

# Upgrading to VMware Identity Manager 2.6 from 2.4

VMware Identity Manager 2.6

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

EN-002016-01

**vmware**<sup>®</sup>

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

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

The VMware Web site also provides the latest product updates.

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

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

Copyright © 2016 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

	Upgrading to VMware Identity Manager 2.6 from 2.4	5
<b>1</b>	<b>About Upgrading to VMware Identity Manager 2.6</b>	<b>7</b>
	Upgrading a Cluster	7
<b>2</b>	<b>Upgrading VMware Identity Manager Online</b>	<b>9</b>
	Prerequisites for Online Upgrade	9
	Check for the Availability of a VMware Identity Manager Upgrade Online	10
	Configure Proxy Server Settings for the VMware Identity Manager Appliance	10
	Perform an Online Upgrade to VMware Identity Manager 2.6	10
<b>3</b>	<b>Upgrading VMware Identity Manager Offline</b>	<b>13</b>
	Prerequisites for Offline Upgrade	13
	Prepare a Local Web Server for Offline Upgrade	13
	Configure the Appliance and Perform Offline Upgrade	14
<b>4</b>	<b>Configure Settings after Upgrade</b>	<b>17</b>
<b>5</b>	<b>Troubleshooting Upgrade Errors</b>	<b>19</b>
	Checking the Upgrade Error Logs	19
	Rolling Back to Snapshots of VMware Identity Manager	19
	Collecting a Log File Bundle	20
	Index	21



# Upgrading to VMware Identity Manager 2.6 from 2.4

---

*Upgrading to VMware Identity Manager 2.6 from 2.4* describes how to upgrade from version 2.4.x to 2.6.

If you would prefer to do a fresh installation of version 2.6, see *VMware Identity Manager Installation and Configuration*. Remember that a new installation does not preserve your existing configurations.

For information about using your updated VMware Identity Manager instance, see the *VMware Identity Manager Administrator's Guide*.

## Intended Audience

This information is intended for anyone who installs, upgrades, and configures VMware Identity Manager. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology.

## VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to <http://www.vmware.com/support/pubs>.



# About Upgrading to VMware Identity Manager 2.6

---

# 1

The following upgrade paths and scenarios are supported.

## Supported Upgrade Paths

The following upgrade paths are supported:

- Version 2.4.x to 2.6

## Internet Connectivity

You can upgrade to VMware Identity Manager 2.6 online or offline.

By default, the VMware Identity Manager appliance uses the VMware Web site for the upgrade procedure, which requires the appliance to have Internet connectivity. You must also configure proxy server settings for the appliance, if applicable.

If your virtual appliance does not have Internet connectivity, you can perform the upgrade offline. For an offline upgrade, you download the upgrade package from My VMware and set up a local Web server to host the upgrade file.

## Upgrade Scenarios

- If you have deployed a single VMware Identity Manager appliance, upgrade it online or offline as described in [Chapter 2, “Upgrading VMware Identity Manager Online,”](#) on page 9 or [Chapter 3, “Upgrading VMware Identity Manager Offline,”](#) on page 13.

---

**NOTE** Expect some downtime because all services are stopped during the upgrade. Plan the timing of your upgrade accordingly.

---

- If you have deployed multiple VMware Identity Manager virtual appliances in a cluster for failover or high availability, see [“Upgrading a Cluster,”](#) on page 7.

## Upgrading a Cluster

If you have deployed multiple VMware Identity Manager virtual appliances in a cluster for failover or high availability, you can upgrade the nodes one at a time. Expect some downtime during upgrade and plan the timing of your upgrade accordingly.

### Procedure

- 1 Take snapshots of the database and the VMware Identity Manager nodes.
- 2 Remove all nodes except one from the load balancer.

- 3 Upgrade the node that is still connected to the load balancer. Follow the process for an online or offline upgrade.

