain controllers, verify that the file and sharing permissions also give Read access to the built-in Active Directory group Domain Controllers. After you set or change permissions, it can take up to 20 minutes for the network share to become accessible.

## Cannot Add ThinApp Applications to View Administrator

View Administrator cannot add ThinApp applications to View Administrator.

**Problem**

No MSI packages are available when you click **Scan New ThinApps** in View Administrator.

**Cause**

Either the application packages are not in MSI format or the View Connection Server host cannot access the directories in the network share.

**Solution**

- Verify that the application packages in the application repository are in MSI format.
- Verify that the network share meets View requirements for ThinApp applications. See [“View Requirements for ThinApp Applications,”](#) on page 211 for more information.
- Verify that the directories in the network share have the proper permissions. See [“Cannot Register an Application Repository,”](#) on page 224 for more information.

Messages appear in the View Connection Server debug log file when an application repository is scanned. View Connection Server log files are located on the View Connection Server host in the *drive*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs directory.

## Cannot Assign a ThinApp Template

You cannot assign a ThinApp template to a machine or desktop pool.

**Problem**

View Administrator returns an assignment error when you attempt to assign a ThinApp template to a machine or desktop pool.

**Cause**

Either the ThinApp template contains an application that is already assigned to the machine or desktop pool, or the ThinApp template was previously assigned to the machine or desktop pool with a different installation type.

## Solution

If the template contains a ThinApp application that is already assigned to the machine or desktop pool, create a new template that does not contain the application or edit the existing template and remove the application. Assign the new or modified template to the machine or desktop pool.

To change the installation type of a ThinApp application, you must remove the existing application assignment from the machine or desktop pool. After the ThinApp application is uninstalled, you can assign it to the machine or desktop pool with a different installation type.

## ThinApp Application Is Not Installed

View Administrator cannot install a ThinApp application.

### Problem

The ThinApp application installation status shows either Pending Install or Install Error.

### Cause

Common causes for this problem include the following:

- There was not enough disk space on the machine to install the ThinApp application.
- Network connectivity was lost between the View Connection Server host and the machine or between the View Connection Server host and the application repository.
- The ThinApp application was not accessible in the network share.
- The ThinApp application was previously installed or the directory or file already exists on the machine.

You can see the Horizon Agent and View Connection Server log files for more information about the cause of the problem.

Horizon Agent log files are located on the machine in *drive*:\ProgramData\VMware\VDM\logs.

View Connection Server log files are located on the View Connection Server host in the *drive*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs directory.

### Solution

- 1 In View Administrator, select **Catalog > ThinApps**.
- 2 Click the name of the ThinApp application.
- 3 On the **Machines** tab, select the machine and click **Retry Install** to reinstall the ThinApp application.

## ThinApp Application Is Not Uninstalled

View Administrator cannot uninstall a ThinApp application.

### Problem

The ThinApp application installation status shows Uninstall Error.

### Cause

Common causes for this error include the following:

- The ThinApp application was busy when View Administrator tried to uninstall it.
- Network connectivity was lost between the View Connection Server host and the machine.

You can see the Horizon Agent and View Connection Server log files for more information about the cause of the problem.

Horizon Agent log files are located on the machine in *drive:\Documents and Settings\All Users\Application Data\VMware\VDM\logs* for Windows XP systems and *drive:\ProgramData\VMware\VDM\logs* for Windows 7 systems.

View Connection Server log files are located on the View Connection Server host in the *drive:\Documents and Settings\All Users\Application Data\VMware\VDM\logs* directory.

### Solution

- 1 In View Administrator, select **Catalog > ThinApps**.
- 2 Click the name of the ThinApp application.
- 3 Click the **Machines** tab, select the machine, and click **Retry Uninstall** to retry the uninstall operation.
- 4 If the uninstall operation still fails, manually remove the ThinApp application from the machine and then click **Remove App Status For Desktop**.

This command clears the ThinApp application assignment in View Administrator. It does not remove any files or settings in the machine.

---

**IMPORTANT** Use this command only after manually removing the ThinApp application from the machine.

---

## MSI Package Is Invalid

View Administrator reports an invalid MSI package in an application repository.

### Problem

View Administrator reports that an MSI package is invalid during a scanning operation.

### Cause

Common causes of this problem include the following:

- The MSI file is corrupted.
- The MSI file was not created with ThinApp.
- The MSI file was created or repackaged with an unsupported version of ThinApp. You must use ThinApp version 4.6 or later.

### Solution

See the *ThinApp User's Guide* for information on troubleshooting problems with MSI packages.

## ThinApp Configuration Example

The ThinApp configuration example takes you step-by-step through a typical ThinApp configuration, beginning with capturing and packaging applications and ending with checking the status of an installation.

### Prerequisites

See these topics for complete information about how to perform the steps in this example.

- [“Capturing and Storing Application Packages,”](#) on page 212
- [“Assigning ThinApp Applications to Machines and Desktop Pools,”](#) on page 215

**Procedure**

- 1 Download the ThinApp software from <http://www.vmware.com/products/thinapp> and install it on a clean computer.  
View supports ThinApp version 4.6 and later.
- 2 Use the ThinApp Setup Capture wizard to capture and package your applications in MSI format.
- 3 Create a shared folder on a computer in an Active Directory domain that is accessible to both your View Connection Server host and your remote desktops and configure the file and sharing permissions on the shared folder to give Read access to the built-in Active Directory group Domain Computers.

If you plan to assign ThinApp applications to domain controllers, also give Read access to the built-in Active Directory group Domain Controllers.

- 4 Copy your MSI packages to the shared folder.
- 5 Register the shared folder as an application repository in View Administrator.
- 6 In View Administrator, scan the MSI packages in the application repository and add selected ThinApp applications to View Administrator.
- 7 Decide whether to assign the ThinApp applications to machines or desktop pools.

If you use a common naming convention for your machines, you can use machine assignments to quickly distribute applications to all of the machines that use that naming convention. If you organize your desktop pools by department or user type, you can use desktop pool assignments to quickly distribute applications to specific departments or users.

- 8 In View Administrator, select the ThinApp applications to assign to your machines or desktop pools and specify the installation method.

Option	Action
<b>Streaming</b>	Installs a shortcut to the application on the machine. The shortcut points to the application on the network share that hosts the repository. Users must have access to the network share to run the application.
<b>Full</b>	Installs the full application on the machine's local file system.

- 9 In View Administrator, check the installation status of the ThinApp applications.

## Setting Up Clients in Kiosk Mode

---

You can set up unattended clients that can obtain access to their desktops from View.

A client in kiosk mode is a thin client or a lock-down PC that runs Horizon Client to connect to a View Connection Server instance and launch a remote session. End users do not typically need to log in to access the client device, although the remote desktop might require them to provide authentication information for some applications. Sample applications include medical data entry workstations, airline check-in stations, customer self-service points, and information terminals for public access.

You should ensure that the desktop application implements authentication mechanisms for secure transactions, that the physical network is secure against tampering and snooping, and that all devices connected to the network are trusted.

Clients in kiosk mode support the standard features for remote access such as automatic redirection of USB devices to the remote session and location-based printing.

View uses the Flexible Authentication feature in View 4.5 and later to authenticate a client device in kiosk mode rather than the end user. You can configure a View Connection Server instance to authenticate clients that identify themselves by their MAC address or by a user name that starts with the characters "custom-" or with an alternate prefix string that you have defined in ADAM. If you configure a client to have an automatically generated password, you can run Horizon Client on the device without specifying a password. If you configure an explicit password, you must specify this password to Horizon Client. As you would usually run Horizon Client from a script, and the password would appear in clear text, you should take precautions to make the script unreadable by unprivileged users.

Only View Connection Server instances that you enable to authenticate clients in kiosk mode can accept connections from accounts that start with the characters "cm-" followed by a MAC address, or that start with the characters "custom-" or an alternate string that you have defined. Horizon Client in View 4.5 and later does not allow the manual entry of user names that take these forms.

As a best practice, use dedicated View Connection Server instances to handle clients in kiosk mode, and to create dedicated organizational units and groups in Active Directory for the accounts of these clients. This practice not only partitions these systems against unwarranted intrusion, but also makes it easier to configure and administer the clients.

## Configure Clients in Kiosk Mode

To configure Active Directory and View to support clients in kiosk mode, you must perform several tasks in sequence.

### Prerequisites

Verify that you have the privileges required to perform the configuration tasks.

- **Domain Admins** or **Account Operators** credentials in Active Directory to make changes to the accounts of users and groups in a domain.

- **Administrators, Inventory Administrators**, or an equivalent role to use View Administrator to entitle users or groups to remote desktops.
- **Administrators** or an equivalent role to run the `vdadmin` command.

### Procedure

- 1 [Prepare Active Directory and View for Clients in Kiosk Mode](#) on page 230  
You must configure Active Directory to accept the accounts that you create to authenticate client devices. Whenever you create a group, you must also entitle that group to the desktop pool that a client accesses. You can also prepare the desktop pool that the clients use.
- 2 [Set Default Values for Clients in Kiosk Mode](#) on page 231  
You can use the `vdadmin` command to set the default values for the organizational unit, password expiry, and group membership in Active Directory for clients in kiosk mode.
- 3 [Display the MAC Addresses of Client Devices](#) on page 232  
If you want to create an account for a client that is based on its MAC address, you can use Horizon Client to discover the MAC address of the client device.
- 4 [Add Accounts for Clients in Kiosk Mode](#) on page 233  
You can use the `vdadmin` command to add accounts for clients to the configuration of a View Connection Server group. After you add a client, it is available for use with a View Connection Server instance on which you have enabled authentication of clients. You can also update the configuration of clients, or remove their accounts from the system.
- 5 [Enable Authentication of Clients in Kiosk Mode](#) on page 234  
You can use the `vdadmin` command to enable authentication of clients that attempt to connect to their remote desktops via a View Connection Server instance.
- 6 [Verify the Configuration of Clients in Kiosk Mode](#) on page 235  
You can use the `vdadmin` command to display information about clients in kiosk mode and View Connection Server instances that are configured to authenticate such clients.
- 7 [Connect to Remote Desktops from Clients in Kiosk Mode](#) on page 236  
You can run the client from the command line or use a script to connect a client to a remote session.

## Prepare Active Directory and View for Clients in Kiosk Mode

You must configure Active Directory to accept the accounts that you create to authenticate client devices. Whenever you create a group, you must also entitle that group to the desktop pool that a client accesses. You can also prepare the desktop pool that the clients use.

As a best practice, create a separate organizational unit and group to help minimize your work in administering clients in kiosk mode. You can add individual accounts for clients that do not belong to any group, but this creates a large administrative overhead if you configure more than a small number of clients.

### Procedure

- 1 In Active Directory, create a separate organizational unit and group to use with clients in kiosk mode.  
You must specify a pre-Windows 2000 name for the group. You use this name to identify the group to the `vdadmin` command.
- 2 Create the image or template for the guest virtual machine.  
You can use a virtual machine that is managed by vCenter Server as a template for an automated pool, as a parent for a linked-clone pool, or as a virtual machine in a manual desktop pool. You can also install and configure applications on the guest operating system.

- 3 Configure the guest operating system so that the clients are not locked when they are left unattended.

View suppresses the pre-login message for clients that connect in kiosk mode. If you require an event to unlock the screen and display a message, you can configure a suitable application on the guest operating system.

- 4 In View Administrator, create the desktop pool that the clients will use and entitle the group to this pool.

For example, you might choose to create a floating-assignment, linked-clone desktop pool as being most suitable for the requirements of your client application. You might also associate one or more ThinApp applications with the desktop pool.

---

**IMPORTANT** Do not entitle a client or a group to more than one desktop pool. If you do, View assigns a remote desktop at random from the pools to which a client is entitled, and generates a warning event.

---

- 5 If you want to enable location-based printing for the clients, configure the Active Directory group policy setting `AutoConnect Location-based Printing for VMware View`, which is located in the Microsoft Group Policy Object Editor in the `Software Settings` folder under `Computer Configuration`.
- 6 Configure other policies that you need to optimize and secure the remote desktops of the clients.

For example, you might want to override the policies that connect local USB devices to the remote desktop when it is launched or when the devices are plugged in. By default, Horizon Client for Windows enables these policies for clients in kiosk mode.

### Example: Preparing Active Directory for Clients in Kiosk Mode

A company intranet has a domain MYORG, and its organizational unit has the distinguished name `OU=myorg-ou,DC=myorg,DC=com`. In Active Directory, you create the organizational unit `kiosk-ou` with the distinguished name `OU=kiosk-ou,DC=myorg,DC=com` and the group `kc-grp` for use with clients in kiosk mode.

#### What to do next

Set default values for the clients.

## Set Default Values for Clients in Kiosk Mode

You can use the `vdadmin` command to set the default values for the organizational unit, password expiry, and group membership in Active Directory for clients in kiosk mode.

You must run the `vdadmin` command on one of the View Connection Server instances in the group that contains the View Connection Server instance that clients will use to connect to their remote desktops.

When you configure defaults for password expiry and Active Directory group membership, these settings are shared by all View Connection Server instances in a group.

#### Procedure

- ◆ Set the default values for clients.

```
vdadmin -Q -clientauth -setdefaults [-b authentication_arguments] [-ou DN]
[-expirepassword | -noexpirepassword] [-group group_name | -nogroup]
```

Option	Description
<b>-expirepassword</b>	Specifies that the expiry time for passwords on the client accounts is the same as for the View Connection Server group. If no expiry time is defined for the group, passwords do not expire.
<b>-group group_name</b>	Specifies the name of the default group to which client accounts are added. The name of the group must be specified as the pre-Windows 2000 group name from Active Directory.

Option	Description
<b>-noexpirepassword</b>	Specifies that passwords on client accounts do not expire.
<b>-nogroup</b>	Clears the setting for the default group.
<b>-ou DN</b>	Specifies the distinguished name of the default organizational unit to which client accounts are added. For example: OU=kiosk-ou,DC=myorg,DC=com <b>NOTE</b> You cannot use the command to change the configuration of an organizational unit.

The command updates the default values for clients in the View Connection Server group.

### Example: Setting Default Values for Clients in Kiosk Mode

Set the default values for the organizational unit, password expiry, and group membership of clients.

```
vdmadmin -Q -clientauth -setdefaults -ou "OU=kiosk-ou,DC=myorg,DC=com" -noexpirepassword -group kc-grp
```

#### What to do next

Find out the MAC addresses of client devices that use their MAC address for authentication.

## Display the MAC Addresses of Client Devices

If you want to create an account for a client that is based on its MAC address, you can use Horizon Client to discover the MAC address of the client device.

#### Prerequisites

Log in on the console of the client.

#### Procedure

- ◆ To display the MAC address, type the appropriate command for your platform.

Option	Action
<b>Windows</b>	Enter <b>C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -printEnvironmentInfo</b> The client uses the default View Connection Server instance that you configured for it. If you have not configured a default value, the client prompts you for the value. The command displays the IP address, MAC address, and machine name of the client device.
<b>Linux</b>	Enter <b>vmware-view --printEnvironmentInfo -s connection_server</b> You must specify the IP address or FQDN of the View Connection Server instance that the client will use to connect to the desktop. The command displays the IP address, MAC address, machine name, domain, name and domain of any logged-on user, and time zone of the client device.

#### What to do next

Add accounts for the clients.

## Add Accounts for Clients in Kiosk Mode

You can use the `vdmadmin` command to add accounts for clients to the configuration of a View Connection Server group. After you add a client, it is available for use with a View Connection Server instance on which you have enabled authentication of clients. You can also update the configuration of clients, or remove their accounts from the system.

You must run the `vdmadmin` command on one of the View Connection Server instances in the group that contains the View Connection Server instance that clients will use to connect to their remote desktops.

When you add a client in kiosk mode, View creates a user account for the client in Active Directory. If you specify a name for a client, this name must start with a recognized prefix string, such as "custom-", or with an alternate prefix string that you have defined in ADAM, and it cannot be more than 20 characters long. If you do not specify a name for a client, View generates a name from the MAC address that you specify for the client device. For example, if the MAC address is 00:10:db:ee:76:80, the corresponding account name is cm-00\_10\_db\_ee\_76\_80. You can only use these accounts with View Connection Server instances that you enable to authenticate clients.

