

Upgrading to VMware Identity Manager 3.0

SEP 2017

VMware AirWatch 9.2

VMware Identity Manager 3.0



vmware®

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

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

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

docfeedback@vmware.com

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

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

Contents

	Upgrading to VMware Identity Manager 3.0	4
1	About Upgrading to VMware Identity Manager 3.0	5
	Upgrading a Cluster	6
2	Upgrading VMware Identity Manager Online	7
	Prerequisites for Online Upgrade	7
	Check for the Availability of a VMware Identity Manager Upgrade Online	8
	Configure Proxy Server Settings for the VMware Identity Manager Appliance	8
	Perform an Online Upgrade	9
3	Upgrading VMware Identity Manager Offline	10
	Prerequisites for Offline Upgrade	10
	Prepare a Local Web Server for Offline Upgrade	11
	Configure the Appliance and Perform Offline Upgrade	11
4	Settings to Configure after Upgrade	13
5	Troubleshooting Upgrade Errors	15
	Checking the Upgrade Error Logs	15
	Rolling Back to Snapshots of VMware Identity Manager	16
	Collecting a Log File Bundle	16

Upgrading to VMware Identity Manager 3.0

Upgrading to VMware Identity Manager 3.0 describes how to upgrade to VMware Identity Manager 3.0 from earlier versions.

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

For information about using your upgraded 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 3.0

1

The following upgrade paths and scenarios are supported.

Supported Upgrade Paths

The following upgrade paths are supported:

- Version 2.8.x and later to 3.0.x

Compatibility with AirWatch

If you upgrade to AirWatch 9.2, you must also upgrade VMware Identity Manager to version 3.0. AirWatch 9.2 is not compatible with earlier versions of VMware Identity Manager.

You can use VMware Identity Manager 3.0 with earlier versions of AirWatch. Using the latest available version of the products is recommended.

Internet Connectivity

You can upgrade VMware Identity Manager 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](#) or [Chapter 3 Upgrading VMware Identity Manager Offline](#).

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](#).
- To upgrade VMware Identity Manager with no downtime in a multi-data center deployment scenario, see "Upgrading VMware Identity Manager with No Downtime" in *Installing and Configuring VMware Identity Manager*.

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, as described in [Chapter 2 Upgrading VMware Identity Manager Online](#) or [Chapter 3 Upgrading VMware Identity Manager Offline](#).

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 Verify that RabbitMQ is not running in cluster mode in the upgraded nodes.

In 2.9.1 and later releases, RabbitMQ clustering has been disabled.

- a Log in to each upgraded node one at a time.
- b Run the following command:

```
rabbitmqctl cluster_status
```

The command should return status similar to the following for each node:

```
sva-1:~ # rabbitmqctl cluster_status
Cluster status of node 'rabbitmq@sva-1' ...
[{nodes, [{disc, ['rabbitmq@sva-1']}]},
 {running_nodes, ['rabbitmq@sva-1']},
 {cluster_name, <<"rabbitmq@sva-1.hs.trcint.com">>},
 {partitions, []},
 {alarms, [{'rabbitmq@sva-1', []}]}
```

- 7 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 section includes the following topics:

- [Prerequisites for Online Upgrade](#)
- [Check for the Availability of a VMware Identity Manager Upgrade Online](#)
- [Configure Proxy Server Settings for the VMware Identity Manager Appliance](#)
- [Perform an Online Upgrade](#)

Prerequisites for Online Upgrade

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

- Verify that at least 4 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](#).
- 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](#).

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

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](#).
- 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.

```
vamicli 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 section includes the following topics:

- [Prerequisites for Offline Upgrade](#)
- [Prepare a Local Web Server for Offline Upgrade](#)
- [Configure the Appliance and Perform Offline Upgrade](#)

Prerequisites for Offline Upgrade

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

- Verify that at least 4 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 for upgrades.
- Prepare a local Web server to host the upgrade file. See [Prepare a Local Web Server for Offline Upgrade](#).

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-3.0.x.x-buildNumber-updaterepo.zip` file. Go to 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/updateLocal.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.](#)

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/updatelocal.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/updatelocal.hzn setdefault
```

- 3 Perform the upgrade.

- a Run the following `updatemgr.hzn` command.

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

- b Run the following command.

```
/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`.

- c Run the `updatemgr.hzn check` command again to verify that a newer update does not exist.

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

Settings to Configure after Upgrade

4

After you upgrade to VMware Identity Manager 3.0, configure these settings.

- If you integrate Citrix published resources with VMware Identity Manager, upgrade to Integration Broker 3.0. VMware Identity Manager 3.0 and VMware Identity Manager Connector 2017.8.1.0 (the connector version in the 3.0 release) are not compatible with older versions of the Integration Broker.

Table 4-1. Supported Versions

VMware Identity Manager or Connector Version	Integration Broker Version Supported
VMware Identity Manager 3.0	3.0
VMware Identity Manager Connector 2017.8.1.0 (Connector version in the VMware Identity Manager 3.0 release)	3.0
VMware Identity Manager 2.9.1 or earlier	2.9.1 or earlier
VMware Identity Manager Connector 2.9.1 or earlier	2.9.1 or earlier

- If you integrate Horizon desktops and applications in VMware Identity Manager and you have deployed a VMware Identity Manager cluster, you must configure Horizon integration again.
 - In the primary connector, where you saved and synced Horizon resources, remove all the Horizon pods, add them again, and click **Save and Sync**.
 - In the other connectors, where you saved the Horizon resources configuration, remove all the Horizon pods, add them again, and click **Save**.

Changes in Earlier Releases

- Bulk sync changes in VMware Identity Manager 2.9.1 and later

In earlier versions, bulk sync was processed with 4 threads per CPU through a global configuration parameter in the database named `bulkSyncThreadLimitPerCPU=4`.

Beginning with version 2.9.1, the number of threads for bulk sync processing is not based on CPU. It is an absolute number, which is the same as the number of CPUs on a node by default.

If you sync large numbers of users and groups and you notice that sync is slow after upgrade, you can specify the number of threads by setting the global configuration parameter called `bulkSyncSharedThreadCount`.

Set the thread value in the database using the following REST API, then restart the nodes for the change to take effect.

HTTP Request:

```
Operation: PUT
URI: bulkSyncSharedThreadCount
```

HTTP Headers:

```
Content-Type: application/vnd.vmware.horizon.manager.systemconfigparameter+json
Accept: application/vnd.vmware.horizon.manager.systemconfigparameter+json
Authorization: HZN <operator token>
```

Request Body (with 8 threads as an example):

```
{
  "name": "bulkSyncSharedThreadCount",
  "values": {
    "values": [
      "8"
    ]
  }
}
```

- 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 have set up a VMware Identity Manager cluster for failover with two nodes, updating it to three nodes is recommended. This is because of a limitation of Elasticsearch, a search and analytics engine embedded in the VMware Identity Manager appliance. You may continue to use two nodes but you should be aware of a few limitations related to Elasticsearch. See "Configuring Failure and Redundancy" in *Installing and Configuring VMware Identity Manager* for more information.
- Transport Layer Security (TLS) protocol 1.0 is disabled by default in VMware Identity Manager. TLS 1.1 and 1.2 are supported.

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 these products have a dependence on TLS 1.0, you can enable TLS 1.0 in VMware Identity Manager 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 section includes the following topics:

- [Checking the Upgrade Error Logs](#)
- [Rolling Back to Snapshots of VMware Identity Manager](#)
- [Collecting a Log File Bundle](#)

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.