---

**IMPORTANT** Expect some downtime during the upgrade process.

---

- 4 After the node is upgraded, leave it connected to the load balancer.  
This ensures that the VMware Identity Manager service is available while you upgrade the other nodes.
- 5 Upgrade the other nodes one at a time.
- 6 After all the nodes are upgraded, add them back to the load balancer.



# Upgrading VMware Identity Manager Online

---

# 2

You can upgrade the VMware Identity Manager virtual appliance online. The virtual appliance must be able to connect to the Internet for an online upgrade.

This chapter includes the following topics:

- [“Prerequisites for Online Upgrade,”](#) on page 9
- [“Check for the Availability of a VMware Identity Manager Upgrade Online,”](#) on page 10
- [“Configure Proxy Server Settings for the VMware Identity Manager Appliance,”](#) on page 10
- [“Perform an Online Upgrade to VMware Identity Manager 2.6,”](#) on page 10

## Prerequisites for Online Upgrade

Before you upgrade the VMware Identity Manager virtual appliance online, perform these prerequisite tasks.

- Verify that at least 2.5 GB of disk space is available on the primary root partition of the virtual appliance.
- Take a snapshot of your virtual appliance to back it up. For information about how to take snapshots, see the vSphere documentation.
- If you are using an external database, take a snapshot or backup of the database.
- Verify that VMware Identity Manager is properly configured.
- Verify that the virtual appliance can resolve and reach vapp-updates.vmware.com on port 80 over HTTP.
- If an HTTP proxy server is required for outbound HTTP access, configure the proxy server settings for the virtual appliance. See [“Configure Proxy Server Settings for the VMware Identity Manager Appliance,”](#) on page 10.
- Confirm that a VMware Identity Manager upgrade exists. Run the appropriate command to check for upgrades. See [“Check for the Availability of a VMware Identity Manager Upgrade Online,”](#) on page 10.

## Check for the Availability of a VMware Identity Manager Upgrade Online

If your VMware Identity Manager virtual appliance can connect to the Internet, you can check for the availability of upgrades online from the appliance.

### Procedure

- 1 Log in to the virtual appliance as the root user.
- 2 Run the following command to check for an online upgrade.

```
/usr/local/horizon/update/updatemgr.hzn check
```

## Configure Proxy Server Settings for the VMware Identity Manager Appliance

The VMware Identity Manager virtual appliance accesses the VMware update servers through the Internet. If your network configuration provides Internet access using an HTTP proxy, you must adjust the proxy settings for the appliance.

Enable your proxy to handle only Internet traffic. To ensure that the proxy is set up correctly, set the parameter for internal traffic to `no-proxy` within the domain.

---

**NOTE** Proxy servers that require authentication are not supported.

---

### Prerequisites

- Verify that you have the root password for the virtual appliance.
- Verify that you have the proxy server information. Note that proxy servers that require authentication are not supported.

### Procedure

- 1 Log in to the VMware Identity Manager virtual appliance as the root user.
- 2 Enter `YaST` on the command line to run the YaST utility.
- 3 Select **Network Services** in the left pane, then select **Proxy**.
- 4 Enter the proxy server URLs in the **HTTP Proxy URL** and **HTTPS Proxy URL** fields.
- 5 Select **Finish** and exit the YaST utility.
- 6 Restart the Tomcat server on the VMware Identity Manager virtual appliance to use the new proxy settings.

```
service horizon-workspace restart
```

The VMware update servers are now available to the VMware Identity Manager virtual appliance.

## Perform an Online Upgrade to VMware Identity Manager 2.6

If your VMware Identity Manager virtual appliance has Internet connectivity, you can upgrade the appliance online.

### Prerequisites

- Ensure that you meet the prerequisites listed in [“Prerequisites for Online Upgrade,”](#) on page 9.
- Verify that the virtual appliance is powered on and functioning.

