VMWARE IDENTITY MANAGER ON-PREMISES DEPLOYMENT CONSIDERATIONS

VMware Identity Manager 2.6
Table of Contents

Introduction .................................................................................................................. 4
  Audience .................................................................................................................. 4
  What Is VMware Identity Manager? ........................................................................... 4
  Architectural Overview ............................................................................................ 5

Deploying VMware Identity Manager ....................................................................... 6
  VMware Identity Manager Virtual Appliance Requirements .................................. 6
  Infrastructure Requirements ..................................................................................... 6
  Network Configuration Requirements ....................................................................... 6
  Firewall Rules and Port Requirements ..................................................................... 7
  VMware vSphere ....................................................................................................... 8
  NTP ............................................................................................................................ 8
  Database ................................................................................................................... 8
  Active Directory ....................................................................................................... 9
  Supported Web Browsers for the Administration Console ....................................... 9
  Supported Browsers for the My Apps Portal ............................................................ 9
  Deploying VMware Identity Manager for High Availability .................................... 10

Installation and Setup ................................................................................................. 12
  Pre-Installation Considerations ............................................................................... 12
    Configure Network ................................................................................................ 12
    Reverse Lookup and IP Addresses ....................................................................... 13
    Database ................................................................................................................ 13
  Installation ............................................................................................................... 14
    Deploy OVA from vCenter ..................................................................................... 14
    Initial Virtual Appliance Settings .......................................................................... 14
    Initial Service Provider Server Settings ............................................................... 14
    Active Directory Configuration .............................................................................. 14
  Post-Installation Configurations .............................................................................. 15
    Set FQDN in VMware Identity Manager ................................................................ 15
    Apply Valid SSL Certificate .................................................................................. 16
    Final Configuration Items ...................................................................................... 16
    Applying the License Key ....................................................................................... 16
  Advanced Configuration ............................................................................................ 16
    Using a Load Balancer ......................................................................................... 16
    Designing for Redundancy ...................................................................................... 17
# VMWare Identity Manager On-Premises Deployment Considerations

## Common Security Standards
- SAML and OAuth ......................................................... 18
- OAuth2 ........................................................................ 19
- OpenID Connect ....................................................... 19
- Kerberos .................................................................... 19
- SSL .............................................................................. 19

## Configurable Authentication Adapters
- Kerberos .................................................................... 20
- Password ..................................................................... 20
- RSA Adaptive Authentication ..................................... 20
- RSA SecurID .................................................................. 20
- Certificate .................................................................... 21
  - Built-In Certificate .................................................. 21
  - Built-In Kerberos ..................................................... 21
- AirWatch Cloud Connector (ACC) Password ............... 22
  - Device Compliance ................................................ 22
- RADIUS ........................................................................ 22
- Authentication Chaining ............................................. 23
- Third-Party IdP Support .............................................. 23

## Integrations
- View in Horizon 7 ..................................................... 24
- ThinApp ....................................................................... 25
- SaaS and Other Applications ..................................... 26
- Citrix XenApp ............................................................. 26

## Monitoring, Troubleshooting, and Reporting
- System Diagnostics Dashboard .................................. 28
- User Engagement Dashboard .................................... 28
- Built-In Reports ......................................................... 29
- Syslog Settings .......................................................... 29
- SNMP v2 Support ...................................................... 29
- Log Collections ......................................................... 29

## Common Issues and Tips

## References

## About This Paper

---

VMware
Introduction
This paper describes general considerations and best practices for planning an on-premises VMware Identity Manager™ deployment, including sizing, design, and gathering of critical environment data. However, because every environment is unique, each deployment of VMware Identity Manager is unique as well. VMware recommends that you consult the VMware Professional Services Organization (PSO) or one of our certified partners for assistance in designing an implementation that meets your specific requirements. VMware Identity Manager is compatible with View in Horizon 7 and Horizon 6 as well as with other earlier releases. For details, see the VMware Product Interoperability Matrix.

Note: To find VMware Identity Manager product documentation referred to in this paper, go to VMware Identity Manager Documentation and, from the drop-down menu, select the version of on-premises software that you are using. Then scroll down to select the specified document.

For detailed information on installing an on-premises implementation, see Installing and Configuring VMware Identity Manager.

For detailed information on integrating with third-party platforms, see VMware Identity Manager Integrations Documentation.

Audience
This paper is intended for IT professionals, such as administrators, managers, and design architects, who are considering an implementation of VMware Identity Manager. The reader should be familiar with identity management, single sign-on (SSO), and basic networking concepts.

What Is VMware Identity Manager?
VMware Identity Manager is an authentication and application access portal that provides a single point of application provisioning and entitlement for enterprise desktop and mobile users. Although this paper describes on-premises deployment, VMware Identity Manager is also offered for Software as a Service (SaaS) deployment.