---

**IMPORTANT** Do not use a specified name with more than one client device. Future releases might not support this configuration.

---

### Procedure

- ◆ Run the `vdmadmin` command using the `-domain` and `-clientid` options to specify the domain and the name or the MAC address of the client.

```
vdmadmin -Q -clientauth -add [-b authentication_arguments] -domain domain_name -clientid
client_id [-password "password" | -genpassword] [-ou DN] [-expirepassword |
-noexpirepassword] [-group group_name | -nogroup] [-description "description_text"]
```

Option	Description
<code>-clientid client_id</code>	Specifies the name or the MAC address of the client.
<code>-description "description_text"</code>	Creates a description of the account for the client device in Active Directory.
<code>-domain domain_name</code>	Specifies the domain for the client.
<code>-expirepassword</code>	Specifies that the expiry time for the password on the client's account is the same as for the View Connection Server group. If no expiry time is defined for the group, the password does not expire.
<code>-genpassword</code>	Generates a password for the client's account. This is the default behavior if you do not specify either <code>-password</code> or <code>-genpassword</code> . A generated password is 16 characters long, contains at least one uppercase letter, one lowercase letter, one symbol, and one number, and can contain repeated characters. If you require a stronger password, use the <code>-password</code> option to specify the password.
<code>-group group_name</code>	Specifies the name of the group to which the client's account is added. The name of the group must be specified as the pre-Windows 2000 group name from Active Directory. If you previously set a default group, client's account is added to this group.
<code>-noexpirepassword</code>	Specifies that the password on the client's account does not expire.
<code>-nogroup</code>	Specifies that the client's account is not added to the default group.
<code>-ou DN</code>	Specifies the distinguished name of the organizational unit to which the client's account is added. For example: OU=kiosk-ou,DC=myorg,DC=com
<code>-password "password"</code>	Specifies an explicit password for the client's account.

The command creates a user account in Active Directory for the client in the specified domain and group (if any).

### Example: Adding Accounts for Clients

Add an account for a client specified by its MAC address to the MYORG domain, using the default settings for the group kc-grp.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -group kc-grp
```

Add an account for a client specified by its MAC address to the MYORG domain, using an automatically generated password.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -genpassword
```

Add an account for a named client, and specify a password to be used with the client.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid custom-Terminal21 -password "guest" -ou "OU=kiosk-ou,DC=myorg,DC=com" -description "Terminal 21"
```

Add an account for a named client, using an automatically generated password.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid custom-Kiosk11 -genpassword -ou "OU=kiosk-ou,DC=myorg,DC=com" -description "Kiosk 11"
```

### What to do next

Enable authentication of the clients.

## Enable Authentication of Clients in Kiosk Mode

You can use the `vdmadmin` command to enable authentication of clients that attempt to connect to their remote desktops via a View Connection Server instance.

You must run the `vdmadmin` command on one of the View Connection Server instances in the group that contains the View Connection Server instance that clients will use to connect to their remote desktops.

Although you enable authentication for an individual View Connection Server instance, all View Connection Server instances in a group share all other settings for client authentication. You need only add an account for a client once. In a View Connection Server group, any enabled View Connection Server instance can authenticate the client.

If you plan to use kiosk mode with a session-based View desktop on an RDS host, you must also add the user account to the Remote Desktop Users group.

### Procedure

- 1 Enable authentication of clients on a View Connection Server instance.

```
vdmadmin -Q -enable [-b authentication_arguments] -s connection_server [-requirepassword]
```

Option	Description
<b>-requirepassword</b>	Specifies that you require clients to provide passwords. <b>IMPORTANT</b> If you specify this option, the View Connection Server instance cannot authenticate clients that have automatically generated passwords. If you change the configuration of a View Connection Server instance to specify this option, such clients cannot authenticate themselves and they fail with the error message <code>Unknown username or bad password</code> .
<b>-s connection_server</b>	Specifies the NetBIOS name of the View Connection Server instance on which to enable authentication of clients.

The command enables the specified View Connection Server instance to authenticate clients.

- 2 If the remote desktop is provided by a Microsoft RDS host, log in to the RDS host and add the user account to the Remote Desktop Users group.

For example, say that on the View server, you entitle the user account custom-11 to a session-based View desktop on an RDS host. You must then log in to the RDS host, and add the user custom-11 to the Remote Desktop Users group by going to **Control Panel > System and Security > System > Remote settings > Select users > Add**.

### Example: Enabling Authentication of Clients in Kiosk Mode

Enable authentication of clients for the View Connection Server instance csvr-2. Clients with automatically generated passwords can authenticate themselves without providing a password.

```
vdadmin -Q -enable -s csvr-2
```

Enable authentication of clients for the View Connection Server instance csvr-3, and require that the clients specify their passwords to Horizon Client. Clients with automatically generated passwords cannot authenticate themselves.

```
vdadmin -Q -enable -s csvr-3 -requirepassword
```

### What to do next

Verify the configuration of the View Connection Server instances and the clients.

## Verify the Configuration of Clients in Kiosk Mode

You can use the `vdadmin` command to display information about clients in kiosk mode and View Connection Server instances that are configured to authenticate such clients.

You must run the `vdadmin` command on one of the View Connection Server instances in the group that contains the View Connection Server instance that clients will use to connect to their remote desktops.

### Procedure

- ◆ Display information about clients in kiosk mode and client authentication.

```
vdadmin -Q -clientauth -list [-b authentication_arguments] [-xml]
```

The command displays information about clients in kiosk mode and the View Connection Server instances on which you have enabled client authentication.

### Example: Displaying Information for Clients in Kiosk Mode

Display information about clients in text format. Client cm-00\_0c\_29\_0d\_a3\_e6 has an automatically generated password, and does not require an end user or an application script to specify this password to Horizon Client. Client cm-00\_22\_19\_12\_6d\_cf has an explicitly specified password and requires the end user to provide this. The View Connection Server instance CONSVR2 accepts authentication requests from clients with automatically generated passwords. CONSVR1 does not accept authentication requests from clients in kiosk mode.

```
C:\> vdadmin -Q -clientauth -list
Client Authentication User List
=====
GUID                : 94be6344-0c9b-4a92-8d54-1brc1c2dc282
ClientID            : cm-00_0c_29_0d_a3_e6
Domain              : myorg.com
Password Generated: true

GUID                : 471d9d35-68b2-40ee-b693-56a7d92b2e25
ClientID            : cm-00_22_19_12_6d_cf
Domain              : myorg.com
```

Password Generated: false

#### Client Authentication Connection Servers

=====

Common Name : CONSVR1

Client Authentication Enabled : false

Password Required : false

Common Name : CONSVR2

Client Authentication Enabled : true

Password Required : false

#### What to do next

Verify that the clients can connect to their remote desktops.

## Connect to Remote Desktops from Clients in Kiosk Mode

You can run the client from the command line or use a script to connect a client to a remote session.

You would usually use a command script to run Horizon Client on a deployed client device.

---

**Note** On a Windows or Mac client, by default USB devices on the client are not forwarded automatically if they are in use by another application or service when the remote desktop session starts. On all clients, human interface devices (HIDs) and smart card readers are not forwarded by default.

---

## Procedure

- ◆ To connect to a remote session, type the appropriate command for your platform.

Option	Description
<b>Windows</b>	<p>Enter  <b>C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -unattended [-serverURL connection_server] [-userName user_name] [-password password]</b></p> <p><b>-password password</b> Specifies the password for the client's account. If you defined a password for the account, you must specify this password.</p> <p><b>-serverURL connection_server</b> Specifies the IP address or FQDN of the View Connection Server instance that Horizon Client will use to connect to its remote desktop. If you do not specify the IP address or FQDN of the View Connection Server instance that the client will use to connect to its remote desktop, the client uses the default View Connection Server instance that you configured for it.</p> <p><b>-userName user_name</b> Specifies the name of the client's account. If you want a client to authenticate itself using an account name that begins with a recognized prefix string, such as "custom-", rather than using its MAC address, you must specify this name.</p>
<b>Linux</b>	<p>Enter  <b>vmware-view --unattended -s connection_server [--once] [-u user_name] [-p password]</b></p> <p><b>--once</b> Specifies that you do not want Horizon Client to retry connecting in the case of an error occurring.  <b>IMPORTANT</b> You should usually specify this option, and use the exit code to handle the error. Otherwise, you might find it difficult to kill the vmware-view process remotely.</p> <p><b>-p password</b> Specifies the password for the client's account. If you defined a password for the account, you must specify this password.</p> <p><b>-s connection_server</b> Specifies the IP address or FQDN of the View Connection Server instance that the client will use to connect to its desktop.</p> <p><b>-u user_name</b> Specifies the name of the client's account. If you want a client to authenticate itself using an account name that begins with a recognized prefix string, such as "custom-", rather than using its MAC address, you must specify this name.</p>

If the server authenticates the kiosk client and a remote desktop is available, the command starts the remote session.

## Example: Running Horizon Client on Clients in Kiosk Mode

Run Horizon Client on a Windows client whose account name is based on its MAC address, and which has an automatically generated password.

```
C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -unattended -serverURL consvr2.myorg.com
```

Run Horizon Client on a Linux client using an assigned name and password.

```
vmware-view -unattended -s 145.124.24.100 --once -u custom-Terminal21 -p "Secret1!"
```

# Troubleshooting View

---

You can use a variety of procedures for diagnosing and fixing problems that you might encounter when using View. You can use troubleshooting procedures to investigate the causes of such problems and attempt to correct them yourself, or you can obtain assistance from VMware Technical Support.

For information about troubleshooting desktops and desktop pools, see the *Setting Up Virtual Desktops in Horizon 7* document.

This chapter includes the following topics:

- [“Monitoring System Health,”](#) on page 239
- [“Monitor Events in View,”](#) on page 240
- [“Collecting Diagnostic Information for View,”](#) on page 241
- [“Update Support Requests,”](#) on page 245
- [“Troubleshooting an Unsuccessful Security Server Pairing with View Connection Server,”](#) on page 245
- [“Troubleshooting View Server Certificate Revocation Checking,”](#) on page 246
- [“Troubleshooting Smart Card Certificate Revocation Checking,”](#) on page 247
- [“Further Troubleshooting Information,”](#) on page 247

## Monitoring System Health

You can use the system health dashboard in View Administrator to quickly see problems that might affect the operation of View or access to remote desktops by end users.

The system health dashboard in the top left of the View Administrator display provides a number of links that you can use to view reports about the operation of View:

<b>Sessions</b>	Provides a link to the Sessions screen, which displays information about the status of remote desktop and application sessions.
<b>Problem vCenter VMs</b>	Provides a link to the Machines screen, which displays information about vCenter virtual machines, RDS hosts, other machines that View has flagged as having problems.
<b>Problem RDS Hosts</b>	Provides a link to the <b>RDS Hosts</b> tab on the Machines screen, which displays information about RDS hosts that View has flagged as having problems.

<b>Events</b>	Provides links to the Events screen filtered for error events and for warning events.
<b>System Health</b>	Provides links to the Dashboard screen, which displays summaries of the status of View components, vSphere components, domains, desktops, and datastore usage.

The system health dashboard displays a numbered link against each item. This value indicates the number of items that the linked report provides details about.

## Monitor Events in View

The event database stores information about events that occur in the View Connection Server host or group, Horizon Agent, and View Administrator, and notifies you of the number of events on the dashboard. You can examine the events in detail on the Events screen.

---

**NOTE** Events are listed in the View Administrator interface for a limited time period. After this time, the events are only available in the historical database tables. You can use Microsoft SQL Server or Oracle database reporting tools to examine events in the database tables. For more information, see the *View Integration* document.

---

In addition to monitoring events in View Administrator, you can generate View events in Syslog format so that the event data can be accessible to analytics software. See [“Generating View Event Log Messages in Syslog Format Using the -I Option,”](#) on page 259 and “Configure Event Logging for Syslog Servers” in the *View Installation* document.

### Prerequisites

Create and configure the event database as described in the *View Installation* document.

### Procedure

- 1 In View Administrator, select **Monitoring > Events**.
- 2 (Optional) In the Events window, you can select the time range of the events, apply filtering to the events, and sort the listed events by one or more of the columns.

## View Event Messages

View reports events whenever the state of the system changes or it encounters a problem. You can use the information in the event messages to take the appropriate action.

[Table 14-1](#) shows the types of events that View reports.

**Table 14-1.** Types of Event Reported by View

Event Type	Description
Audit Failure or Audit Success	Reports the failure or success of a change that an administrator or user makes to the operation or configuration of View.
Error	Reports a failed operation by View.
Information	Reports normal operations within View.
Warning	Reports minor problems with operations or configuration settings that might lead to more serious problems over time.

You might need to take some action if you see messages that are associated with Audit Failure, Error, or Warning events. You do not need to take any action for Audit Success or Information events.

## Collecting Diagnostic Information for View

You can collect diagnostic information to help VMware Technical Support diagnose and resolve issues with View.

You can collect diagnostic information for various components of View. How you collect this information varies depending on the View component.

- [Create a Data Collection Tool Bundle for Horizon Agent](#) on page 241

To assist VMware Technical Support in troubleshooting Horizon Agent, you might need to use the `vdadmin` command to create a Data Collection Tool (DCT) bundle. You can also obtain the DCT bundle manually, without using `vdadmin`.

- [Save Diagnostic Information for Horizon Client](#) on page 242

If you encounter problems using Horizon Client, and cannot resolve the problems using general network troubleshooting techniques, you can save a copy of the log files and information about the configuration.

- [Collect Diagnostic Information for View Composer Using the Support Script](#) on page 243

You can use the View Composer support script to collect configuration data and generate log files for View Composer. This information helps VMware customer support diagnose any issues that arise with View Composer.

- [Collect Diagnostic Information for Horizon Connection Server](#) on page 243

You can use the support tool to set logging levels and generate log files for Horizon Connection Server.

- [Collect Diagnostic Information for Horizon Agent, Horizon Client, or Horizon Connection Server from the Console](#) on page 244

If you have direct access to the console, you can use the support scripts to generate log files for Connection Server, Horizon Client, or remote desktops that are running Horizon Agent. This information helps VMware Technical Support diagnose any issues that arise with these components.

### Create a Data Collection Tool Bundle for Horizon Agent

To assist VMware Technical Support in troubleshooting Horizon Agent, you might need to use the `vdadmin` command to create a Data Collection Tool (DCT) bundle. You can also obtain the DCT bundle manually, without using `vdadmin`.

For your convenience, you can use the `vdadmin` command on a View Connection Server instance to request a DCT bundle from a remote desktop. The bundle is returned to View Connection Server.

You can alternatively log in to a specific remote desktop and run a support command that creates the DCT bundle on that desktop. If User Account Control (UAC) is turned on, you must obtain the DCT bundle in this fashion.

#### Procedure

- 1 Log in as a user with the required privileges.

Option	Action
<b>On View Connection Server, using <code>vdadmin</code></b>	Log in to a standard or replica instance View Connection Server as a user with the <b>Administrators</b> role.
<b>On the remote desktop</b>	Log in to the remote desktop as a user with administrative privileges.

- 2 Open a command prompt and run the command to generate the DCT bundle.

Option	Action
<b>On View Connection Server, using vdmadmin</b>	To specify the names of the output bundle file, desktop pool, and machine, use the <code>-outfile</code> , <code>-d</code> , and <code>-m</code> options with the <code>vdmadmin</code> command. <code>vdmadmin -A [-b authentication_arguments] -getDCT -outfile local_file -d desktop -m machine</code>
<b>On the remote desktop</b>	Change directories to <code>c:\Program Files\VMware\VMware View\Agent\DCT</code> and run the following command: <code>support</code>

The command writes the bundle to the specified output file.

### Example: Using vdmadmin to Create a Bundle File for Horizon Agent

Create the DCT bundle for the machine `machine1` in the desktop pool `dtpool2` and write it to the zip file `C:\myfile.zip`.

```
vdmadmin -A -d dtpool2 -m machine1 -getDCT -outfile C:\myfile.zip
```

#### What to do next

If you have an existing support request, you can update it by attaching the DCT bundle file.