**Procedure**

- 1 Log in to the VMware Identity Manager virtual appliance as the root user.
- 2 Run the following `updatemgr.hzn` command.  

```
/usr/local/horizon/update/updatemgr.hzn updateinstaller
```
- 3 Run the following command to check that an online upgrade exists.  

```
/usr/local/horizon/update/updatemgr.hzn check
```
- 4 Run the following command to update the appliance.  

```
/usr/local/horizon/update/updatemgr.hzn update
```

Messages that occur during the upgrade are saved to the `update.log` file at `/opt/vmware/var/log/update.log`.
- 5 Run the `updatemgr.hzn check` command again to verify that a newer update does not exist.  

```
/usr/local/horizon/update/updatemgr.hzn check
```
- 6 Check the version of the upgraded appliance.  

```
vami-cli version --appliance
```

The new version is displayed.
- 7 Restart the virtual appliance.  

```
reboot
```

The upgrade is complete.



# Upgrading VMware Identity Manager Offline

# 3

If your VMware Identity Manager virtual appliance cannot connect to the Internet for upgrade, you can perform an offline upgrade. You must set up an upgrade repository on a local Web server and configure the appliance to use the local Web server for upgrade.

This chapter includes the following topics:

- “Prerequisites for Offline Upgrade,” on page 13
- “Prepare a Local Web Server for Offline Upgrade,” on page 13
- “Configure the Appliance and Perform Offline Upgrade,” on page 14

## Prerequisites for Offline Upgrade

Before you upgrade the VMware Identity Manager virtual appliance offline, perform these prerequisite tasks.

- Verify that at least 2.5 GB of disk space is available on the primary root partition of the virtual appliance.
- Take a snapshot of your virtual appliance to back it up. For information about how to take snapshots, see the vSphere documentation.
- If you are using an external database, take a snapshot or backup of the database.
- Verify that VMware Identity Manager is properly configured.
- Confirm that a VMware Identity Manager upgrade exists. Check the My VMware site at [my.vmware.com](http://my.vmware.com) for upgrades.
- Prepare a local Web server to host the upgrade file. See “Prepare a Local Web Server for Offline Upgrade,” on page 13.

## Prepare a Local Web Server for Offline Upgrade

Before you start the offline upgrade, set up the local Web server by creating a directory structure that includes a subdirectory for the VMware Identity Manager virtual appliance.

### Prerequisites

- Obtain the `identity-manager-2.6.x.x-buildNumber-updaterepo.zip` file. Go to [my.vmware.com](http://my.vmware.com) and navigate to the VMware Identity Manager product download page to download the file.
- If you use an IIS Web server, configure the Web server to allow special characters in file names. You configure this in the **Request Filtering** section by selecting the **Allow double escaping** option.

### Procedure

- 1 Create a directory on the Web server at `http://YourWebServer/VM/` and copy the downloaded zip file to it.
- 2 Verify that your Web server includes mime types for `.sig` (text/plain) and `.sha256` (text/plain).  
Without these mime types your Web server fails to check for updates.
- 3 Unzip the file.  
The contents of the extracted ZIP file are served by `http://YourWebServer/VM/`.  
The extracted contents of the file contain the following subdirectories: `/manifest` and `/package-pool`.
- 4 Run the following `updateLocal.hzn` command to check that the URL has valid update contents.  

```
/usr/local/horizon/update/updatesLocal.hzn checkurl http://YourWebServer/VM
```

## Configure the Appliance and Perform Offline Upgrade

Configure the VMware Identity Manager appliance to point to the local Web server to perform an offline upgrade. Then upgrade the appliance.

### Prerequisites

[“Prepare a Local Web Server for Offline Upgrade,”](#) on page 13.