With VMware Identity Manager, you can

• Deliver an easy-to-use SSO authentication experience to end users.
• Offer end users a self-service catalog of applications and desktops that they have permission to use.
• Provide a single administrative point of control for application provisioning and de-provisioning across desktop and mobile platforms.
• Provide a consistent administration and delivery mechanism, whether on premises or in a SaaS environment, for in-house packaged applications and third-party-vendor solutions that are compliant with the Security Assertion Markup Language (SAML).
• Provide a consistent application access and delivery experience for users, whether accessed on-premises or through a shared cloud, on any supported endpoint device.
Architectural Overview

You can use VMware Identity Manager for both on-premises and SaaS implementations. This paper covers the architectural components of an on-premises implementation. For details on the SaaS implementation, see the VMware Identity Manager documentation.

In an on-premises VMware Identity Manager implementation, the only VMware Identity Manager component is the virtual appliance (VA), which includes the connector. You can download the virtual appliance as an Open Virtual Appliance (OVA) and deploy it through VMware vCenter™.
Deploying VMware Identity Manager

Deploying the VMware Identity Manager OVA can be straightforward if all the requirements listed below are met. For detailed instructions on deploying VMware Identity Manager, see Installing and Configuring VMware Identity Manager.

**Note:** For information on upgrades, see Upgrading to VMware Identity Manager 2.6 from 2.4.

**VMware Identity Manager Virtual Appliance Requirements**

Make sure that the resources allocated to the virtual appliance meet the following minimum requirements.

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>MINIMUM REQUIREMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>2</td>
</tr>
<tr>
<td>RAM</td>
<td>6 GB</td>
</tr>
<tr>
<td>Disk space</td>
<td>36 GB</td>
</tr>
<tr>
<td>Database</td>
<td>You can use the PostgreSQL database that is included in the VMware Identity Manager virtual appliance, or you can use an external database server. For information about specific database versions and service pack configurations supported with VMware Identity Manager, see the VMware Product Interoperability Matrixes.</td>
</tr>
</tbody>
</table>
| Database sizing | 64 GB for first 100,000 users  
20 GB for each additional 10,000 users |
| Storage   | 32 GB                |

**Table 1:** Minimum Requirements for the VMware Identity Manager Virtual Appliance

**Infrastructure Requirements**

The following sections describe the various categories of infrastructure requirements for a VMware Identity Manager deployment.

**Network Configuration Requirements**

The requirements for network configuration are summarized in Table 2.

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>MINIMUM REQUIREMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS record and IP address</td>
<td>IP address and DNS Forward (A) and Reverse (PTR) records.</td>
</tr>
<tr>
<td>Firewall port</td>
<td>Make sure the inbound firewall port 443 is open so that users outside the network can connect to the VMware Identity Manager instance or the load balancer.</td>
</tr>
</tbody>
</table>

**Table 2:** Network Configuration Requirements
Firewall Rules and Port Requirements

If there are firewalls between the VMware Identity Manager appliance and critical resources such as AD domain controllers, DNS servers, or vCenter, make sure the correct ports are opened. The ports are listed in Table 3.

A given deployment might include only a subset of these ports, for instance:

- To sync users and groups, VMware Identity Manager must connect to Active Directory.
- To sync with VMware ThinApp®, VMware Identity Manager must join the Active Directory (AD) domain and connect to the ThinApp repository share.

<table>
<thead>
<tr>
<th>PORT</th>
<th>SOURCE</th>
<th>TARGET</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>Load balancer</td>
<td>VMware Identity Manager VA</td>
<td>HTTPS</td>
</tr>
<tr>
<td>443</td>
<td>VMware Identity Manager VA</td>
<td>VMware Identity Manager VA</td>
<td>HTTPS</td>
</tr>
<tr>
<td>443</td>
<td>Browsers</td>
<td>VMware Identity Manager VA</td>
<td>HTTPS</td>
</tr>
<tr>
<td>443</td>
<td>VMware Identity Manager VA</td>
<td>vapp-updates.vmware.com</td>
<td>Access to the upgrade server</td>
</tr>
<tr>
<td>8443</td>
<td>Browsers</td>
<td>VMware Identity Manager VA</td>
<td>Administrator port HTTPS</td>
</tr>
<tr>
<td>25</td>
<td>VMware Identity Manager VA</td>
<td>SMTP</td>
<td>TCP port to relay outbound mail</td>
</tr>
<tr>
<td>389</td>
<td>VMware Identity Manager VA</td>
<td>Active Directory</td>
<td>Default values are shown. These ports are configurable.</td>
</tr>
<tr>
<td>636</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3268</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3269</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>445</td>
<td>VMware Identity Manager VA</td>
<td>VMware ThinApp repository</td>
<td>Access to ThinApp repository</td>
</tr>
<tr>
<td>5500</td>
<td>VMware Identity Manager VA</td>
<td>RSA SecurID system</td>
<td>Default value is shown. This port is configurable.</td>
</tr>
<tr>
<td>53</td>
<td>VMware Identity Manager VA</td>
<td>DNS server</td>
<td>TCP/UDP Every VA must have access to the DNS server on port 53 and allow incoming SSH traffic on port 22.</td>
</tr>
<tr>
<td>88</td>
<td>VMware Identity Manager VA</td>
<td>Domain controller</td>
<td>TCP/UDP AD domain authentication traffic from VMware Identity Manager to AD</td>
</tr>
<tr>
<td>464</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>135</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>88</td>
<td>External mobile devices</td>
<td>Level 4 load balancer in front of VMware Identity Manager appliance or VMware Identity Manager appliance</td>
<td>TCP (UDP optional) Cloud KDC Kerberos authentication from mobile devices to VMware Identity Manager</td>
</tr>
</tbody>
</table>