## Save Diagnostic Information for Horizon Client

If you encounter problems using Horizon Client, and cannot resolve the problems using general network troubleshooting techniques, you can save a copy of the log files and information about the configuration.

You can attempt to resolve connection problems for Horizon Client before saving the diagnostic information and contacting VMware Technical Support. For more information, see "Connection Problems Between Horizon Client and Horizon Connection Server" in the *Setting Up Virtual Desktops in Horizon 7* document.

#### Procedure

- 1 In Horizon Client, click **Support Information**, or, on the remote desktop menu, select **Options > Support Information**.
- 2 In the Support Information window, click **Collect Support Data** and click **Yes** when prompted.  
A command window shows the progress of gathering the information. This process can take several minutes.
- 3 In the command window, respond to the prompts by entering the URLs of the Horizon Connection Server instances against which you want to test the configuration of Horizon Client, and, if required, selecting to generate diagnostic dumps of the Horizon 7 processes.  
The information is written to a zip file in a folder on the client machine's desktop.
- 4 File a support request on the Support page of the VMware Web site, and attach the output zip file.

## Collect Diagnostic Information for View Composer Using the Support Script

You can use the View Composer support script to collect configuration data and generate log files for View Composer. This information helps VMware customer support diagnose any issues that arise with View Composer.

### Prerequisites

Log in to the computer on which View Composer is installed.

Because you must use the Windows Script Host utility (cscript) to run the support script, familiarize yourself with using cscript. See <http://technet.microsoft.com/library/bb490887.aspx>.

### Procedure

- 1 Open a command prompt window and change to the C:\Program Files\VMware\VMware View Composer directory.

If you did not install the software in the default directories, substitute the appropriate drive letter and path.

- 2 Type the command to run the svi-support script.

```
cscript ".\svi-support.wsf" /zip
```

You can use the /? option to display information about other command options that are available with the script.

When the script finishes, it informs you of the name and location of the output file.

- 3 File a support request on the Support page of the VMware Web site and attach the output file.

## Collect Diagnostic Information for Horizon Connection Server

You can use the support tool to set logging levels and generate log files for Horizon Connection Server.

The support tool collects logging data for Connection Server. This information helps VMware Technical Support diagnose any issues that arise with Connection Server. The support tool is not intended to collect diagnostic information for Horizon Client or Horizon Agent. You must instead use the support script. See [“Collect Diagnostic Information for Horizon Agent, Horizon Client, or Horizon Connection Server from the Console,”](#) on page 244.

### Prerequisites

Log in to a standard or replica instance of the Connection Server as a user in the **Administrators** role.

### Procedure

- 1 Select **Start > All Programs > VMware > Set View Connection Server Log Levels**.
- 2 In the **Choice** text box, type a numeric value to set the logging level and press Enter.

Option	Description
<b>0</b>	Resets the logging level to the default value.
<b>1</b>	Selects a normal level of logging.
<b>2</b>	Selects a debug level of logging (default).
<b>3</b>	Selects full logging.

The system starts recording log information with the level of detail that you have selected.

- 3 When you have collected enough information about the behavior of Connection Server, select **Start > All Programs > VMware > Generate View Connection Server Log Bundle**.

The support tool writes the log files to a folder called `vdm-sdct` on the desktop of the Connection Server instance.

- 4 File a support request on the Support page of the VMware Web site and attach the output files.

## Collect Diagnostic Information for Horizon Agent , Horizon Client, or Horizon Connection Server from the Console

If you have direct access to the console, you can use the support scripts to generate log files for Connection Server, Horizon Client, or remote desktops that are running Horizon Agent. This information helps VMware Technical Support diagnose any issues that arise with these components.

### Prerequisites

Log in to the system that you want to collect information for. You must log in as a user with administrator privileges.

- For Horizon Agent, log in to the virtual machine that has Horizon Agent installed.
- For Horizon Client, log in to the system with Horizon Client installed.
- For Connection Server, log in to the Connection Server host.

### Procedure

- 1 Open a command prompt window and change to the appropriate directory for the Horizon 7 component that you want to collect diagnostic information for.

Option	Description
<b>Horizon Agent</b>	Change to the <code>C:\Program Files\VMware View\Agent\DCT</code> directory.
<b>Horizon Client</b>	Change to the <code>C:\Program Files\VMware View\Client\DCT</code> directory.
<b>View Connection Server</b>	Change to the <code>C:\Program Files\VMware View\Server\DCT</code> directory.

If you did not install the software in the default directories, substitute the appropriate drive letter and path.

- 2 Type the command to run the support script.

```
.\support.bat [loglevels]
```

If you want to enable advanced logging, specify the `loglevels` option and enter the numeric value for the logging level when prompted.

Option	Description
<b>0</b>	Resets the logging level to the default value.
<b>1</b>	Selects a normal level of logging.
<b>2</b>	Selects a debug level of logging (default).
<b>3</b>	Selects full logging.
<b>4</b>	Selects informational logging for PCoIP (Horizon Agent and Horizon Client only).
<b>5</b>	Selects debug logging for PCoIP (Horizon Agent and Horizon Client only).
<b>6</b>	Selects informational logging for virtual channels (Horizon Agent and Horizon Client only).

Option	Description
7	Selects debug logging for virtual channels (Horizon Agent and Horizon Client only).
8	Selects trace logging for virtual channels (Horizon Agent and Horizon Client only).

The script writes the zipped log files to the folder `vdm-sdct` on the desktop.

- 3 You can find the View Composer guest agent logs in the `C:\Program Files\Common Files\VMware\View Composer Guest Agent svi-ga-support` directory.
- 4 File a support request on the Support page of the VMware Web site and attach the output file.

## Update Support Requests

You can update your existing support request at the Support Web site.

After you file a support request, you might receive an email request from VMware Technical Support asking for the output file from the `support` or `svi-support` scripts. When you run the scripts, they inform you of the name and location of the output file. Reply to the email message and attach the output file to the reply.

If the output file is too large to include as an attachment (10MB or more), contact VMware Technical Support, tell them the number of your support request, and request FTP upload instructions. Alternatively, you can attach the file to your existing support request at the Support Web site.

### Procedure

- 1 Visit the Support page at the VMware Web site and log in.
- 2 Click **Support Request History** and find the applicable support request number.
- 3 Update the support request and attach the output that you obtained by running the `support` or `svi-support` script.

## Troubleshooting an Unsuccessful Security Server Pairing with View Connection Server

A security server might not be working if it failed to pair successfully with a View Connection Server instance.

### Problem

The following security server issues might occur if a security server failed to pair with View Connection Server:

- When you try to install the security server a second time, the security server cannot connect to View Connection Server.
- Horizon Client cannot connect to View. The following error message appears: The View Connection Server authentication failed. No gateway is available to provide a secure connection to a desktop. Contact your network administrator.
- The security server is displayed in the View Administrator dashboard as Down.

### Cause

This problem can occur if you started to install a security server and the attempt was cancelled or otherwise aborted after you entered a security server pairing password.

## Solution

If you intend to keep the security server in your View environment, take these steps:

- 1 In View Administrator, select **View Configuration > Servers**.
- 2 On the **Security Servers** tab, select a security server, select **Prepare for Upgrade or Reinstallation** from the **More Commands** drop-down menu, and click **OK**.
- 3 On the **Connection Servers** tab, select the View Connection Server instance that you want to pair with the security server, select **Specify Security Server Pairing Password** from the **More Commands** drop-down menu, type a password, and click **OK**.
- 4 Install the security server again.

If you intend to remove the security server entry from your View environment, run the `vdadmin -S` command.

For example: `vdadmin -S -r -s security_server_name`

## Troubleshooting View Server Certificate Revocation Checking

A security server or a View Connection Server instance that is used for secure Horizon Client connections might show as red in View Administrator if certificate revocation checking cannot be performed on the server's SSL certificate.

### Problem

A security server or View Connection Server icon is red on the View Administrator dashboard. The View server's status shows the following message: `Server's certificate cannot be checked`.

### Cause

Certificate revocation checking might fail if your organization uses a proxy server for Internet access, or if a View Connection Server instance cannot reach the servers that provide revocation checking because of firewalls or other controls.

A View Connection Server instance performs certificate revocation checking on its own certificate and on those of the security servers paired to it. By default, the VMware Horizon View Connection Server service is started with the `LocalSystem` account. When it runs under `LocalSystem`, a View Connection Server instance cannot use the proxy settings configured in Internet Explorer to access the CRL DP URL or OCSP responder to determine the revocation status of the certificate.

You can use Microsoft `Netshell` commands to import the proxy settings to the View Connection Server instance so that the server can access the certificate revocation checking sites on the Internet.

### Solution

- 1 On the View Connection Server computer, open a command-line window with the **Run as administrator** setting.  
For example, click **Start**, type `cmd`, right-click the `cmd.exe` icon, and select **Run as administrator**.
- 2 Type `netsh` and press Enter.
- 3 Type `winhttp` and press Enter.
- 4 Type `show proxy` and press Enter.

`Netshell` shows that the proxy was set to `DIRECT` connection. With this setting, the View Connection Server computer cannot connect to the Internet if a proxy is in use in your organization.

- 5 Configure the proxy settings.  
For example, at the netsh winhttp> prompt, type **import proxy source=ie**.  
The proxy settings are imported to the View Connection Server computer.
- 6 Verify the proxy settings by typing **show proxy**.
- 7 Restart the VMware Horizon View Connection Server service.
- 8 On the View Administrator dashboard, verify that the security server or View Connection Server icon is green.

## Troubleshooting Smart Card Certificate Revocation Checking

The View Connection Server instance or security server that has the smart card connected cannot perform certificate revocation checking on the server's SSL certificate unless you have configured smart card certificate revocation checking.

### Problem

Certificate revocation checking might fail if your organization uses a proxy server for Internet access, or if a View Connection Server instance or security server cannot reach the servers that provide revocation checking because of firewalls or other controls.

---

**IMPORTANT** Make sure the CRL file is up to date.

---

### Cause

View supports certificate revocation checking with certificate revocation lists (CRLs) and with the Online Certificate Status Protocol (OCSP). A CRL is a list of revoked certificates published by the CA (Certificate Authority) that issued the certificates. OCSP is a certificate validation protocol that is used to get the revocation status of an X.509 certificate. The CA must be accessible from the View Connection Server or security server host. This issue can only occur if you configured revocation checking of smart card certificates. See [“Using Smart Card Certificate Revocation Checking,”](#) on page 53.

### Solution

- 1 Create your own (manual) procedure for downloading an up-to-date CRL from the CA website you use to a path on your View server.
- 2 Create or edit the `locked.properties` file in the SSL gateway configuration folder on the View Connection Server or security server host.  
  
For example: `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`
- 3 Add the `enableRevocationChecking` and `crlLocation` properties in the `locked.properties` file to the local path to where the CRL is stored.
- 4 Restart the View Connection Server service or security server service to make your changes take effect.

## Further Troubleshooting Information

You can find further troubleshooting information in VMware Knowledge Base articles.

The VMware Knowledge Base (KB) is continually updated with new troubleshooting information for VMware products.

For more information about troubleshooting View, see the KB articles that are available on the VMware KB Web site:

<http://kb.vmware.com/selfservice/microsites/microsite.do>



## Using the vdmadmin Command

---

You can use the `vdmadmin` command line interface to perform a variety of administration tasks on a View Connection Server instance.

You can use `vdmadmin` to perform administration tasks that are not possible from within the View Administrator user interface or to perform administration tasks that need to run automatically from scripts.

For a comparison of the operations that are possible in View Administrator, View cmdlets, and `vdmadmin`, see the *View Integration* document.

- [vdmadmin Command Usage](#) on page 251  
The syntax of the `vdmadmin` command controls its operation.
- [Configuring Logging in Horizon Agent Using the -A Option](#) on page 253  
You can use the `vdmadmin` command with the `-A` option to configure logging by Horizon Agent.
- [Overriding IP Addresses Using the -A Option](#) on page 254  
You can use the `vdmadmin` command with the `-A` option to override the IP address reported by Horizon Agent.
- [Setting the Name of a View Connection Server Group Using the -C Option](#) on page 255  
You can use the `vdmadmin` command with the `-C` option to set the name of a View Connection Server group. The Microsoft System Center Operations Manager (SCOM) console displays this name to help you identify the group within SCOM.
- [Updating Foreign Security Principals Using the -F Option](#) on page 256  
You can use the `vdmadmin` command with the `-F` option to update the foreign security principals (FSPs) of Windows users in Active Directory who are authorized to use a desktop.
- [Listing and Displaying Health Monitors Using the -H Option](#) on page 257  
You can use the `vdmadmin` command `-H` to list the existing health monitors, to monitor instances for View components, and to display the details of a specific health monitor or monitor instance.
- [Listing and Displaying Reports of View Operation Using the -I Option](#) on page 258  
You can use the `vdmadmin` command with the `-I` option to list the available reports of View operation and to display the results of running one of these reports.
- [Generating View Event Log Messages in Syslog Format Using the -I Option](#) on page 259  
You can use the `vdmadmin` command with the `-I` option to record View event messages in Syslog format in event log files. Many third-party analytics products require flat-file Syslog data as input for their analytics operations.

- [Assigning Dedicated Machines Using the -L Option](#) on page 260  
You can use the `vdadmin` command with the `-L` option to assign machines from a dedicated pool to users.
- [Displaying Information About Machines Using the -M Option](#) on page 261  
You can use the `vdadmin` command with the `-M` option to display information about the configuration of virtual machines or physical computers.
- [Reclaiming Disk Space on Virtual Machines Using the -M Option](#) on page 262  
You can use the `vdadmin` command with the `-M` option to mark a linked-clone virtual machine for disk space reclamation. Horizon 7 directs the ESXi host to reclaim disk space on the linked-clone OS disk without waiting for the unused space on the OS disk to reach the minimum threshold that is specified in Horizon Administrator.
- [Configuring Domain Filters Using the -N Option](#) on page 263  
You can use the `vdadmin` command with the `-N` option to control the domains that View makes available to end users.
- [Configuring Domain Filters](#) on page 265  
You can configure domain filters to limit the domains that a View Connection Server instance or security server makes available to end users.
- [Displaying the Machines and Policies of Unentitled Users Using the -O and -P Options](#) on page 269  
You can use the `vdadmin` command with the `-O` and `-P` options to display the virtual machines and policies that are assigned to users who are no longer entitled to use the system.
- [Configuring Clients in Kiosk Mode Using the -Q Option](#) on page 270  
You can use the `vdadmin` command with the `-Q` option to set defaults and create accounts for clients in kiosk mode, to enable authentication for these clients, and to display information about their configuration.
- [Displaying the First User of a Machine Using the -R Option](#) on page 274  
You can use the `vdadmin` command with the `-R` option to find out the initial assignment of a managed virtual machine. For example, in the event of the loss of LDAP data, you might need this information so that you can reassign virtual machines to users.
- [Removing the Entry for a View Connection Server Instance or Security Server Using the -S Option](#) on page 274  
You can use the `vdadmin` command with the `-S` option to remove the entry for a View Connection Server instance or security server from the View configuration.
- [Providing Secondary Credentials for Administrators Using the -T Option](#) on page 275  
You can use the `vdadmin` command with the `-T` option to provide Active Directory secondary credentials to administrator users.
- [Displaying Information About Users Using the -U Option](#) on page 277  
You can use the `vdadmin` command with the `-U` option to display detailed information about users.
- [Unlocking or Locking Virtual Machines Using the -V Option](#) on page 277  
You can use the `vdadmin` command with the `-V` option to unlock or lock virtual machines in the datacenter.
- [Detecting and Resolving LDAP Entry Collisions Using the -X Option](#) on page 278  
You can use the `vdadmin` command with the `-X` option to detect and resolve colliding LDAP entries on replicated View Connection Server instances in a group.

## vdmadmin Command Usage

The syntax of the vdmadmin command controls its operation.

Use the following form of the vdmadmin command from a Windows command prompt.

```
vdmadmin command_option [additional_option argument] ...
```

The additional options that you can use depend on the command option.

By default, the path to the vdmadmin command executable file is C:\Program Files\VMware\VMware View\Server\tools\bin. To avoid having to enter the path on the command line, add the path to your *PATH* environment variable.