### Procedure

- 1 Log in to the VMware Identity Manager appliance as the root user.
- 2 Run the following command to configure an upgrade repository that uses a local Web server.  

```
/usr/local/horizon/update/updatesLocal.hzn seturl http://YourWebServer/VM/
```

---

**NOTE** To undo the configuration and restore the ability to perform an online upgrade, you can run the following command.

```
/usr/local/horizon/update/updatesLocal.hzn setdefault
```

---

- 3 Perform the upgrade.
  - a Run the following `updateMgr.hzn` command.  

```
/usr/local/horizon/update/updatesMgr.hzn updateinstaller
```
  - b Run the following command.  

```
/usr/local/horizon/update/updatesMgr.hzn update
```

  
Messages that occur during the upgrade are saved to the `update.log` file at `/opt/vmware/var/log/update.log`.
  - c Run the `updateMgr.hzn check` command again to verify that a newer update does not exist.  

```
/usr/local/horizon/update/updatesMgr.hzn check
```

- d Check the version of the upgraded appliance.

```
vamicli version --appliance
```

The command should display the new version.

- e Restart the virtual appliance.

For example, from the command line run the following command.

```
reboot
```

The upgrade is complete.





## Configure Settings after Upgrade

---

After you upgrade to VMware Identity Manager 2.6, configure these settings.

- Enable the new portal user interface.
  - a In the administration console, click the arrow on the **Catalog** tab and select **Settings**.
  - b Select **New End User Portal UI** in the left pane and click **Enable New Portal UI**.
- If you use ThinApps, Kerberos authentication, or Active Directory (Integrated Windows Authentication) directories, you must leave the domain and then rejoin it. This is required for all the virtual appliances in your deployment.
  - a Click the **Identity & Access Management** tab.
  - b Click **Setup**.
  - c In the Connectors page, for each connector that is being used for ThinApps integration, Kerberos authentication, or an Active Directory (Integrated Windows Authentication) directory, click **Leave Domain**.
  - d Click **Join Domain** to join the domain again.

To join the domain, you need Active Directory credentials with the privileges to join the domain. See "Integrating with Active Directory" in *Installing and Configuring VMware Identity Manager* for more information about joining a domain.
  - e If you are using Kerberos authentication, enable the Kerberos authentication adapter again. To access the Auth Adapters page, in the Connectors page click the appropriate link in the **Worker** column and select the **Auth Adapters** tab.
  - f Verify that the other authentication adapters you are using are enabled.
- If you are using Active Directory (Integrated Windows Authentication), or Active Directory over LDAP with the **This Directory supports DNS Service Location** option enabled, save the directory's Domains page.
  - a Click the **Identity & Access Management** tab.
  - b In the Directories page, click the directory.
  - c Provide the password for the Bind DN user and click **Save**.
  - d Click **Sync Settings** on the left of the page and select the **Domains** tab.

- e Click **Save**.

---

**NOTE** In VMware Identity Manager 2.6, a `domain_krb.properties` file is automatically created and auto-populated with domain controllers when a directory with DNS Service Location enabled is created. When you save the Domains page after upgrade, if you had a `domain_krb.properties` file in your original deployment, the file is updated with domains that you may have added subsequently and that were not in the file. If you did not have a `domain_krb.properties` file in your original deployment, the file is created and auto-populated with domain controllers. See "Integrating with Active Directory" in *Installing and Configuring VMware Identity Manager* for more information about the `domain_krb.properties` file.

---

- Beginning with 2.6, you can sync users and groups that have the same username or group name across multiple Active Directory domains. The uniqueness rule was updated to be a combination of username or group name and domain. For example, a username Administrator can have both an Active Directory account in multiple Active Directory domains, as well as a local user account in the VMware Identity Manager service. When you upgrade to 2.6, this feature is not enabled. Contact support for information about how to enable the username and group name uniqueness rule.
- Transport Layer Security (TLS) protocol 1.0 is disabled by default in VMware Identity Manager 2.6. During upgrade to 2.6, TLS 1.0 is disabled. TLS 1.1 and 1.2 are supported in VMware Identity Manager 2.6.

External product issues are known to occur when TLS 1.0 is disabled. Updating your other product configurations to use TLS 1.1 or 1.2 is recommended. However, if your version of products such as Horizon, Horizon Air, Citrix, or load balancers have a dependence on TLS 1.0, you can enable TLS 1.0 in VMware Identity Manager after upgrade by following the instructions in [Knowledge Base article 2144805](#).