Every VA must have access to the DNS server on port 53 and allow incoming SSH traffic on port 22.
<table>
<thead>
<tr>
<th>PORT</th>
<th>SOURCE</th>
<th>TARGET</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP: 9300-9400</td>
<td>VMware Identity Manager VA</td>
<td>VMware Identity Manager VA</td>
<td>Audit needs</td>
</tr>
<tr>
<td>UDP: 54328</td>
<td>VMware Identity Manager VA</td>
<td>VMware Identity Manager VA</td>
<td>PostgreSQL default port: 5432 Oracle default port: 1521</td>
</tr>
<tr>
<td>5432</td>
<td>VMware Identity Manager VA</td>
<td>Database</td>
<td>Access to View Connection Server</td>
</tr>
<tr>
<td>389 443</td>
<td>VMware Identity Manager VA</td>
<td>View Connection Server</td>
<td>Access to View Connection Server</td>
</tr>
</tbody>
</table>

Table 3: VMware Identity Manager Port Requirements

**VMware vSphere**

Make sure that you are using the correct version of VMware vSphere® and a supporting vCenter.

The following versions of vSphere and VMware ESXi™ server are supported:

- 5.0 U2 and later
- 5.1 and later
- 5.5 and later
- 6.0 and later

**NTP**

The Network Time Protocol (NTP) must be correctly configured on all hosts and time-synchronized to an NTP server. You must turn on time sync at the ESXi host level, using an NTP server to prevent a time drift between virtual appliances. If you deploy multiple virtual appliances on different hosts, consider disabling the Sync to Host option for time synchronization. Instead, configure the NTP server in each virtual appliance directly to make sure that there is no time drift between virtual appliances.

**Database**

VMware Identity Manager can be set up with an internal or external database to store and organize server data. You can use the PostgreSQL database that is embedded in the VMware Identity Manager VA, or you can set up an external database. The internal database is the default.

The embedded PostgreSQL database configuration is useful for small deployments. It does not require any additional configuration outside VMware Identity Manager, but it is recommended that you configure your internal database for high availability. See the VMware Knowledge Base article, Using embedded vPostgres in production for VMware Workspace Portal VA 2.1 (and VMware Identity Manager 2.4) (2094258).

To use an external database, have your database administrator prepare an empty external database and schema before you use the VMware Identity Manager Setup wizard to connect to the external database. Licensed users can use an external Microsoft SQL 2014 database server, an Oracle database server, or an external PostgreSQL database server to set up a high-availability external database environment. See Connecting to the Database in Installing and Configuring VMware Identity Manager.
Active Directory
VMware Identity Manager supports AD configurations on Windows 2008, 2008 R2, 2012, and 2012 R2, including
• Single AD domain
• Multi-domain, single forest
• Multi-forest with trust relationships
• Multi-forest with untrusted relationships (requires external connector configuration)
• Optional AD Global Catalog for Directory Sync
A connector is needed only when there is no two-way trust.

Supported Web Browsers for the Administration Console
The VMware Identity Manager administration console is a Web-based application you use to manage your VMware Identity Manager environment. You can access the administration console from the following browsers:
• Internet Explorer 10 and 11 for Windows systems
• Google Chrome 42.0 and later for Windows and Mac systems
• Mozilla Firefox 40 and later for Windows and Mac systems
• Safari 6.2.8 and later for Mac systems
These browsers can also be used to access the Connector Services and Appliance Configurator pages.

Supported Browsers for the My Apps Portal
End users can access their My Apps portal from the following browsers:
• Mozilla Firefox
• Google Chrome
• Safari
• Internet Explorer 10 and later
• Microsoft Edge browser
• Native browser and Google Chrome on Android devices
• Safari on iOS devices
Deploying VMware Identity Manager for High Availability

Deploy VMware Identity Manager to secondary data centers for active / hot-standby connectivity in read-only mode. This arrangement allows a secondary data center to be powered on and active with read-only access to eliminate downtime during failover. The read-only capability allows end users to view and launch their applications from the secondary data center while the primary data center is down.

*Figure 2: HA Configuration*
In a read-only configuration, administrators cannot modify anything until either the slave database is promoted to be the master database, or the original master database is brought back online.