- [vdmadmin Command Authentication](#) on page 251  
You must run the vdmadmin command as a user who is in the **Administrators** role for a specified action to succeed.
- [vdmadmin Command Output Format](#) on page 251  
Some vdmadmin command options allow you to specify the format of the output information.
- [vdmadmin Command Options](#) on page 252  
You use the command options of the vdmadmin command to specify the operation that you want it to perform.

### vdmadmin Command Authentication

You must run the vdmadmin command as a user who is in the **Administrators** role for a specified action to succeed.

You can use View Administrator to assign the **Administrators** role to a user. See [Chapter 6, “Configuring Role-Based Delegated Administration,”](#) on page 95.

If you are logged in as a user with insufficient privileges, you can use the **-b** option to run the command as a user who has been assigned the **Administrators** role, if you know that user's password. You can specify the **-b** option to run the vdmadmin command as the specified user in the specified domain. The following usage forms of the **-b** option are equivalent.

```
-b username domain [password | *]
```

```
-b username@domain [password | *]
```

```
-b domain\username [password | *]
```

If you specify an asterisk (\*) instead a password, you are prompted to enter the password, and the vdmadmin command does not leave sensitive passwords in the command history on the command line.

You can use the **-b** option with all command options except the **-R** and **-T** options.

### vdmadmin Command Output Format

Some vdmadmin command options allow you to specify the format of the output information.

[Table 15-1](#) shows the options that some vdmadmin command options provide for formatting output text.

**Table 15-1.** Options for Selecting Output Format

Option	Description
-csv	Formats the output as comma-separated values.
-n	Display the output using ASCII (UTF-8) characters. This is the default character set for comma-separated values and plain text output.
-w	Display the output using Unicode (UTF-16) characters. This is the default character set for XML output.
-xml	Formats the output as XML.

## vdmadmin Command Options

You use the command options of the `vdmadmin` command to specify the operation that you want it to perform.

[Table 15-2](#) shows the command options that you can use with the `vdmadmin` command to control and examine the operation of View.

**Table 15-2.** Vdmadmin Command Options

Option	Description
-A	Administers the information that Horizon Agent records in its log files. See <a href="#">“Configuring Logging in Horizon Agent Using the -A Option,”</a> on page 253. Overrides the IP address reported by Horizon Agent. See <a href="#">“Overriding IP Addresses Using the -A Option,”</a> on page 254
-C	Sets the name for a View Connection Server group. See <a href="#">“Setting the Name of a View Connection Server Group Using the -C Option,”</a> on page 255.
-F	Updates the Foreign Security Principals (FSPs) in Active Directory for all users or for specified users. See <a href="#">“Updating Foreign Security Principals Using the -F Option,”</a> on page 256.
-H	Displays health information about View services. See <a href="#">“Listing and Displaying Health Monitors Using the -H Option,”</a> on page 257.
-I	Generates reports about View operation. See <a href="#">“Listing and Displaying Reports of View Operation Using the -I Option,”</a> on page 258.
-L	Assigns a dedicated desktop to a user or removes an assignment. See <a href="#">“Assigning Dedicated Machines Using the -L Option,”</a> on page 260.
-M	Displays information about a virtual machine or physical computer. See <a href="#">“Displaying Information About Machines Using the -M Option,”</a> on page 261.
-N	Configures the domains that a View Connection Server instance or group makes available to Horizon Client. See <a href="#">“Configuring Domain Filters Using the -N Option,”</a> on page 263.
-O	Displays the remote desktops that are assigned to users who are no longer entitled to those desktops. See <a href="#">“Displaying the Machines and Policies of Unentitled Users Using the -O and -P Options,”</a> on page 269.
-P	Displays the user policies that are associated with the remote desktops of unentitled users. See <a href="#">“Displaying the Machines and Policies of Unentitled Users Using the -O and -P Options,”</a> on page 269.
-Q	Configures the account in Active Directory account and View configuration of a client device in kiosk mode. See <a href="#">“Configuring Clients in Kiosk Mode Using the -Q Option,”</a> on page 270.
-R	Reports the first user who accessed a remote desktop. See <a href="#">“Displaying the First User of a Machine Using the -R Option,”</a> on page 274.
-S	Removes a configuration entry for a View Connection Server instance from the configuration of View. See <a href="#">“Removing the Entry for a View Connection Server Instance or Security Server Using the -S Option,”</a> on page 274.
-T	Provides Active Directory secondary credentials to administrator users. See <a href="#">“Providing Secondary Credentials for Administrators Using the -T Option,”</a> on page 275.

**Table 15-2.** Vdmadmin Command Options (Continued)

Option	Description
-U	Displays information about a user including their remote desktop entitlements and ThinApp assignments, and Administrator roles. See <a href="#">“Displaying Information About Users Using the -U Option,”</a> on page 277.
-V	Unlocks or locks virtual machines. See <a href="#">“Unlocking or Locking Virtual Machines Using the -V Option,”</a> on page 277.
-X	Detects and resolves duplicated LDAP entries on replicated View Connection Server instances. See <a href="#">“Detecting and Resolving LDAP Entry Collisions Using the -X Option,”</a> on page 278.

## Configuring Logging in Horizon Agent Using the -A Option

You can use the vdmadmin command with the -A option to configure logging by Horizon Agent.

### Syntax

```
vdmadmin -A [-b authentication_arguments] -getDCT-outfile local_file -d desktop -m machine
```

```
vdmadmin -A [-b authentication_arguments] -getlogfile logfile -outfile local_file -d desktop -m machine
```

```
vdmadmin -A [-b authentication_arguments] -getloglevel [-xml] -d desktop [-m machine]
```

```
vdmadmin -A [-b authentication_arguments] -getstatus [-xml] -d desktop [-m machine]
```

```
vdmadmin -A [-b authentication_arguments] -getversion [-xml] -d desktop [-m machine]
```

```
vdmadmin -A [-b authentication_arguments] -list [-xml] [-w | -n] -d desktop -m machine
```

```
vdmadmin -A [-b authentication_arguments] -setloglevel level -d desktop [-m machine]
```

### Usage Notes

To assist VMware Technical Support in troubleshooting Horizon Agent, you can create a Data Collection Tool (DCT) bundle. You can also change the logging level, display the version and status of Horizon Agent, and save individual log files to your local disk.

### Options

[Table 15-3](#) shows the options that you can specify to configure logging in Horizon Agent.

**Table 15-3.** Options for Configuring Logging in Horizon Agent

Option	Description
-d desktop	Specifies the desktop pool.
-getDCT	Creates a Data Collection Tool (DCT) bundle and saves it to a local file.
-getlogfile logfile	Specifies the name of the log file to save a copy of.
-getloglevel	Displays the current logging level of Horizon Agent.
-getstatus	Displays the status of Horizon Agent.
-getversion	Displays the version of Horizon Agent.
-list	List the log files for Horizon Agent.
-m machine	Specifies the machine within a desktop pool.

**Table 15-3.** Options for Configuring Logging in Horizon Agent (Continued)

Option	Description
<code>-outfile <i>local_file</i></code>	Specifies the name of the local file in which to save a DCT bundle or a copy of a log file.
<code>-setloglevel <i>level</i></code>	Sets the logging level of Horizon Agent.
	<b>debug</b> Logs error, warning, and debugging events.
	<b>normal</b> Logs error and warning events.
	<b>trace</b> Logs error, warning, informational, and debugging events.

## Examples

Display the logging level of Horizon Agent for the machine `machine1` in the desktop pool `dtpool2`.

```
vdadmin -A -d dtpool2 -m machine1 -getloglevel
```

Set the logging level of Horizon Agent for the machine `machine1` in the desktop pool `dtpool2` to `debug`.

```
vdadmin -A -d dtpool2 -m machine1 -setloglevel debug
```

Display the list of the Horizon Agent log files for the machine `machine1` in the desktop pool `dtpool2`.

```
vdadmin -A -d dtpool2 -m machine1 -list
```

Save a copy of the Horizon Agent log file `log-2009-01-02.txt` for the machine `machine1` in the desktop pool `dtpool2` as `C:\mycopiedlog.txt`.

```
vdadmin -A -d dtpool2 -m machine1 -getlogfile log-2009-01-02.txt -outfile C:\mycopiedlog.txt
```

Display the version of Horizon Agent for the machine `machine1` in the desktop pool `dtpool2`.

```
vdadmin -A -d dtpool2 -m machine1 -getversion
```

Display the status of Horizon Agent for the machine `machine1` in the desktop pool `dtpool2`.

```
vdadmin -A -d dtpool2 -m machine1 -getstatus
```

Create the DCT bundle for the machine `machine1` in the desktop pool `dtpool2` and write it to the zip file `C:\myfile.zip`.

```
vdadmin -A -d dtpool2 -m machine1 -getDCT -outfile C:\myfile.zip
```

## Overriding IP Addresses Using the -A Option

You can use the `vdadmin` command with the `-A` option to override the IP address reported by Horizon Agent.

### Syntax

```
vdadmin -A [-b authentication_arguments] -override -i ip_or_dns -d desktop -m machine
```

```
vdadmin -A [-b authentication_arguments] -override -list -d desktop -m machine
```

```
vdadmin -A [-b authentication_arguments] -override -r -d desktop [-m machine]
```

## Usage Notes

Horizon Agent reports the discovered IP address of the machine on which it is running to the View Connection Server instance. In secure configurations where the View Connection Server instance cannot trust the value that Horizon Agent reports, you can override the value provided by Horizon Agent and specify the IP address that the managed machine should be using. If the address of a machine that Horizon Agent reports does not match the defined address, you cannot use Horizon Client to access the machine.

## Options

[Table 15-4](#) shows the options that you can specify to override IP addresses.

**Table 15-4.** Options for Overriding IP Addresses

Option	Description
<code>-d desktop</code>	Specifies the desktop pool.
<code>-i ip_or_dns</code>	Specifies the IP address or resolvable domain name in DNS.
<code>-m machine</code>	Specifies the name of the machine in a desktop pool.
<code>-override</code>	Specifies an operation for overriding IP addresses.
<code>-r</code>	Removes an overridden IP address.

## Examples

Override the IP address for the machine machine2 in the desktop pool dtpool2.

```
vdmadmin -A -override -i 10.20.54.165 -d dtpool2 -m machine2
```

Display the IP addresses that are defined for the machine machine2 in the desktop pool dtpool2.

```
vdmadmin -A -override -list -d dtpool2 -m machine2
```

Remove the IP addresses that is defined for the machine machine2 in the desktop pool dtpool2.

```
vdmadmin -A -override -r -d dtpool2 -m machine2
```

Remove the IP addresses that are defined for the desktops in the desktop pool dtpool3.

```
vdmadmin -A -override -r -d dtpool3
```

## Setting the Name of a View Connection Server Group Using the -C Option

You can use the vdmadmin command with the `-C` option to set the name of a View Connection Server group. The Microsoft System Center Operations Manager (SCOM) console displays this name to help you identify the group within SCOM.

## Syntax

```
vdmadmin -C [-b authentication_arguments] [-c groupname]
```

## Usage Notes

You must name a View Connection Server group if you intend to use SCOM to monitor and manage the state of View components. View Administrator does not display the name of a group. Run the command on a member of the group that you want to name.

If you do not specify a name for the group, the command returns the GUID of the group to which the local View Connection Server instance belongs. You can use the GUID to verify whether a View Connection Server instance is a member of the same View Connection Server group as another View Connection Server instance.

For a description of how to use SCOM with View, see the *View Integration* document.

## Options

The `-c` option specifies the name of the View Connection Server group. If you do not specify this option, the command returns the GUID of the group.

## Examples

Set the name of a View Connection Server group to VCSG01.

```
vdadmin -C -c VCSG01
```

Return the GUID of the group.

```
vdadmin -C
```

## Updating Foreign Security Principals Using the -F Option

You can use the `vdadmin` command with the `-F` option to update the foreign security principals (FSPs) of Windows users in Active Directory who are authorized to use a desktop.

## Syntax

```
vdadmin -F [-b authentication_arguments] [-u domain\user]
```

## Usage Notes

If you trust domains outside of your local domains, you allow access by security principals in the external domains to the local domains' resources. Active Directory uses FSPs to represent security principals in trusted external domains. You might want to update the FSPs of users if you modify the list of trusted external domains.

## Options

The `-u` option specifies the name and domain of the user whose FSP you want to update. If you do not specify this option, the command updates the FSPs of all users in Active Directory.

## Examples

Update the FSP of the user Jim in the EXTERNAL domain.

```
vdadmin -F -u EXTERNAL\Jim
```

Update the FSPs of all users in Active Directory.

```
vdadmin -F
```

## Listing and Displaying Health Monitors Using the -H Option

You can use the `vdmadmin` command `-H` to list the existing health monitors, to monitor instances for View components, and to display the details of a specific health monitor or monitor instance.

### Syntax

```
vdmadmin -H [-b authentication_arguments] -list -xml [-w | -n]

vdmadmin -H [-b authentication_arguments] -list -monitorid monitor_id -xml [-w | -n]

vdmadmin -H [-b authentication_arguments] -monitorid monitor_id -instanceid instance_id -xml [-w | -n]
```

### Usage Notes

[Table 15-5](#) shows the health monitors that View uses to monitor the health of its components.

**Table 15-5.** Health Monitors

Monitor	Description
CBMonitor	Monitors the health of View Connection Server instances.
DBMonitor	Monitors the health of the events database.
DomainMonitor	Monitors the health of the View Connection Server host's local domain and all trusted domains.
SGMonitor	Monitors the health of security gateway services and security servers.
VCMonitor	Monitors the health of vCenter servers.

If a component has several instances, View creates a separate monitor instance to monitor each instance of the component.

The command outputs all information about health monitors and monitor instances in XML format.

### Options

[Table 15-6](#) shows the options that you can specify to list and display health monitors.

**Table 15-6.** Options for Listing and Displaying Health Monitors

Option	Description
<code>-instanceid instance_id</code>	Specifies a health monitor instance
<code>-list</code>	Displays the existing health monitors if a health monitor ID is not specified.
<code>-list -monitorid monitor_id</code>	Displays the monitor instances for the specified health monitor ID.
<code>-monitorid monitor_id</code>	Specifies a health monitor ID.

### Examples

List all existing health monitors in XML using Unicode characters.

```
vdmadmin -H -list -xml
```

List all instances of the vCenter monitor (VCMonitor) in XML using ASCII characters.

```
vdmadmin -H -list -monitorid VCMonitor -xml -n
```

Display the health of a specified vCenter monitor instance.

```
vdmdadmin -H -monitorid VCMonitor -instanceid 4aec2c99-4879-96b2-de408064d035 -xml
```

## Listing and Displaying Reports of View Operation Using the -I Option

You can use the `vdmdadmin` command with the `-I` option to list the available reports of View operation and to display the results of running one of these reports.

### Syntax

```
vdmdadmin -I [-b authentication_arguments] -list [-xml] [-w | -n]
vdmdadmin -I [-b authentication_arguments] -report report -view view [-startdate yyyy-MM-dd-
HH:mm:ss][-enddate yyyy-MM-dd-HH:mm:ss] [-w | -n] -xml | -csv
```

### Usage Notes

You can use the command to display the available reports and views, and to display the information that View has recorded for a specified report and view.

You can also use the `vdmdadmin` command with the `-I` option to generate View log messages in syslog format. See [“Generating View Event Log Messages in Syslog Format Using the -I Option,”](#) on page 259.

### Options

[Table 15-7](#) shows the options that you can specify to list and display reports and views.

**Table 15-7.** Options for Listing and Displaying Reports and Views

Option	Description
<code>-enddate yyyy-MM-dd-HH:mm:ss</code>	Specifies a upper limit for the date of information to be displayed.
<code>-list</code>	Lists the available reports and views.
<code>-report report</code>	Specifies a report.
<code>-startdate yyyy-MM-dd-HH:mm:ss</code>	Specifies a lower limit for the date of information to be displayed.
<code>-view view</code>	Specifies a view.

### Examples

List the available reports and views in XML using Unicode characters.

```
vdmdadmin -I -list -xml -w
```

Display a list of user events that occurred since August 1, 2010 as comma-separated values using ASCII characters.

```
vdmdadmin -I -report events -view user_events -startdate 2010-08-01-00:00:00 -csv -n
```

## Generating View Event Log Messages in Syslog Format Using the -I Option

You can use the `vdmadmin` command with the `-I` option to record View event messages in Syslog format in event log files. Many third-party analytics products require flat-file Syslog data as input for their analytics operations.