# Troubleshooting Upgrade Errors

---

You can troubleshoot upgrade problems by reviewing the error logs. If VMware Identity Manager does not start, you can revert to a previous instance by rolling back to a snapshot.

This chapter includes the following topics:

- [“Checking the Upgrade Error Logs,”](#) on page 19
- [“Rolling Back to Snapshots of VMware Identity Manager,”](#) on page 19
- [“Collecting a Log File Bundle,”](#) on page 20

## Checking the Upgrade Error Logs

Resolve errors that occur during upgrade by reviewing the error logs. Upgrade log files are in the `/opt/vmware/var/log` directory.

### Problem

After the upgrade finishes, VMware Identity Manager does not start and errors appear in the error logs.

### Cause

Errors occurred during upgrade.

### Solution

- 1 Log in to the VMware Identity Manager virtual appliance.
- 2 Go to the directory located at `/opt/vmware/var/log`.
- 3 Open the `update.log` file and review the error messages.
- 4 Resolve the errors and rerun the upgrade command. The upgrade command resumes from the point where it stopped.

---

**NOTE** Alternatively, you can revert to a snapshot and run the upgrade again.

---

## Rolling Back to Snapshots of VMware Identity Manager

If VMware Identity Manager does not start properly after an upgrade, you can roll back to a previous instance.

### Problem

After you upgrade VMware Identity Manager, it does not start correctly. You reviewed the upgrade error logs and ran the upgrade command again but it did not resolve the issue.

**Cause**

Errors occurred during the upgrade process.

**Solution**

- ◆ Revert to one of the snapshots you took as a backup of your original VMware Identity Manager instance and external database, if applicable. For information, see the vSphere documentation.

## Collecting a Log File Bundle

You can collect a bundle of log files. You obtain the bundle from the VMware Identity Manager appliance configuration page.

The following log files are collected in the bundle.

**Table 5-1.** Log Files

Component	Location of Log File	Description
Apache Tomcat Logs (catalina.log)	/opt/vmware/horizon/workspace/logs/catalina.log	Apache Tomcat records messages that are not recorded in other log files.
Configurator Logs (configurator.log)	/opt/vmware/horizon/workspace/logs/configurator.log	Requests that the Configurator receives from the REST client and the Web interface.
Connector Logs (connector.log)	/opt/vmware/horizon/workspace/logs/connector.log	A record of each request received from the Web interface. Each log entry also includes the request URL, timestamp, and exceptions. No sync actions are recorded.
Service Logs (horizon.log)	/opt/vmware/horizon/workspace/logs/horizon.log	The service log records activity that takes place on the VMware Identity Manager appliance, such as activity related to entitlements, users, and groups.
Unified Catalog Logs (greenbox_web.log)	/opt/vmware/horizon/workspace/logs/greenbox_web.log	Records activity related to the unified catalog.

**Procedure**

- 1 Log in to the VMware Identity Manager appliance configuration page at <https://identitymanagerURL:8443/cfg/logs>.
- 2 Click **Prepare log bundle**.
- 3 Download the bundle.

# Index

## C

check for upgrade online **10**  
cluster, upgrade **7**  
collect log bundle **20**

## D

domain **17**  
domain\_krb.properties file **17**

## E

error logs **19**  
errors **19**

## G

glossary **5**

## H

HTTP proxy **10**

## I

intended audience **5**

## J

join domain **17**

## L

local Web server **14**  
log bundle **20**

## N

new portal user interface **17**

## O

offline upgrade **13**  
online upgrade **9, 10**

## P

point to local Web server **14**  
prepare local Web server **13**  
prerequisites for offline upgrade **13**  
prerequisites for online upgrade **9**  
proxy server **10**

## R

roll back to snapshot **19**

## S

snapshots **19**

## T

troubleshooting **19**

## U

upgrade **7**  
upgrade errors **19**