Implementing a high-availability configuration depends on the database that you are using. If you are using the internal PostgreSQL database, the primary virtual appliance is set up and configured first, then it is cloned to the local data center and exported or imported (if necessary) for use in remote data centers. See the VMware Knowledge Base article, Using embedded vPostgres in production for VMware Workspace Portal VA 2.1 (and VMware Identity Manager 2.4) (2094258) for details.

For more information on how to set up VMware Identity Manager in a high-availability configuration, see Advanced Configuration for the VMware Identity Manager Appliance in Installing and Configuring VMware Identity Manager.

If you are using an external Microsoft SQL database, the following additional configuration items are required:

- Use the same security ID (SID) to create the VMware Horizon® 7 login on any secondary nodes, to maintain continuity of user login association when there is a failover event. See the Microsoft knowledge base article, How to transfer logins and passwords between instances of SQL Server (918992) for details on exporting login information. The preferred method is to use the sp_help_revlogin script.
- Use the Full Recovery option on the secondary node(s) to fully initialize them based on the BAK file from the primary.
- Point all VMware Identity Manager VA Java Database Connectivity (JDBC) connection strings to the Active GridLink (AGL). Do not point them directly to a node.

In addition, the following changes are recommended:

- Add multiSubnetFailover=true as part of the JDBC connection string.
- Change HostRecordTTL to a lower value than the default, such as 120 seconds, in multi-site deployments.
- Change RegisterAllProvidersIP to false in multi-site deployments.
Installation and Setup
There are three main steps involved with setting up VMware Identity Manager:

1. Complete all network configuration prerequisites, including NTP time sync.
2. Deploy and configure an external database (optional but recommended).
3. Deploy the VMware Identity Manager OVA.

**Important:** It is critical to have a properly configured network, with Active Directory available and NTP configured, before the VMware Identity Manager OVA is deployed.

Pre-Installation Considerations
The VMware Identity Manager OVA appliance is a single virtual machine that is configured to run all the VMware Identity Manager services shown in Figure 3.

---

**Figure 3: VMware Identity Manager Services**

**Configure Network**
The VMware Identity Manager VA requires a DNS entry and a static IP address. Because each organization administers its IP addresses and DNS records differently, request the DNS record and IP addresses before you begin your installation.
Reverse Lookup and IP Addresses

Reverse lookup configuration is required. When you implement reverse lookup, you must define a PTR record on the DNS server so the virtual appliance uses the correct network configuration.

You can use the following sample DNS records when you talk to your network administrator. Replace the sample information with information from your environment. This example shows forward DNS records and IP addresses.

<table>
<thead>
<tr>
<th>DOMAIN NAME</th>
<th>RESOURCE TYPE</th>
<th>IP ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>my-identitymanager.company.com</td>
<td>A</td>
<td>10.28.128.3</td>
</tr>
</tbody>
</table>

The next example shows reverse DNS records and IP addresses:

<table>
<thead>
<tr>
<th>DOMAIN NAME</th>
<th>RESOURCE TYPE</th>
<th>IP ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>128.28.10.in-addr.arpa.</td>
<td>PTR</td>
<td>PTR my-identitymanager.company.com</td>
</tr>
</tbody>
</table>

After you complete the DNS configuration, verify that the reverse DNS lookup is properly configured. For example, the VA command host IP address must resolve to the DNS name lookup.

If you are using a UNIX- or Linux-based DNS server and plan to join VMware Identity Manager to the AD domain, make sure that the appropriate service (SRV) resource records are created for each AD domain controller.

Database

There are multiple options for configuring the VMware Identity Manager database.

- For a smaller deployment or a proof of concept, it is easier to use the internal database. For true backup, load balancing, and high availability, use an external database.
- For large, production-level deployments, it is possible to use the internal database with replication configured; however, an external database is recommended for true backup, load balancing, and high availability. See Deploying VMware Identity Manager for High Availability for details.
- For guidance on setting up and configuring failover and migration for a PostgreSQL database implementation, see the VMware Technology Network article, Horizon Workspace - External vFabric Postgres database.
- For a full list of database versions that are supported, see the VMware Product Interoperability Matrixes.
Installation
The major steps for on-premises installation of VMware Identity Manager are illustrated in Figure 4 and described in the following sections.

Figure 4: VMware Identity Manager Installation Steps

Deploy OVA from vCenter
For instructions on deploying the OVA, see Install the VMware Identity Manager OVA File in Installing and Configuring VMware Identity Manager.

Initial Virtual Appliance Settings
After deploying and powering on the virtual appliance, set all the necessary appliance passwords, including the passwords for the admin user, root user, and sshuser.

For detailed setup information, see Configure VMware Identity Manager Settings and Manage Your Appliance Passwords in Installing and Configuring VMware Identity Manager.

Initial Service Provider Server Settings
After completing the initial connector settings, specify the initial service settings, such as license information, user attributes, and an SMTP server for internal message routing. See Managing Appliance System Configuration Settings in Installing and Configuring VMware Identity Manager.