### Syntax

```
vdmadmin -I -eventSyslog -disable
vdmadmin -I -eventSyslog -enable -localOnly
vdmadmin -I -eventSyslog -enable -path path
vdmadmin -I -eventSyslog -enable -path path
            -user DomainName\username -password password
```

### Usage Notes

You can use the command to generate View event log messages in Syslog format. In a Syslog file, View event log messages are formatted in key-value pairs, which makes the logging data accessible to analytics software.

You can also use the `vdmadmin` command with the `-I` option to list the available reports and views and to display the contents of a specified report. See [“Listing and Displaying Reports of View Operation Using the -I Option,”](#) on page 258.

### Options

You can disable or enable the `eventSyslog` option. You can direct the Syslog output to the local system only or to another location. Direct UDP connection to a Syslog server is supported with View 5.2 or later. See “Configure Event Logging for Syslog Servers” in the *View Installation* document.

**Table 15-8.** Options for Generating View Event Log Messages in Syslog Format

Option	Description
<code>-disable</code>	Disables Syslog logging.
<code>-e -enable</code>	Enables Syslog logging.
<code>-eventSyslog</code>	Specifies that View events are generated in Syslog format.
<code>-localOnly</code>	Stores the Syslog output on the local system only. When you use the <code>-localOnly</code> option, the default destination of the Syslog output is <code>%PROGRAMDATA%\VMware\VDM\events\</code> .
<code>-password password</code>	Specifies the password for the user that authorizes access to the specified destination path for the Syslog output.
<code>-path</code>	Determines the destination UNC path for the Syslog output.
<code>-u -user DomainName\username</code>	Specifies the domain and username that can access the destination path for the Syslog output.

## Examples

Disable generating View events in Syslog format.

```
vdadmin -I -eventSyslog -disable
```

Direct Syslog output of View events to the local system only.

```
vdadmin -I -eventSyslog -enable -localOnly
```

Direct Syslog output of View events to a specified path.

```
vdadmin -I -eventSyslog -enable -path path
```

Direct Syslog output of View events to a specified path that requires access by an authorized domain user.

```
vdadmin -I -eventSyslog -enable -path \\logserver\share\ViewEvents -user mydomain\myuser
      -password mypassword
```

## Assigning Dedicated Machines Using the -L Option

You can use the `vdadmin` command with the `-L` option to assign machines from a dedicated pool to users.

### Syntax

```
vdadmin -L [-b authentication_arguments] -d desktop -m machine -u domain\user
```

```
vdadmin -L [-b authentication_arguments] -d desktop [-m machine | -u domain\user] -r
```

### Usage Notes

View assigns machines to users when they first connect to a dedicated desktop pool. Under some circumstances, you might want to preassign machines to users. For example, you might want to prepare their system environments in advance of their initial connection. After a user connects to a remote desktop that View assigns from a dedicated pool, the virtual machine that hosts the desktop remains assigned to the user for the life span of the virtual machine. You can assign a user to a single machine in a dedicated pool.

You can assign a machine to any entitled user. You might want to do this when recovering from the loss of View LDAP data on a View Connection Server instance, or when you want to change ownership of a particular machine.

After a user connects to a remote desktop that View assigns from a dedicated pool, that remote desktop remains assigned to the user for the life span of the virtual machine that hosts the desktop. You might want to remove the assignment of a machine to a user who has left the organization, who no longer requires access to the desktop, or who will use a desktop in a different desktop pool. You can also remove assignments for all users who access a desktop pool.

---

**NOTE** The `vdadmin -L` command does not assign ownership to View Composer persistent disks. To assign linked-clone desktops with persistent disks to users, use the **Assign User** menu option in View Administrator or the `View PowerCLI Update-UserOwnership` cmdlet.

If you do use `vdadmin -L` to assign a linked-clone desktop with a persistent disk to a user, unexpected results can occur in certain situations. For example, if you detach a persistent disk and use it to recreate a desktop, the recreated desktop is not assigned to the owner of the original desktop.

---

### Options

[Table 15-9](#) shows the options that you can specify to assign a desktop to a user or to remove an assignment.

**Table 15-9.** Options for Assigning Dedicated Desktops

Option	Description
<code>-d desktop</code>	Specifies the name of the desktop pool.
<code>-m machine</code>	Specifies the name of the virtual machine that hosts the remote desktop.
<code>-r</code>	Removes an assignment to a specified user, or all assignments to a specified machine.
<code>-u domain\user</code>	Specifies the login name and domain of the user.

## Examples

Assign the machine `machine2` in the desktop pool `dtpool1` to the user `Jo` in the `CORP` domain.

```
vdmadmin -L -d dtpool1 -m machine2 -u CORP\Jo
```

Remove the assignments for the user `Jo` in the `CORP` domain to desktops in the pool `dtpool1`.

```
vdmadmin -L -d dtpool1 -u Corp\Jo -r
```

Remove all user assignments to the machine `machine1` in the desktop pool `dtpool3`.

```
vdmadmin -L -d dtpool3 -m machine1 -r
```

## Displaying Information About Machines Using the -M Option

You can use the `vdmadmin` command with the `-M` option to display information about the configuration of virtual machines or physical computers.

### Syntax

```
vdmadmin -M [-b authentication_arguments] [-m machine | [-u domain\user][-d desktop]] [-xml | -csv] [-w | -n]
```

### Usage Notes

The command displays information about a remote desktop's underlying virtual machine or physical computer.

- Display name of the machine.
- Name of the desktop pool.
- State of the machine.

The machine state can be one of the following values: `UNDEFINED`, `PRE_PROVISIONED`, `CLONING`, `CLONINGERROR`, `CUSTOMIZING`, `READY`, `DELETING`, `MAINTENANCE`, `ERROR`, `LOGOUT`.

The command does not display all dynamic machine states, such as `Connected` or `Disconnected`, that are displayed in View Administrator.

- SID of the assigned user.
- Account name of the assigned user.
- Domain name of the assigned user.
- Inventory path of the virtual machine (if applicable).
- Date on which the machine was created.
- Template path of the machine (if applicable).

- URL of the vCenter Server (if applicable).

## Options

Table 15-10 shows the options that you can use to specify the machine whose details you want to display.

**Table 15-10.** Options for Displaying Information About Machines

Option	Description
<code>-d desktop</code>	Specifies the name of the desktop pool.
<code>-m machine</code>	Specifies the name of the virtual machine.
<code>-u domain\user</code>	Specifies the login name and domain of the user.

## Examples

Display information about the underlying machine for the remote desktop in the pool `dtpool2` that is assigned to the user `Jo` in the `CORP` domain and format the output as XML using ASCII characters.

```
vdmadmin -M -u CORP\Jo -d dtpool2 -xml -n
```

Display information about the machine `machine3` and format the output as comma-separated values.

```
vdmadmin -M -m machine3 -csv
```

## Reclaiming Disk Space on Virtual Machines Using the -M Option

You can use the `vdmadmin` command with the `-M` option to mark a linked-clone virtual machine for disk space reclamation. Horizon 7 directs the ESXi host to reclaim disk space on the linked-clone OS disk without waiting for the unused space on the OS disk to reach the minimum threshold that is specified in Horizon Administrator.

## Syntax

```
vdmadmin -M [-b authentication_arguments] -d desktop -m machine -markForSpaceReclamation
```

## Usage Notes

With this option, you can initiate disk space reclamation on a particular virtual machine for demonstration or troubleshooting purposes.

Space reclamation does not take place if you run this command when a blackout period is in effect.

The following prerequisites must be met before you can reclaim disk space by using the `vdmadmin` command with the `-M` option:

- Verify that Horizon 7 is using vCenter Server and ESXi version 5.1 or later.
- Verify that VMware Tools that are provided with vSphere version 5.1 or later are installed on the virtual machine.
- Verify that the virtual machine is virtual hardware version 9 or later.
- In Horizon Administrator, verify that the **Enable space reclamation** option is selected for vCenter Server. See [“Allow vSphere to Reclaim Disk Space in Linked-Clone Virtual Machines,”](#) on page 18.
- In Horizon Administrator, verify that the **Reclaim VM disk space** option was selected for the desktop pool. See “Reclaim Disk Space on View Composer Linked Clones” in the *Setting Up Virtual Desktops in Horizon 7* document.
- Verify that the virtual machine is powered on before you initiate the space reclamation operation.

- Verify that a blackout period is not in effect. See "Set Storage Accelerator and Space Reclamation Blackout Times for View Composer Linked Clones" in the *Setting Up Virtual Desktops in Horizon 7* document.

## Options

**Table 15-11.** Options for Reclaiming Disk Space on Virtual Machines

Option	Description
<code>-d desktop</code>	Specifies the name of the desktop pool.
<code>-m machine</code>	Specifies the name of the virtual machine.
<code>-MarkForSpaceReclamation</code>	Marks the virtual machine for disk space reclamation.

## Example

Marks the virtual machine `machine3` in the desktop pool `pool1` for disk space reclamation.

```
vdmadmin -M -d pool1 -m machine3 -markForSpaceReclamation
```

## Configuring Domain Filters Using the -N Option

You can use the `vdmadmin` command with the `-N` option to control the domains that View makes available to end users.

## Syntax

```
vdmadmin -N [-b authentication_arguments] -domains {-exclude | -include | -search} -domain domain -add [-s connsvr]
```

```
vdmadmin -N [-b authentication_arguments] -domains -list [-w | -n] [-xml]
```

```
vdmadmin -N [-b authentication_arguments] -domains -list -active [-w | -n] [-xml]
```

```
vdmadmin -N [-b authentication_arguments] -domains {-exclude | -include | -search} -domain domain -remove [-s connsvr]
```

```
vdmadmin -N [-b authentication_arguments] -domains {-exclude | -include | -search} -removeall [-s connsvr]
```

## Usage Notes

Specify one of the `-exclude`, `-include`, or `-search` options to apply an operation to the exclusion list, inclusion list, or search exclusion list respectively.

If you add a domain to a search exclusion list, the domain is excluded from an automated domain search.

If you add a domain to an inclusion list, the domain is included in the results of the search.

If you add a domain to an exclusion list, the domain is excluded from the results of the search.

## Options

[Table 15-12](#) shows the options that you can specify to configure domain filters.

**Table 15-12.** Options for Configuring Domain Filters

Option	Description
<code>-add</code>	Adds a domain to a list.
<code>-domain <i>domain</i></code>	Specifies the domain to be filtered. You must specify domains by their NetBIOS names and not by their DNS names.
<code>-domains</code>	Specifies a domain filter operation.
<code>-exclude</code>	Specifies an operation on a exclusion list.
<code>-include</code>	Specifies an operation on an inclusion list.
<code>-list</code>	Displays the domains that are configured in the search exclusion list, exclusion list, and inclusion list on each View Connection Server instance and for the View Connection Server group.
<code>-list -active</code>	Displays the available domains for the View Connection Server instance on which you run the command.
<code>-remove</code>	Removes a domain from a list.
<code>-removeall</code>	Removes all domains from a list.
<code>-s <i>connsvr</i></code>	Specifies that the operation applies to the domain filters on a View Connection Server instance. You can specify the View Connection Server instance by its name or IP address. If you do not specify this option, any change that you make to the search configuration applies to all View Connection Server instances in the group.
<code>-search</code>	Specifies an operation on a search exclusion list.

## Examples

Add the domain FARDOM to the search exclusion list for the View Connection Server instance csvr1.

```
vdadmin -N -domains -search -domain FARDOM -add -s csvr1
```

Add the domain NEARDOM to the exclusion list for a View Connection Server group.

```
vdadmin -N -domains -exclude -domain NEARDOM -add
```

Display the domain search configuration on both View Connection Server instances in the group, and for the group.

```
C:\> vdadmin -N -domains -list
```

```
Domain Configuration
```

```
=====
```

```
Cluster Settings
```

```
Include:
```

```
Exclude:
```

```
Search :
```

```
FARDOM
```

```
DEPTX
```

```
Broker Settings: CONSVR-1
```

```
Include:
```

```
(*)Exclude:
```

```
YOURDOM
```

```
Search :
```

Broker Settings: CONSVR-2

Include:

Exclude:

Search :

View limits the domain search on each View Connection Server host in the group to exclude the domains FARDOM and DEPTX. The characters (\*) next to the exclusion list for CONSVR-1 indicates that View excludes the YOURDOM domain from the results of the domain search on CONSVR-1.

Display the domain filters in XML using ASCII characters.

```
vdmadmin -N -domains -list -xml -n
```

Display the domains that are available to View on the local View Connection Server instance.

```
C:\ vdmadmin -N -domains -list -active
```

Domain Information (CONSVR)

=====

Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com

Domain: YOURDOM DNS:yourdom.mycorp.com

Domain: FARDOM DNS:fardom.mycorp.com

Domain: DEPTX DNS:deptx.mycorp.com

Domain: DEPTY DNS:depty.mycorp.com

Domain: DEPTZ DNS:deptz.mycorp.com

Display the available domains in XML using ASCII characters.

```
vdmadmin -N -domains -list -active -xml -n
```

Remove the domain NEARDOM from the exclusion list for a View Connection Server group.

```
vdmadmin -N -domains -exclude -domain NEARDOM -remove
```

Remove all domains from the inclusion list for the View Connection Server instance csvr1.

```
vdmadmin -N -domains -include -removeall -s csvr1
```

## Configuring Domain Filters

You can configure domain filters to limit the domains that a View Connection Server instance or security server makes available to end users.

View determines which domains are accessible by traversing trust relationships, starting with the domain in which a View Connection Server instance or security server resides. For a small, well-connected set of domains, View can quickly determine a full list of domains, but the time that this operation takes increases as the number of domains increases or as the connectivity between the domains decreases. View might also include domains in the search results that you would prefer not to offer to users when they log in to their remote desktops.

If you have previously set the value of the Windows registry key that controls recursive domain enumeration (HKEY\_LOCAL\_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\RecursiveDomainEnum) to false, recursive domain searching is disabled, and the View Connection Server instance uses only the primary domain. To use the domain filtering feature, delete the registry key or set its value to true, and restart the system. You must do this for every View Connection Server instance on which you have set this key.

[Table 15-13](#) shows the types of domain lists that you can specify to configure domain filtering.

**Table 15-13.** Types of Domain List

Domain List Type	Description
Search exclusion list	Specifies the domains that View can traverse during an automated search. The search ignores domains that are included in the search exclusion list, and does not attempt to locate domains that the excluded domain trusts. You cannot exclude the primary domain from the search.
Exclusion list	Specifies the domains that View excludes from the results of a domain search. You cannot exclude the primary domain.
Inclusion list	Specifies the domains that View does not exclude from the results of a domain search. All other domains are removed apart from the primary domain.

The automated domain search retrieves a list of domains, excluding those domains that you specify in the search exclusion list and domains that are trusted by those excluded domains. View selects the first non-empty exclusion or inclusion list in this order.

- 1 Exclusion list configured for the View Connection Server instance.
- 2 Exclusion list configured for the View Connection Server group.
- 3 Inclusion list configured for the View Connection Server instance.
- 4 Inclusion list configured for the View Connection Server group

View applies only the first list that it selects to the search results.

If you specify a domain for inclusion, and its domain controller is not currently accessible, View does not include that domain in the list of active domains.

You cannot exclude the primary domain to which a View Connection Server instance or security server belongs.

## Example of Filtering to Include Domains

You can use an inclusion list to specify the domains that View does not exclude from the results of a domain search. All other domains, apart from the primary domain, are removed.

A View Connection Server instance is joined to the primary MYDOM domain and has a trusted relationship with the YOURDOM domain. The YOURDOM domain has a trusted relationship with the DEPTX domain.

Display the currently active domains for the View Connection Server instance.

```
C:\> vdmadmin -N -domains -list -active
```

```
Domain Information (CONSVR)
```

```
=====
```

```
Primary Domain: MYDOM
```

```
Domain: MYDOM DNS:mydom.mycorp.com
```

```
Domain: YOURDOM DNS:yourdom.mycorp.com
```

```
Domain: FARDOM DNS: fardom.mycorp.com
```

```
Domain: DEPTX DNS:deptx.mycorp.com
```

```
Domain: DEPTY DNS:depty.mycorp.com
```

```
Domain: DEPTZ DNS:deptz.mycorp.com
```

The DEPTY and DEPTZ domains appear in the list because they are trusted domains of the DEPTX domain.