Active Directory Configuration
AD configurations include defining the directory connection type (LDAP or Integrated Windows login) and the Bind information as well as specifying which users and groups to synchronize before conducting the initial directory sync.

The concepts described in the following sections are essential for a good understanding of how the VMware Identity Manager service integrates with an AD environment.

Connector Service
The connector, a component of the VMware Identity Manager virtual appliance, syncs user and group data between AD and the service. When used as an identity provider, it authenticates users to the service.

The connector is the default identity provider. You can also use third-party identity providers that support the SAML 2.0 protocol for authentication types not supported by the connector or if the third-party identity provider is preferable based on your enterprise security policy.
Directory
The VMware Identity Manager service has its own concept of the directory that synchronizes to AD. This directory uses Active Directory attributes and parameters to define users and groups. You create one or more directories and then sync those directories with your AD deployment. You can create the following directory types in the service:

- **AD over LDAP** – Create this directory type for simple connectivity to AD single or multi-forest domain structures that do not require Integrated Windows Authentication (IWA) with Windows Challenge/Response (NTLM) and Kerberos.
- **AD, Integrated Windows Authentication** – Create this directory for connectivity to complex or legacy AD domains, whether single-forest or multi-forest, that require IWA to support authentication types such as NTLM and Kerberos on the same connector. The connector binds to Active Directory using IWA.

The type and number of directories that you create can vary depending, for instance, on whether your AD environment is single-domain or multi-domain and on the type of trust used between domains. In most environments, you create one directory.

For further information on Active Directory structural elements, see the Microsoft knowledge base article, *What Are Domains and Forests?*

User Attributes
You must complete the definition of user attributes before configuring a directory in VMware Identity Manager. See *Select Attributes to Sync with Directory* in *VMware Identity Manager Administration*.

Worker
When you associate a directory with a connector instance, the connector creates a partition for the associated directory called a worker. A connector instance can be associated with multiple workers, each of which acts as an identity provider. You can define and configure authentication methods for each worker.

The connector syncs user and group data between AD and the service through one or more workers. You cannot have two workers of the IWA type on the same connector instance, otherwise identity data can become corrupted.

For more details on the proper configuration and preparation of Active Directory for VMware Identity Manager, see *Integrating with Active Directory* in *Installing and Configuring VMware Identity Manager*.

Post-Installation Configurations
After installation is complete, there are still several configurations to be completed.

**Set FQDN in VMware Identity Manager**
Define the fully qualified domain name (FQDN) if load balancers are used, and complete the following items:

- Set the Secure Sockets Layer (SSL) certificate information.
- Configure any load balancer settings (optional).
- Set syslog information (optional).
Apply Valid SSL Certificate
When the VMware Identity Manager VA is installed, a default SSL server certificate is generated automatically. You can use this self-signed certificate for general testing of your implementation in nonproduction environments; however, VMware strongly recommends that you generate and install commercial SSL certificates in your production environment.

A certificate authority (CA) is a trusted entity that guarantees the identity of the certificate and its creator. When a certificate is signed by a trusted CA, users no longer receive messages asking them to verify the certificate.

If you deploy VMware Identity Manager with the self-signed SSL certificate, the root CA certificate must be available as a trusted CA for any client that accesses the VMware Identity Manager.

Final Configuration Items
The final configuration items include joining the AD domain, defining network ranges, enabling and configuring any additional AUTH Adapters, and applying custom branding options, if desired.

For detailed instructions, see
- Join Active Directory Domain in Setting Up Resources in VMware Identity Manager
- Configuring User Authentication in VMware Identity Manager in VMware Identity Manager Administration
- Customize Branding in VMware Identity Manager Administration

Applying the License Key
After you deploy the VMware Identity Manager appliance, enter your license key.

1. Log in to the VMware Identity Manager administration console.
2. Click the Appliance Settings tab, then click License.
3. On the License Settings page, enter the license key and click Save.

Advanced Configuration
After you complete the basic VMware Identity Manager VA installation, you might need to complete other configuration tasks, such as enabling external access to the VMware Identity Manager, and configuring redundancy.

Using a Load Balancer
During deployment, the VMware Identity Manager VA is set up inside the internal network. If you want to provide access to the service for users connecting from outside networks, you must install a load balancer, such as Apache, NGINX, or F5, in the demilitarized zone (DMZ).

If you do not use a load balancer, you cannot expand the number of VMware Identity Manager appliances later. You might need to add more appliances to provide redundancy as well as load balancing.
Designing for Redundancy
You can set up the VMware Identity Manager VA for failover and redundancy by adding multiple VMware Identity Manager VAs in a cluster, so that if one VA becomes unavailable for any reason, VMware Identity Manager remains available.

To set up failover, install and configure the VMware Identity Manager VA, then clone it. Cloning the VA creates a duplicate of the appliance with the same configuration as the original. You can customize the cloned VA to change the name, network settings, and other properties as required.

Before you clone the VMware Identity Manager VA, you must configure it behind a load balancer and change its FQDN to match the load balancer’s FQDN. You must also complete directory configuration in the VMware Identity Manager service before you clone the appliance.

After cloning, you assign a new IP address to the cloned VA before powering it on. The cloned VA’s IP address must follow the same guidelines as the IP address of the original VA. The IP address must resolve to a valid host name using forward and reverse DNS.

All nodes in the VMware Identity Manager cluster are nearly identical copies of each other. Syncing to AD and to resources that are configured, such as Horizon 7 or ThinApp, is disabled on the cloned VAs.

For more information on this topic, see Configuring Redundancy in Installing and Configuring VMware Identity Manager. See Figure 2 for a visual representation.

Note: If you are upgrading from an earlier version of VMware Identity Manager or VMware Workspace™ Portal, you can use the load balancer information that you already have in place.
Common Security Standards

To work with VMware Identity Manager, it is important to understand the basic security standards and concepts summarized in the following sections.

SAML and OAuth

Security Assertion Markup Language (SAML) is an open standard. When used for SSO, it enables a user to log in to one system in an environment and then access other systems in that environment without needing to log in again until the Web browser session is ended.

VMware Identity Manager utilizes the SAML and Open Authorization (OAuth) industry standards for SSO. These are trusted, secure ticketing methods embraced by the IT Industry for secure authentication and authorization of end users from any device.

For instance, SAML Web Browser SSO involves three entities: an identity provider (IdP), a service provider (SP), and a principal (usually an end user). The identity provider maintains a directory of users and an authentication mechanism to authenticate them. The service provider is the target application that a user tries to use. The principal must be registered in the IdP.

The authentication sequence is illustrated in Figure 5.

![Authentication Overview Diagram]

**Figure 5: Authentication Overview**

1. An end user accesses the service provider with a SAML-secured application.
2. The service provider sends a request to a preregistered identity provider for authentication.
3. If the end user is not authenticated yet, the identity provider interacts with the end user to provide authentication.
4. The identity provider responds to the service provider with a token for that user.
**TERM** | **DEFINITION**
---|---
AuthN | Authentication – Confirms the identity of a person or application
AuthZ | Authorization – Grants the ability to access without requiring the authenticated state to be passed between entities
Service Provider (SP) | Service Provider – Typically the external SaaS application, such as Salesforce, Workday, or Concur
Identity Provider (IdP) | The trusted authority – Provides AuthN for users
Client/user agent | Normally, in VMware Identity Manager, the end-user’s browser acts as the agent

**Table 4: Common SAML Terminology**

**OAuth2**
Open Standard for Authorization version 2.0 defines a framework for securing application access to protected resources through the use of APIs. For more information, see the [OAuth Wikipedia page](#).

**OpenID Connect**
OpenID Connect provides an identity layer on top of OAuth2 that enables verification of end users’ identities. For a fuller description, see [Welcome to OpenID Connect](#).

**Kerberos**
Kerberos authentication provides users who are successfully signed in to their AD domain with access to their application portal without additional credential prompts.

Enabling Windows authentication allows the Kerberos protocol to secure the interactions between users’ browsers and the VMware Identity Manager service. VMware Identity Manager validates user desktop credentials, using Kerberos tickets distributed by the key distribution center (KDC). You do not need to configure AD directly to make Kerberos function with your deployment.

**Note:** Interactions between a user’s browser and the service are authenticated by Kerberos only on the Windows operating systems.

**SSL**
The SSL cryptographic protocol secures TCP traffic between Web servers and Web browsers, operating in Layer 5 (session layer) of the Open Systems Interconnect (OSI) model.
Configurable Authentication Adapters
For detailed instructions on configuring user authentication adapters, see *Configuring User Authentication in VMware Identity Manager* in VMware Identity Manager Administration.

Kerberos
The Kerberos authentication adapter provides domain users with SSO access to their apps portal, eliminating the need for domain users to sign in to their apps portal again after they log in to the enterprise network. VMware Identity Manager validates user desktop credentials using Kerberos tickets distributed by the key distribution center (KDC).

Password
VMware Identity Manager supports AD password authentication. This method authenticates users directly against Active Directory.

RSA Adaptive Authentication
VMware Identity Manager supports RSA Adaptive Authentication. An RSA Adaptive Authentication Connector in VMware Identity Manager, separate from the RSA SecurID Authentication Connector, provides cross-channel protection, including policy management and device and behavior profiling.

There are two ways to synchronize user accounts to an RSA Adaptive Authentication engine: through just-in-time user provisioning, which is the configuration option that VMware Identity Manager supports, or through a third-party means. User accounts are first synchronized from the organization’s AD domain into VMware Identity Manager, then users are provisioned just in time to the RSA Adaptive Authentication system through the RSA SOAP API. Users are self-enrolled into the RSA Adaptive Authentication system through a challenge-response authentication mechanism of the organization’s choosing, such as SMS tokens, email tokens, or secret questions.