Specify that the View Connection Server instance should make only the YOURDOM and DEPTX domains available, in addition to the primary MYDOM domain.

```
vdmadmin -N -domains -include -domain YOURDOM -add
```

```
vdmadmin -N -domains -include -domain DEPTX -add
```

Display the currently active domains after including the YOURDOM and DEPTX domains.

```
C:\ vdmadmin -N -domains -list -active
```

```
Domain Information (CONSVR)
=====
Primary Domain: MYDOM
Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
```

View applies the include list to the results of a domain search. If the domain hierarchy is very complex or network connectivity to some domains is poor, the domain search can be slow. In such cases, use search exclusion instead.

## Example of Filtering to Exclude Domains

You can use an inclusion list to specify the domains that View excludes from the results of a domain search.

A group of two View Connection Server instances, CONSVR-1 and CONSVR-2, is joined to the primary MYDOM domain and has a trusted relationship with the YOURDOM domain. The YOURDOM domain has a trusted relationship with the DEPTX and FARDOM domains.

The FARDOM domain is in a remote geographical location, and network connectivity to that domain is over a slow, high-latency link. There is no requirement for users in the FARDOM domain to be able to access the View Connection Server group in the MYDOM domain.

Display the currently active domains for a member of the View Connection Server group.

```
C:\ vdmadmin -N -domains -list -active
```

```
Domain Information (CONSVR-1)
=====
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: FARDOM DNS: fardom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

The DEPTY and DEPTZ domains are trusted domains of the DEPTX domain.

To improve connection performance for Horizon Client, exclude the FARDOM domain from being searched by the View Connection Server group.

```
vdmadmin -N -domains -search -domain FARDOM -add
```

The command displays the currently active domains after excluding the FARDOM domain from the search.

```
C:\ vdmadmin -N -domains -list -active
```

```
Domain Information (CONSVR-1)
=====
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
```

```
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

Extend the search exclusion list to exclude the DEPTX domain and all its trusted domains from the domain search for all View Connection Server instances in a group. Also, exclude the YOURDOM domain from being available on CONSVR-1.

```
vdmadmin -N -domains -search -domain DEPTX -add
vdmadmin -N -domains -exclude -domain YOURDOM -add -s CONSVR-1
```

Display the new domain search configuration.

```
C:\ vdmadmin -N -domains -list
```

```
Domain Configuration
```

```
=====
```

```
Cluster Settings
```

```
Include:
```

```
Exclude:
```

```
Search :
```

```
FARDOM
```

```
DEPTX
```

```
Broker Settings: CONSVR-1
```

```
Include:
```

```
(*)Exclude:
```

```
YOURDOM
```

```
Search :
```

```
Broker Settings: CONSVR-2
```

```
Include:
```

```
Exclude:
```

```
Search :
```

View limits the domain search on each View Connection Server host in the group to exclude the domains FARDOM and DEPTX. The characters (\*) next to the exclusion list for CONSVR-1 indicates that View excludes the YOURDOM domain from the results of the domain search on CONSVR-1.

On CONSVR-1, display the currently active domains.

```
C:\ vdmadmin -N -domains -list -active
```

```
Domain Information (CONSVR-1)
```

```
=====
```

```
Primary Domain: MYDOM
```

```
Domain: MYDOM DNS:mydom.mycorp.com
```

On CONSVR-2, display the currently active domains.

```
C:\ vdmadmin -N -domains -list -active
```

```
Domain Information (CONSVR-2)
```

```
=====
```

```
Primary Domain: MYDOM
```

```
Domain: MYDOM DNS:mydom.mycorp.com
```

```
Domain: YOURDOM DNS:yourdom.mycorp.com
```

## Displaying the Machines and Policies of Unentitled Users Using the -O and -P Options

You can use the `vdmadmin` command with the `-O` and `-P` options to display the virtual machines and policies that are assigned to users who are no longer entitled to use the system.

### Syntax

```
vdmadmin -O [-b authentication_arguments] [-ld | -lu] [-w | -n] [-xml [-noxslt | -xsltpath path]]
```

```
vdmadmin -P [-b authentication_arguments] [-ld | -lu] [-w | -n] [-xml [-noxslt | -xsltpath path]]
```

### Usage Notes

If you revoke a user's entitlement to a persistent virtual machine or to a physical system, the associated remote desktop assignment is not automatically revoked. This condition might be acceptable if you have temporarily suspended a user's account or if the user is on a sabbatical. When you reenable entitlement, the user can continue using the same virtual machine as previously. If a user has left the organization, other users cannot access the virtual machine, and it is considered to be orphaned. You might also want to examine any policies that are assigned to unentitled users.

### Options

[Table 15-14](#) shows the options that you can specify to display the virtual machines and policies of unentitled users.

**Table 15-14.** Options for Displaying the Machines and Policies of Unentitled Users

Option	Description
<code>-ld</code>	Orders output entries by machine.
<code>-lu</code>	Orders output entries by user.
<code>-noxslt</code>	Specifies that the default stylesheet should not be applied to the XML output.
<code>-xsltpath path</code>	Specifies the path to the stylesheet that is used to transform XML output.

[Table 15-15](#) shows the stylesheets that you can apply to the XML output to transform it into HTML. The stylesheets are located in the directory `C:\Program Files\VMware\VMware View\server\etc`.

**Table 15-15.** XSL Stylesheets

Stylesheet File Name	Description
<code>unentitled-machines.xsl</code>	Transforms reports containing a list of unentitled virtual machines, grouped either by user or system, and which are currently assigned to a user. This is the default stylesheet.
<code>unentitled-policies.xsl</code>	Transforms reports containing a list of virtual machines with user-level policies that are applied to unentitled users.

### Examples

Display the virtual machines that are assigned to unentitled users, grouped by virtual machine in text format.

```
vdmadmin -O -ld
```

Display virtual machines that are assigned to unentitled users, grouped by user, in XML format using ASCII characters.

```
vdadmin -O -lu -xml -n
```

Apply your own stylesheet C:\tmp\unentitled-users.xml and redirect the output to the file uu-output.html.

```
vdadmin -O -lu -xml -xsltpath "C:\tmp\unentitled-users.xml" > uu-output.html
```

Display the user policies that are associated with unentitled users' virtual machines, grouped by desktop, in XML format using Unicode characters.

```
vdadmin -P -ld -xml -w
```

Apply your own stylesheet C:\tmp\unentitled-policies.xml and redirect the output to the file up-output.html.

```
vdadmin -P -ld -xml -xsltpath "C:\tmp\unentitled-policies.xml" > up-output.html
```

## Configuring Clients in Kiosk Mode Using the -Q Option

You can use the `vdadmin` command with the `-Q` option to set defaults and create accounts for clients in kiosk mode, to enable authentication for these clients, and to display information about their configuration.

### Syntax

```
vdadmin -Q -clientauth -add [-b authentication_arguments] -domain domain_name-clientid client_id [-password "password" | -genpassword] [-ou DN] [-expirepassword | -noexpirepassword] [-group group_name | -nogroup] [-description "description_text"]
```

```
vdadmin -Q -disable [-b authentication_arguments] -s connection_server
```

```
vdadmin -Q -enable [-b authentication_arguments] -s connection_server [-requirepassword]
```

```
vdadmin -Q -clientauth -getdefaults [-b authentication_arguments] [-xml]
```

```
vdadmin -Q -clientauth -list [-b authentication_arguments] [-xml]
```

```
vdadmin -Q -clientauth -remove [-b authentication_arguments] -domain domain_name-clientid client_id
```

```
vdadmin -Q -clientauth -removeall [-b authentication_arguments] [-force]
```

```
vdadmin -Q -clientauth -setdefaults [-b authentication_arguments] [-ou DN] [-expirepassword | -noexpirepassword] [-group group_name | -nogroup]
```

```
vdadmin -Q -clientauth -update [-b authentication_arguments] -domain domain_name-clientid client_id [-password "password" | -genpassword] [-description "description_text"]
```

### Usage Notes

You must run the `vdadmin` command on one of the View Connection Server instances in the group that contains the View Connection Server instance that clients use to connect to their remote desktops.

When you configure defaults for password expiry and Active Directory group membership, these settings are shared by all View Connection Server instances in a group.

When you add a client in kiosk mode, View creates a user account for the client in Active Directory. If you specify a name for a client, this name must start with the characters "custom-" or with one of the alternate strings that you can define in ADAM, and it cannot be more than 20 characters long. You should use each specified name with no more than one client device.

You can define alternate prefixes to "custom-" in the `pae-ClientAuthPrefix` multi-valued attribute under `cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int` in ADAM on a View Connection Server instance. Avoid using these prefixes with ordinary user accounts.

If you do not specify a name for a client, View generates a name from the MAC address that you specify for the client device. For example, if the MAC address is 00:10:db:ee:76:80, the corresponding account name is `cm-00_10_db_ee_76_80`. You can only use these accounts with View Connection Server instances that you enable to authenticate clients.

Some thin clients allow only account names that start with the characters "custom-" or "cm-" to be used with kiosk mode.

An automatically generated password is 16 characters long, contains at least one uppercase letter, one lowercase letter, one symbol, and one number, and can contain repeated characters. If you require a stronger password, you must use the `-password` option to specify the password.

If you use the `-group` option to specify a group or you have previously set a default group, View adds the client's account to this group. You can specify the `-nogroup` option to prevent the account being added to any group.

If you enable a View Connection Server instance to authenticate clients in kiosk mode, you can optionally specify that clients must provide a password. If you disable authentication, clients cannot connect to their remote desktops.

Although you enable or disable authentication for an individual View Connection Server instance, all View Connection Server instances in a group share all other settings for client authentication. You need only add a client once for all View Connection Server instances in a group to be capable of accepting requests from the client.

If you specify the `-requirepassword` option when enabling authentication, the View Connection Server instance cannot authenticate clients that have automatically generated passwords. If you change the configuration of a View Connection Server instance to specify this option, such clients cannot authenticate themselves, and they fail with the error message `Unknown username or bad password`.

## Options

Table 15-16 shows the options that you can specify to configure clients in kiosk mode.

**Table 15-16.** Options for Configuring Clients in Kiosk Mode

Option	Description
<code>-add</code>	Adds an account for a client in kiosk mode.
<code>-clientauth</code>	Specifies an operation that configures authentication for a client in kiosk mode.
<code>-clientid <i>client_id</i></code>	Specifies the name or the MAC address of the client.
<code>-description "<i>description_text</i>"</code>	Creates a description of the account for the client device in Active Directory.
<code>-disable</code>	Disables authentication of clients in kiosk mode on a specified View Connection Server instance.
<code>-domain <i>domain_name</i></code>	Specifies the domain for the account for the client device.
<code>-enable</code>	Enables authentication of clients in kiosk mode on a specified View Connection Server instance.
<code>-expirepassword</code>	Specifies that the expiry time for the password on client accounts is the same as for the View Connection Server group. If no expiry time is defined for the group, passwords do not expire.

**Table 15-16.** Options for Configuring Clients in Kiosk Mode (Continued)

Option	Description
<code>-force</code>	Disables the confirmation prompt when removing the account for a client in kiosk mode.
<code>-genpassword</code>	Generates a password for the client's account. This is the default behavior if you do not specify either <code>-password</code> or <code>-genpassword</code> .
<code>-getdefaults</code>	Gets the default values that are used for adding client accounts.
<code>-group group_name</code>	Specifies the name of the default group to which client accounts are added. The name of the group must be specified as the pre-Windows 2000 group name from Active Directory.
<code>-list</code>	Displays information about clients in kiosk mode and about the View Connection Server instances on which you have enabled authentication of clients in kiosk mode.
<code>-noexpirepassword</code>	Specifies that the password on an account does not expire.
<code>-nogroup</code>	When adding an account for a client, specifies that the client's account is not added to the default group. When setting the default values for clients, clears the setting for the default group.
<code>-ou DN</code>	Specifies the distinguished name of the organizational unit to which client accounts are added. For example: <code>OU=kiosk-ou,DC=myorg,DC=com</code> <b>NOTE</b> You cannot use the <code>-setdefaults</code> option to change the configuration of an organizational unit.
<code>-password "password"</code>	Specifies an explicit password for the client's account.
<code>-remove</code>	Removes the account for a client in kiosk mode.
<code>-removeall</code>	Removes the accounts of all clients in kiosk mode.
<code>-requirepassword</code>	Specifies that clients in kiosk mode must provide passwords. View will not accept generated passwords for new connections.
<code>-s connection_server</code>	Specifies the NetBIOS name of the View Connection Server instance on which to enable or disable the authentication of clients in kiosk mode.
<code>-setdefaults</code>	Sets the default values that are used for adding client accounts.
<code>-update</code>	Updates an account for a client in kiosk mode.

## Examples

Set the default values for the organizational unit, password expiry, and group membership of clients.

```
vdadmin -Q -clientauth -setdefaults -ou "OU=kiosk-ou,DC=myorg,DC=com" -noexpirepassword -group kc-grp
```

Get the current default values for clients in plain text format.

```
vdadmin -Q -clientauth -getdefaults
```

Get the current default values for clients in XML format.

```
vdadmin -Q -clientauth -getdefaults -xml
```

Add an account for a client specified by its MAC address to the MYORG domain, and use the default settings for the group kc-grp.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -group kc-grp
```

Add an account for a client specified by its MAC address to the MYORG domain, and use an automatically generated password.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -genpassword -ou "OU=kiosk-ou,DC=myorg,DC=com" -group kc-grp
```

Add an account for a named client, and specify a password to be used with the client.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid custom-Terminal21 -password "guest" -ou "OU=kiosk-ou,DC=myorg,DC=com" -description "Terminal 21"
```

Update an account for a client, specifying a new password and descriptive text.

```
vdmadmin -Q -clientauth -update -domain MYORG -clientid custom-Terminal21 -password "Secret1!" -description "Foyer Entry Workstation"
```

Remove the account for a kiosk client specified by its MAC address from the MYORG domain.

```
vdmadmin -Q -clientauth -remove -domain MYORG -clientid 00:10:db:ee:54:12
```

Remove the accounts of all clients without prompting to confirm the removal.

```
vdmadmin -Q -clientauth -removeall -force
```

Enable authentication of clients for the View Connection Server instance csvr-2. Clients with automatically generated passwords can authenticate themselves without providing a password.

```
vdmadmin -Q -enable -s csvr-2
```

Enable authentication of clients for the View Connection Server instance csvr-3, and require that the clients specify their passwords to Horizon Client. Clients with automatically generated passwords cannot authenticate themselves.

```
vdmadmin -Q -enable -s csvr-3 -requirepassword
```

Disable authentication of clients for the View Connection Server instance csvr-1.

```
vdmadmin -Q -disable -s csvr-1
```

Display information about clients in text format. Client cm-00\_0c\_29\_0d\_a3\_e6 has an automatically generated password, and does not require an end user or an application script to specify this password to Horizon Client. Client cm-00\_22\_19\_12\_6d\_cf has an explicitly specified password, and requires the end user to provide this. The View Connection Server instance CONSVR2 accepts authentication requests from clients with automatically generated passwords. CONSVR1 does not accept authentication requests from clients in kiosk mode.