For more information, see the RSA Adaptive Authentication page.

RSA SecurID
VMware Identity Manager can be configured to leverage an on-premises RSA SecurID implementation to provide two-factor authentication. This is a separate authentication method from RSA Adaptive Authentication.

To configure an RSA SecurID server, add the VMware Identity Manager service information as the authentication agent on the RSA SecurID server, and configure the RSA SecurID server information on the VMware Identity Manager service.

Make sure that your network is properly configured for your VMware Identity Manager deployment, specifically, make sure that the appropriate port is open to enable SecurID to authenticate users outside your network.

Run the VMware Identity Manager Setup wizard and configure your AD connection to make the necessary information available to prepare the RSA SecurID server. After you prepare the RSA SecurID server for VMware Identity Manager, enable SecurID in the administration console.

For more information, see *Configuring SecurID for VMware Identity Manager* in VMware Identity Manager Administration.
Certificate
The VMware Identity Manager Certificate Authentication Adapter provides additional security and flexibility in authentication and authorization of end users across various endpoints by allowing certificate and smart card authentication methods.

To set up the Certificate Authentication Adapter, open the worker assigned to the connector that is designated to handle certificate authentication. Select the CertificateAuthAdapter to enable, and configure its settings.

You can configure X.509 certificate authentication to allow users to authenticate either with certificates on their desktop and mobile devices or with a smart card adapter. Certificate-based authentication relies on the user’s private key or smart card, and the password to the private key or the smart-card PIN. An X.509 certificate uses the public key infrastructure (PKI) standard to verify that a public key in the certificate belongs to the user.

Certificates must be the first authentication method listed in the policy page when you use certificates for authentication. To use certificates, you need the root certificate and intermediate certificates from the CA that signed the certificates presented by your users. For revocation checking, you also need the file location of the certificate revocation list (CRL) and the URL of the Online Certificate Status Protocol (OCSP) server. You also need consent form content if you plan to enable a consent form to display before authentication. See Using Certificate Revocation Checking in VMware Identity Manager Administration.

A list of object identifiers (OIDs) of valid certificate policies for certificate authentication and an OCSP Response Signing certificate file location are optional.

Built-In Certificate
The difference between built-in certificate authentication and certificate authentication is that built-in certificate authentication applies only to mobile devices enrolled in VMware AirWatch®.

When you use the built-in certificate authentication method, it must be the first authentication method defined in a given policy. This is not the case when you use the certificate authentication method.

To use built-in certificates, you need the root certificate and intermediate certificates from the CA that signed the certificates presented to your users. For revocation checking, you also need the file location of the certificate revocation list (CRL) and the URL of the Online Certificate Status Protocol (OCSP) server. You also need consent form content if you plan to enable a consent form to display before authentication.

Built-In Kerberos
For Kerberos with iOS device authentication, VMware Identity Manager uses an identity provider that is built into the VMware Identity Manager service to access built-in Kerberos. Kerberos uses a Key Distribution Center (KDC) without the use of a connector or a third-party system.

For detailed information on how to implement Kerberos authentication for AirWatch-managed iOS 9 devices, follow the steps in Implementing Built-in Kerberos Authentication for AirWatch-Managed iOS Devices in VMware Identity Manager Administration.
AirWatch Cloud Connector (ACC) Password
You can integrate your VMware AirWatch Cloud Connector™ with the VMware Identity Manager service for user password authentication and management. You can configure the VMware Identity Manager service to sync users from the AirWatch directory instead of deploying a VMware Identity Manager connector.

To implement AirWatch Cloud Connector authentication, see Implementing Authentication with AirWatch Cloud Connector in VMware Identity Manager Administration.

Device Compliance
Device Compliance is a secondary authentication adapter for iOS devices only and requires built-in Kerberos as the primary authentication adapter. For more information, see Enable Compliance Checking for AirWatch Managed iOS Devices in Setting up VMware Workspace ONE App on Devices.

RADIUS
VMware Identity Manager supports the ability to integrate with a Remote Authentication Dial-In Service (RADIUS) system as an authentication method to provide additional two-step verification for authentication of users. Combined with VMware Identity Manager policies, RADIUS is a highly adaptive and secure single-sign-on identity management portal.

RADIUS is used to
• Authenticate users or devices before allowing them access to a network
• Authorize those users or devices for specific network services
• Account for and track the usage of those services

With a RADIUS server on the organization network, use VMware Identity Manager to navigate to the Connectors window in the Setup option of the Identity & Access Management tab, then select the RadiusAuthAdapter, and enable and configure it on the Authentication Adapter screen.

VMware Identity Manager has options for enabling two RADIUS servers for backup and redundancy as well as supporting the Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), Microsoft Challenge-Handshake Authentication Protocol version 1 (MSCHAPv1), and Microsoft Challenge-Handshake Authentication Protocol version 2 (MSCHAPv2) authentication types.