```
C:\ vdmadmin -Q -clientauth -list
```

```
Client Authentication User List
```

```
=====
GUID           : 94be6344-0c9b-4a92-8d54-1brc1c2dc282
ClientID       : cm-00_0c_29_0d_a3_e6
Domain        : myorg.com
Password Generated: true
```

```
GUID           : 471d9d35-68b2-40ee-b693-56a7d92b2e25
ClientID       : cm-00_22_19_12_6d_cf
Domain        : myorg.com
Password Generated: false
```

```
Client Authentication Connection Servers
```

```
=====
Common Name           : CONSVR1
Client Authentication Enabled : false
Password Required      : false

Common Name           : CONSVR2
Client Authentication Enabled : true
Password Required      : false
```

## Displaying the First User of a Machine Using the -R Option

You can use the `vdadmin` command with the `-R` option to find out the initial assignment of a managed virtual machine. For example, in the event of the loss of LDAP data, you might need this information so that you can reassign virtual machines to users.

---

**NOTE** The `vdadmin` command with the `-R` option works only on virtual machines that are earlier than View Agent 5.1. On virtual machines that run View Agent 5.1 and later and Horizon Agent 7.0 and later versions, this option does not work. To locate the first user of a virtual machine, use the Events database to determine which users logged into the machine.

---

### Syntax

```
vdadmin -R -i network_address
```

### Usage Notes

You cannot use the `-b` option to run this command as a privileged user. You must be logged in as a user in the **Administrator** role.

### Options

The `-i` option specifies the IP address of the virtual machine.

### Examples

Display the first user who accessed the virtual machine at the IP address 10.20.34.120.

```
vdadmin -R -i 10.20.34.120
```

## Removing the Entry for a View Connection Server Instance or Security Server Using the -S Option

You can use the `vdadmin` command with the `-S` option to remove the entry for a View Connection Server instance or security server from the View configuration.

### Syntax

```
vdadmin -S [-b authentication_arguments] -r -s server
```

### Usage Notes

To ensure high availability, View allows you to configure one or more replica View Connection Server instances in a View Connection Server group. If you disable a View Connection Server instance in a group, the entry for the server persists within the View configuration.

You can also use the `vdmadmin` command with the `-S` option to remove a security server from your View environment. You do not have to use this option if you intend to upgrade or reinstall a security server without removing it permanently.

To make the removal permanent, perform these tasks:

- 1 Uninstall the View Connection Server instance or security server from the Windows Server computer by running the View Connection Server installer.
- 2 Remove the Adam Instance VMwareVDMDS program from the Windows Server computer by running the Add or Remove Programs tool.
- 3 On another View Connection Server instance, use the `vdmadmin` command to remove the entry for the uninstalled View Connection Server instance or security server from the configuration.

If you want to reinstall View on the removed systems without replicating the View configuration of the original group, restart all the View Connection Server hosts in the original group before performing the reinstallation. This prevents the reinstalled View Connection Server instances from receiving configuration updates from their original group.

## Options

The `-s` option specifies the NetBIOS name of the View Connection Server instance or security server to be removed.

## Examples

Remove the entry for the View Connection Server instance `connsvr3`.

```
vdmadmin -S -r -s connsvr3
```

## Providing Secondary Credentials for Administrators Using the -T Option

You can use the `vdmadmin` command with the `-T` option to provide Active Directory secondary credentials to administrator users.

## Syntax

```
vdmadmin -T [-b authentication_arguments] -domainauth  
{-add | -update | -remove | -removeall | -list} -owner domain\user -user domain\user [-password  
password]
```

## Usage Notes

If your users and groups are in a domain with a one-way trust relationship with the View Connection Server domain, you must provide secondary credentials for the administrator users in View Administrator. Administrators must have secondary credentials to give them access to the one-way trusted domains. A one-way trusted domain can be an external domain or a domain in a transitive forest trust.

Secondary credentials are required only for View Administrator sessions, not for end users' desktop or application sessions. Only administrator users require secondary credentials.

With the `vdmadmin` command, you configure secondary credentials on a per-user basis. You cannot configure globally specified secondary credentials.

For a forest trust, you typically configure secondary credentials only for the forest root domain. View Connection Server can then enumerate the child domains in the forest trust.

Active Directory account lock, disable, and logon hours checks can be performed only when a user in a one-way trusted domain first logs on.

PowerShell administration and smart card authentication of users is not supported in one-way trusted domains. SAML authentication of users in one-way trusted domains is not supported.

Secondary credential accounts require the following permissions. A standard user account should have these permissions by default.

- List Contents
- Read All Properties
- Read Permissions
- Read tokenGroupsGlobalAndUniversal (implied by Read All Properties)

## Options

**Table 15-17.** Options for Providing Secondary Credentials

Option	Description
<code>-add</code>	Adds a secondary credential for the owner account. A Windows logon is performed to verify that the specified credentials are valid. A foreign security principal (FSP) is created for the user in View LDAP.
<code>-update</code>	Updates a secondary credential for the owner account. A Windows logon is performed to verify that the updated credentials are valid.
<code>-list</code>	Displays the security credentials for the owner account. Passwords are not displayed.
<code>-remove</code>	Removes a security credential from the owner account.
<code>-removeall</code>	Removes all security credentials from the owner account.

## Examples

Add a secondary credential for the specified owner account. A Windows logon is performed to verify that the specified credentials are valid.

```
vdmadmin -T -domainauth -add -owner domain\user -user domain\user -password password
```

Update a secondary credential for the specified owner account. A Windows logon is performed to verify that the updated credentials are valid.

```
vdmadmin -T -domainauth -update -owner domain\user -user domain\user -password password
```

Remove a secondary credential for the specified owner account.

```
vdmadmin -T -domainauth -remove -owner domain\user -user domain\user
```

Remove all secondary credentials for the specified owner account.

```
vdmadmin -T -domainauth -removeall -owner domain\user
```

Display all secondary credentials for the specified owner account. Passwords are not displayed.

```
vdmadmin -T -domainauth -list -owner domain\user
```

## Displaying Information About Users Using the -U Option

You can use the `vdmadmin` command with the `-U` option to display detailed information about users.

### Syntax

```
vdmadmin -U [-b authentication_arguments] -u domain\user [-w | -n] [-xml]
```

### Usage Notes

The command displays information about a user obtained from Active Directory and View.

- Details from Active Directory about the user's account.
- Membership of Active Directory groups.
- Machine entitlements including the machine ID, display name, description, folder, and whether a machine has been disabled.
- ThinApp assignments.
- Administrator roles including the administrative rights of a user and the folders in which they have those rights.

### Options

The `-u` option specifies the name and domain of the user.

### Examples

Display information about the user Jo in the CORP domain in XML using ASCII characters.

```
vdmadmin -U -u CORP\Jo -n -xml
```

## Unlocking or Locking Virtual Machines Using the -V Option

You can use the `vdmadmin` command with the `-V` option to unlock or lock virtual machines in the datacenter.

### Syntax

```
vdmadmin -V [-b authentication_arguments] -e -d desktop -m machine [-m machine] ...
```

```
vdmadmin -V [-b authentication_arguments] -e -vcdn vCenter_dn -vmppath inventory_path
```

```
vdmadmin -V [-b authentication_arguments] -p -d desktop -m machine [-m machine] ...
```

```
vdmadmin -V [-b authentication_arguments] -p -vcdn vCenter_dn -vmppath inventory_path
```

### Usage Notes

You should only use the `vdmadmin` command to unlock or lock a virtual machine if you encounter a problem that has left a remote desktop in an incorrect state. Do not use the command to administer remote desktops that are operating normally.

If a remote desktop is locked and the entry for its virtual machine no longer exists in ADAM, use the `-vmppath` and `-vcdn` options to specify the inventory path of the virtual machine and the vCenter Server. You can use vCenter Client to find out the inventory path of a virtual machine for a remote desktop under `Home/Inventory/VMs` and `Templates`. You can use ADAM ADSI Edit to find out the distinguished name of the vCenter Server under the `OU=Properties` heading.

## Options

Table 15-18 shows the options that you can specify to unlock or lock virtual machines.

**Table 15-18.** Options for Unlocking or Locking Virtual Machines

Option	Description
<code>-d desktop</code>	Specifies the desktop pool.
<code>-e</code>	Unlocks a virtual machine.
<code>-m machine</code>	Specifies the name of the virtual machine.
<code>-p</code>	Locks a virtual machine.
<code>-vcdn vCenter_dn</code>	Specifies the distinguished name of the vCenter Server.
<code>-vmopath inventory_path</code>	Specifies the inventory path of the virtual machine.

## Examples

Unlock the virtual machines machine 1 and machine2 in desktop pool dtpool3.

```
vdmadmin -V -e -d dtpool3 -m machine1 -m machine2
```

Lock the virtual machine machine3 in desktop pool dtpool3.

```
vdmadmin -V -p -d dtpool3 -m machine3
```

## Detecting and Resolving LDAP Entry Collisions Using the -X Option

You can use the `vdmadmin` command with the `-X` option to detect and resolve colliding LDAP entries on replicated View Connection Server instances in a group.

## Syntax

```
vdmadmin -X [-b authentication_arguments] -collisions [-resolve]
```

## Usage Notes

If duplicate LDAP entries are created on two or more View Connection Server instances, this can cause problems with the integrity of LDAP data in View. For example, this condition can happen during an upgrade while LDAP replication is inoperative. Although View checks for this error condition at regular intervals, you can run the `vdmadmin` command on one of the View Connection Server instances in the group to detect and resolve LDAP entry collisions manually.

## Options

Table 15-19 shows the options that you can specify to detect and resolve colliding LDAP entries.

**Table 15-19.** Options for Detecting and Resolving LDAP Entry Collisions

Option	Description
<code>-collisions</code>	Specifies an operation for detecting LDAP collisions in a View Connection Server group.
<code>-resolve</code>	Resolves all detected LDAP collisions.

## Examples

Detect LDAP entry collisions in a View Connection Server group.

```
vdmadmin -X -collisions
```

Detect and resolve LDAP entry collisions.

```
vdmadmin -X -collisions -resolve
```



# Index

## A

- access groups
  - changing, for a desktop pool or a farm **102**
  - creating **96, 97, 102**
  - managing **101**
  - organizing desktops and pools **96**
  - removing **102**
  - reviewing desktop pools, application pools, or farms **103**
  - reviewing vCenter virtual machines **103**
  - root **96**
- Active Directory
  - preparing for clients in kiosk mode **230**
  - preparing for smart card authentication **50**
  - updating Foreign Security Principals of users **256**
  - updating general user information **135**
- ADM template files
  - View components **115**
  - View Common Configuration **118**
  - View Server Configuration **117**
  - where to find **116**
- administration
  - configuring **95**
  - delegating **96**
- administrator groups
  - creating **98**
  - managing **95, 98**
  - removing **99**
- administrator permissions
  - adding **100**
  - deleting **100**
  - managing **99**
  - viewing **101**
- administrator privileges
  - command line utilities **110**
  - common tasks **109**
  - desktop management **109**
  - general administration **110**
  - global **107**
  - internal **108**
  - object-specific **108**
  - persistent disk management **109**
  - pool management **109**
  - predefined **105**
  - understanding **95**
  - user and administrator management **110**
- administrator roles
  - adding custom **95, 104, 105**
  - managing custom **103**
  - modifying custom **104**
  - predefined **95, 105**
  - removing custom **104**
  - understanding **95**
- administrator users
  - creating **98, 99**
  - managing **98**
- Administrators (Read only) role **105**
- Administrators role **105**
- Adobe Flash
  - quality modes **180**
  - RDS desktops **202**
  - reducing bandwidth **180**
  - setting quality modes **180**
  - setting throttling modes **180**
  - throttling modes **180**
- Agent Registration Administrators role **105**
- alarm settings, performance **118**
- allowCertCRLs property **56**
- anti-affinity feature **209, 210**
- application pools
  - deleting **194**
  - editing **193**
  - managing **193**
- application packages, capturing and storing **212**
- application repositories
  - creating a network share **213**
  - load balancing **212**
  - problems registering **224**
  - problems scanning **225**
  - registering **213**
  - removing **224**
  - scanning **214**
- applications, monitoring concurrent users **134**
- ASP.NET IIS registration tool, RSA key container **140**
- audience information **7**
- authentication
  - enabling for clients in kiosk mode **234**
  - vdadmin command **251**
- authenticators for True SSO **89**

- automated farms
  - maintenance **196**
  - recompose **195**
- automated desktop pools
  - adding machines manually **178**
  - changing the pool size **177**
- B**
- backing up
  - configuration backup settings **125**
  - scheduling backups **124**
  - View configuration data **123**
  - View Connection Server **25**
- biometric authentication, configuring **65**
- Blast Extreme **34**
- Blast Secure Gateway service **133**
- C**
- CBRC, configuring for vCenter Server **19**
- certificate templates **78**
- certificate revocation checking
  - enabling **53**
  - troubleshooting for security server **246**
- certificates
  - accept the thumbprint **22**
  - updating on View Connection Server **141**
- certutil command **51**
- client accounts, adding for kiosk mode **233**
- client session policies
  - configuring global **114**
  - configuring pool-level **114**
  - configuring user-level **114**
  - defined **113**
  - general **115**
  - inheritance **113**
- client sessions
  - global settings **25, 26**
  - session timeouts **26**
  - setting timeouts **25**
- client systems
  - configuring in kiosk mode **229**
  - displaying information about kiosk mode **235, 270**
  - displaying MAC addresses **232**
  - preparing Active Directory for kiosk mode **230**
  - setting defaults for kiosk mode **231**
  - setting up in kiosk mode **229**
- configuration data
  - exporting with vdmexport **125**
  - importing with vdmimport **126**
- Connection Server service **133**
- Connection Server use, schedule maintenance
  - for automated farms **196**
- connectors for True SSO **88**

- Console Interaction privilege **107**
- credentials **73**
- credentials, user **72**
- CRL checking
  - configuring **54**
  - logging in **54**
- crlLocation property **54, 56**
- CSV output, vdmadmin command **251**
- custom administrator roles
  - creating **95**
  - managing **103**
  - modifying **104**
  - removing **104**
- customer experience program
  - additional features **144**
  - Cloud Pod Architecture data **155**
  - collecting data **142**
  - desktop pool data **148, 155, 157**
  - ensuring privacy **143**
  - global data **144**
  - joining or withdrawing **39**
  - machine data **151**
  - previewing collected data **143**
  - security server data **148**
  - ThinApp data **154**
  - vCenter Server data **153**
  - View Connection Server data **145**
- D**
- dashboard, monitoring View components **131**
- Data Collection Tool bundles, creating for View
  - Agent **241, 253**
- data recovery password, changing **26**
- database restore, View Composer sviconfig **128**
- DCT bundles, creating for View Agent **241, 253**
- dedicated-assignment pools
  - assigning user ownership **183**
  - removing user assignments **183**
  - user ownership **260**
- delegating administration **96**
- delete an unauthenticated access user **71**
- desktop management
  - deleting machines **187**
  - monitoring concurrent sessions **134**
  - understanding **183**
- desktop pools, managing **174**
- desktop pool deletion property, configuring **182**
- desktop pool management
  - deleting desktop pools **181**
  - disabling provisioning **179**
  - disabling desktop pools **179**
  - editable desktop pool settings **175**
  - editing desktop pools **174**
  - fixed desktop pool settings **177**

- desktop recomposition
  - linked-clone virtual machines **162**
  - preparing a parent virtual machine **161**
- detached persistent disks
  - attaching **169**
  - deleting **172**
  - editing the desktop pool or user **170**
  - recreating a virtual machine **170**
- detecting LDAP entry collisions **278**
- diagnostic information
  - collecting **241**
  - collecting for View Composer **243**
  - collecting using the support tool **243**
  - using support scripts **244**
- direct connections, configuring **33**
- Direct Interaction privilege **107**
- disjoint namespaces **211**
- domain filters
  - configuring **265**
  - displaying **263**
  - example of excluding domains **267**
  - example of including domains **266**
- domains
  - enumerating trusted **117**
  - filter lists **263**
  - secondary credentials **275**

## E

- Enable Farms and Desktop Pools privilege **108**
- enable unauthenticated access **69**
- enableOCSP property **55, 56**
- enableRevocationChecking property **54–56**
- encryption, of user credentials **72**
- enrollment server **79**
- enrollment servers, commands for managing **87**
- Enrollment Service Client certificate **81, 82**
- enterprise CA **76**
- Enterprise NTAAuth store, adding root certificates **51**
- Entitle Desktop and Application Pools privilege **108**
- entitle unauthenticated access users **70**
- events
  - generating output in syslog format **259**
  - monitoring **240**
  - types and descriptions **240**
- exclusion lists **265**
- expiration period for SAML metadata **64**
- external URL, editing **38**

## F

- farms
  - deleting **194**

- disabling **195**
- editing **194**
- enabling **195**
- managing **193, 194**
- filter lists, adding and removing domains **263**
- Flexible Authentication **229**
- Foreign Security Principals, updating **256**
- Framework Component service **133**
- FSPs, updating **256**
- Full (Read only) privilege **108**

## G

- gatewayLocation **37**
- global policies, configuring **114**
- Global Configuration and Policy Administrators role **105**
- Global Configuration and Policy Administrators (Read only) role **105**
- global settings
  - client sessions **25, 26**
  - message security mode **30**
- group policies
  - ADM template files **116**
  - View common configuration **118**
  - View components **115**
  - View Connection Server **117**
- GUIDs, displaying for View Connection Server group **255**

## H

- health monitors, listing and displaying **257**
- Horizon Client
  - collecting diagnostic information **244**
  - saving log files **242**
  - troubleshooting **239**
  - using with kiosk clients **236**
- host caching, for vCenter Server **19**
- HTML access, configuring **34**
- HTTP, allowing for SSL off-loading **36**

## I

- inclusion lists **265**
- instant clones, recover **188**
- instant-clone desktop pools
  - cancel a push-image operation **174**
  - change the image **173**
  - managing **173**
  - monitor a push-image operation **174**
  - push-image operations
    - cancel **174**
    - reschedule **174**
  - reschedule a push-image operation **174**
  - schedule a push image **173**

- intermediate certificates
  - adding to intermediate certification authorities **52**
  - See also* certificates
- Intermediate Certification Authorities policy **52**
- Inventory Administrators (Read only) role **105**
- Inventory Administrators role **105**
- IP addresses, overriding for View Agent **254**
- IPSec, security server connections **29**

## J

- JMS message security mode **31**

## K

- keytool utility **46**
- kiosk mode
  - adding client accounts **233**
  - configuring **229**
  - connecting to desktops **236**
  - displaying information about clients **235**
  - displaying MAC address of client devices **232**
  - enabling authentication of clients **234**
  - managing client authentication **270**
  - preparing Active Directory **230**
  - setting defaults for clients **231**
  - setting up **229**
  - viewing and modifying client accounts **270**
- Knowledge Base articles, where to find **247**

## L

- LDAP entries, detecting and resolving collisions **278**
- LDAP repository
  - backing up **125**
  - importing **126**
- licenses
  - adding to View **134**
  - monitoring usage **134**
  - resetting **135**
- linked-clone desktop management, managing persistent disks **168**
- linked-clone desktop virtual machine management, understanding **159**
- linked-clone machine management
  - refresh operation guidelines **160**
  - refreshing **159**
- linked-clone virtual machine management
  - detaching persistent disks **168**
  - disk filenames after a rebalance **167**
  - managing persistent disks **168**
  - migrating to another datastore **167**
  - preparing a parent virtual machine for recompositon **161**
  - rebalancing **165, 166**

- recomposing **162, 163**
- recomposing machines **161**
- restoring persistent disks from vSphere **171**
- linked-clone virtual machine troubleshooting,
  - correcting an unsuccessful recomposition **164**
- Linux systems, using with View Administrator **12**
- load balancers, off-loading SSL connections **35**
- load balancing scripts **203–206**
- load balancing, application repositories **212**
- load balancing RDS hosts **203, 207**
- locked.properties file
  - configuring CRL checking **54**
  - configuring OCSP checking **55**
  - configuring smart card authentication **47**
  - configuring smart card certificate revocation **56**
  - off-loading SSL connections **36**
- locking, machines **277**
- log files
  - collecting for Horizon Client **242**
  - configuring settings **118**
  - configuring in View Agent **253**
  - displaying for View Connection Server **52**
- Log in as current user feature **72**
- logging levels, View Agent **253**

## M

- MAC addresses, displaying for client systems **232**
- Mac systems, using with View Administrator **12**
- machine management
  - displaying machines for unentitled users **269**
  - displaying the first user of a machine **274**
  - exporting information to a file **191**
  - monitoring machine status **131, 184**
- machine recomposition, linked-clone virtual machines **161**
- machine refresh, linked clones **160**
- machine status
  - locating machines **131, 184**
  - physical computers **189**
  - RDS hosts **189, 201**
  - virtual machines **185**
- machines
  - locking and unlocking **277**
  - managing physical computers **188**
- maintenance mode
  - entering **184**
  - exiting **184**
- Manage Composer Desktop Pool Image privilege **108**
- Manage Farms and Desktop and Application Pools privilege **108**

- Manage Global Configuration and Policies privilege **107**
- Manage Global Configuration and Policies (Read only) privilege **108**
- Manage Inventory (Read only) privilege **108**
- Manage Persistent Disks privilege **108**
- Manage Reboot Operation privilege **108**
- Manage Roles and Permissions privilege **107**
- Manage Sessions privilege **108**
- manual farms
  - adding an RDS host **199**
  - removing an RDS host **200**
- max concurrent power operations, configuration guidelines **21**
- Message Bus Component service **133**
- message security mode
  - global settings **30**
  - JMS **31**
- migrating
  - linked-clone virtual machines **167**
  - View Composer with an existing database **137**
  - View Composer without linked clones **139**
  - View Composer to another machine **136**
- MSI packages
  - creating **212**
  - invalid **227**

## N

- NET Framework, migrating RSA key container **140**

## O

- OCSP certificate revocation checking
  - configuring **55**
  - logging in **54**
- ocspCRLFailover property **56**
- ocspSendNonce property **56**
- ocspSigningCert **56**
- ocspSigningCert property **55**
- ocspURL property **55, 56**
- orphaned machines, displaying **269**
- OS disks, machine refresh **159, 160**
- OUs, creating for kiosk mode clients **230**
- output formats, vdmadmin command **251**
- overriding IP addresses for View Agent **254**

## P

- passwords **73**
- pcoip.adm, ADM template files **116**
- performance alarms, configuring **118**
- permissions
  - adding **100**
  - deleting **100**
  - viewing **97**

- persistent disks
  - attaching **169**
  - deleting detached disks **172**
  - detaching **168**
  - editing the desktop pool or user **170**
  - importing from a vSphere datastore **171**
  - recreating a virtual machine **170**
  - understanding **168**
  - View Composer **168**
- physical computers
  - adding to a pool **188**
  - displaying information about **261**
  - machine status **189**
  - removing from a pool **188**
- policies
  - client session **113**
  - client session inheritance **113**
  - configuring for View **113**
  - displaying for unentitled users **269**
  - general client session **115**
  - global **114**
  - Intermediate Certification Authorities **52**
  - pool-level **114**
  - Trusted Root Certification Authorities **51**
  - user-level **114**
- pool size, changing **177**
- power operations, setting concurrency limits **21**
- pre-login messages, displaying to clients **26**
- predefined administrator roles **95**
- privileges, *See* administrator privileges
- problem desktops, viewing **239**
- product license key, resetting **135**
- push image **173**
- push-image operations, monitor **174**

## R

- RADIUS authentication
  - enabling **58**
  - logging in **58**
- RDS desktops, Adobe Flash Throttling **202**
- RDS hosts
  - adding to a manual farm **199**
  - desktop status **189**
  - disabling **200**
  - editing **199**
  - enabling **200**
  - machine status **201**
  - managing **193, 199**
  - monitoring **201**
  - removing from View **200**
  - removing from a manual farm **200**
  - view properties of **201**
- rebalancing linked-clone virtual machines, disk filenames after a rebalance **167**

- recomposing linked-clone virtual machines **162**
- recomposing machines, View Composer **161**
- recomposing virtual machines
  - correcting an unsuccessful recomposition **164**
  - View Composer **163**
- refresh
  - linked-clone machines **159**
  - View Composer **160**
- Register Agent privilege **107**
- registered machines
  - removing **189**
  - removing from View **189**
- Remember this password check box **72**
- remote sessions
  - privileges for managing **109**
  - viewing **239**
- removing registered machines **189**
- reports, displaying **258**
- resolving LDAP entry collisions **278**
- restored data, result codes **129**
- restoring, View configuration data **123, 126**
- result codes, restored data operation **129**
- role-based delegated administration
  - best practices **111**
  - configuring **95**
- roles, *See* administrator roles
- root certificates
  - adding to the Enterprise NTAAuth store **51**
  - adding to trusted roots **51**
  - exporting **45**
  - importing to a server truststore file **46**
  - obtaining **45**
- root access group **96**
- RSA Agent host node secret, resetting **60**
- RSA key container
  - migrating to View Composer **140**
  - using NET Framework **140**
- RSA SecurID authentication
  - configuring **57**
  - enabling **58**
  - logging in **58**
  - troubleshooting **60**

## S

- SAML **62, 65**
- SAML 2.0 Authentication **61**
- SAML 2.0 authenticators, configuring in View
  - Administrator **62, 65**
- SAML authentication with True SSO **83**
- SAML metadata for View Connection Server **65**
- Save password check box **72**
- Save Password check box **73**
- saving credential information **73**
- saving credentials **72**

- SCOM, setting the name of a View Connection
  - Server group **255**
- Script Host service **133, 205**
- search exclusion lists **265**
- secondary credentials, providing for
  - administrators **275**
- security server
  - problems with certificate revocation
    - checking **246**
  - removing entry from configuration **274**
  - troubleshooting pairing with View Connection
    - Server **245**
- Security Gateway Component service **133**
- Security Server service **133**
- security servers
  - enabling smart card authentication **47**
  - services **133**
  - updating certificates **141**
- services
  - security server hosts **133**
  - stopping and starting **132**
  - understanding **132**
  - View Connection Server hosts **133**
- session management **191**
- sessions, privileges for managing **108**
- Setup Capture wizard, ThinApp **212**
- single sign-on (SSO) **72**
- smart card authentication
  - Active Directory preparation **50**
  - certificate revocation checking **53**
  - configuring **44, 47, 49**
  - understanding **43**
  - UPNs for smart card users **50**
  - verifying configuration **52**
- smart card certificates, revoking **53**
- smart cards
  - exporting user certificates **45**
  - using to authenticate **44**
- sparse disks, configuring for vCenter Server **18**
- SSL
  - accept a certificate thumbprint **22**
  - enabling for client connections **25, 29**
  - importing certificates to View servers **35**
  - off-loading to intermediate servers **35**
  - setting external URLs for intermediate
    - servers **36**
- SSL certificates, *See* certificates
- SSO
  - disabling **26**
  - enabling **26**
  - setting timeout limits **26**
- storage, reclaiming disk space **18**
- Storage vMotion, migrating linked clones **167**

- support requests
  - collecting log files **242**
  - updating **245**
- support scripts
  - collecting diagnostic information **244**
  - View Composer **243**
- support tool, using to collect diagnostic information **243**
- svconfig utility
  - restoring the database **128**
  - result codes for restoredata **129**
- Syslog format, generating log messages **259**
- system health dashboard **239**

## T

- templates, certificate **78**
- text display issues, View Administrator **12**
- ThinApp applications
  - assigning **215–218**
  - checking installation status **220**
  - configuration walkthrough **227**
  - displaying MSI package information **221**
  - maintaining **221**
  - packaging **212**
  - problems assigning **225**
  - problems installing **226**
  - problems uninstalling **226**
  - removing assignments **222, 223**
  - removing from View Administrator **223**
  - requirements **211**
  - reviewing assignments **220**
  - troubleshooting **224**
  - upgrading **221**
- ThinApp templates
  - assigning **219**
  - creating **214**
  - removing **224**
- ThinApp Setup Capture wizard **212**
- thumbprint, accept for a default certificate **22**
- True SSO
  - advanced configuration settings through Windows Registry **90**
  - agent configuration settings **90**
  - configuring **84, 86**
  - connection server configuration settings **92**
  - enrollment server configuration settings **90**
    - troubleshooting, using the system health dashboard **92**
- trusted domains, enumerating **117**
- Trusted Root Certification Authorities policy **51**
- trustKeyfile property **47**
- trustStoretype property **47**
- two-factor authentication **57, 60**

## U

- unassigning users, dedicated-assignment pools **183**
- unauthenticated access **67**
- unauthenticated access user **69**
- unauthenticated access for Horizon Clients **71**
- unauthenticated access user sessions **70**
- unentitled users, displaying machines **269**
- Unix systems, using with View Administrator **12**
- Unknown username or bad password **234, 270**
- unlocking, machines **277**
- unmanaged machines
  - adding to a pool **188**
  - managing **188**
  - removing from a pool **188**
- updating linked-clone virtual machines
  - correcting an unsuccessful recomposition **164**
  - machine recomposition **161**
- UPNs, smart card users **50**
- useCertAuth property **47, 52**
- user authentication, configuring **57**
- user accounts, View Composer AD operations **13**
- userPrincipalName attribute **50**
- users
  - displaying information about **277**
  - updating general user information **135**

## V

- vCenter Server
  - configuring concurrent operations limits **21**
  - configuring host caching **19**
  - configuring sparse disks **18**
- vCenter Server instances
  - adding in View Administrator **13, 14**
  - correcting conflicting unique IDs **24**
  - removing in View Administrator **23**
- vdm\_agent.adm **116**
- vdm\_client.adm **116**
- vdm\_common.adm **116, 118**
- vdm\_server.adm **116, 117**
- vdmadmin command
  - authentication **251**
  - command options **252**
  - introduction **249**
  - output formats **251**
  - syntax **251**
- vdmutil command-line utility **31, 84, 86**
- View Storage Accelerator, configuring for vCenter Server **19**
- View Administrator
  - logging in **10**
  - managing a View deployment **9**
  - navigating **10**

- overview **9**
  - text display issues **12**
  - tips for using **10**
  - using the health dashboard **239**
  - using with Linux, Unix, or Mac **12**
  - View Agent
    - collecting diagnostic information **244**
    - configuring logging levels **253**
    - creating a Data Collection Tool bundle **241**
    - overriding IP addresses **254**
  - View components, maintaining **123**
  - View Composer configuration
    - concurrent operations limits **21**
    - configuring settings for vCenter Server **16**
    - creating a user account **13**
    - domains **17**
    - removing the service from vCenter Server **24**
  - View Composer maintenance
    - backing up configuration data **25, 123**
    - guidelines for migrating **137**
    - migrating an RSA key container **140**
    - migrating View Composer to another machine **136**
    - migrating with the existing database **137**
    - restoring configuration data **126**
    - restoring the database **128**
    - scheduling backups **124**
  - View Composer persistent disks
    - attaching **169**
    - deleting detached **172**
    - detaching **168**
    - editing the desktop pool or user **170**
    - importing from vSphere **171**
    - management overview **168**
    - understanding **168**
  - View Composer troubleshooting
    - collecting diagnostic information **243**
    - correcting an unsuccessful recomposition **164**
    - overview **239**
  - View Composer use
    - managing linked-clone desktop virtual machines **159**
    - migrating linked-clone virtual machines **167**
    - preparing a parent virtual machine for recomposition **161**
    - rebalancing linked-clone virtual machines **165, 166**
    - recomposing automated farms **195**
    - recomposing linked-clone virtual machines **162**
    - recreating a virtual machine with a detached persistent disk **170**
    - refreshing machines **159**
    - understanding desktop recomposition **161**
    - understanding machine refresh operations **160**
    - understanding virtual machine recomposition **163**
  - View Connection Server
    - backing up configuration data **25, 123**
    - collecting diagnostic information **244**
    - configuring **13**
    - configuring direct connections **33**
    - disabling **38**
    - editing the external URL **38**
    - exporting configuration data **125**
    - removing entry from configuration **274**
    - restoring configuration data **126**
    - scheduling backups **124**
    - services **132, 133**
    - setting names of groups **255**
    - View LDAP configuration data **40**
  - View Connection Server configuration, server certificate **141**
  - View LDAP, configuration data **40**
  - View services, stopping and starting **132**
  - ViewPM.adm, ADM template files **116**
  - virtual machines
    - displaying information about **261**
    - machine status **185**
    - managing **173, 183**
    - reclaiming disk space **262**
  - virtual machine recomposition
    - correcting an unsuccessful recomposition **164**
    - linked-clone virtual machines **163**
  - VMware Identity Manager **67**
  - VMware ThinApp
    - integrating with View **211**
    - using the Setup Capture wizard **212**
  - VMwareVDMDS service **133**
- ## W
- Web Component service **133**
- ## X
- XML output, vdmadmin command **251**