Links to further information on RADIUS are listed in Table 5.

<table>
<thead>
<tr>
<th>PROTOCOL</th>
<th>REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAP</td>
<td><a href="https://en.wikipedia.org/wiki/Password_Authentication_Protocol">https://en.wikipedia.org/wiki/Password_Authentication_Protocol</a></td>
</tr>
</tbody>
</table>

Table 5: Links to Further Information for RADIUS
Authentication Chaining
An authentication chain lets administrators connect authentication options and tie them to selected network locations for enhanced security, so that if one option fails, the authentication falls back to the next option in the chain. For example, you can allow end users to pass through multiple security checks when they access one internal network from another but require additional authentication measures when they try to access corporate assets from an external or public network. These fallback measures are illustrated in Figure 6.

![Authentication Chaining](image)

Figure 6: Authentication Chaining

Third-Party IdP Support
VMware Identity Manager integrates with third-party identity solutions so that you do not need to replace legacy systems. For details, see Configuring User Authentication in VMware Identity Manager in VMware Identity Manager Administration.
Integrations
The following sections provide important information on how to integrate VMware Identity Manager with View in Horizon 7, ThinApp, SaaS, and other applications, including Citrix XenApp.

View in Horizon 7
To deliver View desktops and hosted applications, configure the integration in the administration console of the VMware Identity Manager appliance and the View Connection Server.

- Integration requires SAML 2.0 authentication configuration on the View Connection Servers. (The integration is required on all View Connection Servers in the View pod.)
- The VMware Identity Manager VA must be domain-joined.
- Cloud Pod Architecture is supported along with multiple View pods.

Figure 7 and Figure 8 illustrate how the hosted application and hosted desktop integrations work with VMware Identity Manager.

![Figure 7: Hosted Applications](image-url)
View in Horizon 7 provides two options for syncing the global environments: View API bindings and XML APIs. The View API is designed primarily for managing the View implementation, particularly for adding or querying and editing the environment details such as user information or global entitlements.

Local entitlements are synchronized through direct query of the View Connection Server LDAP. The View APIs are available for syncing global entitlements. If any pod in a federation is configured in VMware Identity Manager, then global entitlements can be synced because they are replicated across the federated pods. Like other entitlements, the synced entitlements are displayed in VMware Identity Manager. For more information, see Integrating View Cloud Pod Architecture (CPA) Deployments in Setting Up Resources in VMware Identity Manager and VMware Identity Manager Integration with Active Directory Federation Services 2.0.

ThinApp
VMware Identity Manager can be leveraged to deliver ThinApp packages to users through the VMware Workspace™ ONE™ Web interface. This feature enhances user experience with nonpersistent View desktops.

Note: HTTP delivery of ThinApp packages no longer needs to be defined as an installation parameter. VMware Identity Manager clients try to use Kerberos login to leverage DFS and CIFS shares as viable delivery mechanisms. If those shares are not viable, the clients use HTTP instead.
SaaS and Other Applications
The VMware Identity Manager Cloud Catalog includes templates for many third-party SaaS providers. VMware has worked with these partners to make their applications easy to implement through VMware Identity Manager by pre-populating some of the information needed for integration.

For detailed instructions on how to configure VMware Identity Manager to work with other SaaS implementations that use SAML, see VMware Identity Manager Integrations Documentation.

Integration recipes are currently available for:

- ADP
- AirWatch applications
- Ariba
- Amazon Web Services
- BambooHR
- Bonusly
- ClearSlide
- Dropbox
- Expensify
- Freshdesk
- Freshservice
- GoogleApps
- MangoApps
- Marketo
- Mingle
- Office 365
- Oominitza
- QuickBase
- RO ReferenceView
- Salesforce
- ServiceNow
- ScreenSteps
- WebEx
- Zendesk
Citrix XenApp

VMware Identity Manager supports Citrix XenApp 5.x and 6.x and Citrix XenDesktop 7.x integration. Applications and desktops provided by these solutions appear in the VMware Identity Manager catalog and launcher for self-provisioning and use by authorized users.

See Providing Access to Citrix-Published Resources in Setting Up Resources in VMware Identity Manager for more detail.

Figure 9: XenApp Applications Published to the Workspace ONE User Interface

VMware Identity Manager supports organizations that have Citrix NetScaler in their existing XenApp Farm environments. This provides additional options for access to applications and delivers them all through a single VMware Identity Manager application portal.

Organizations with existing Citrix XenApp infrastructures secured by Citrix NetScalers can use VMware Identity Manager to access all desktops and applications provided through XenApp 5.x, XenApp 6.x, or XenDesktop 7.x. End users can then open a Web page to access the VMware Identity Manager portal and gain access to all their Citrix XenApp-published applications, which are launched through the locally installed Citrix Receiver. End users still have access to all their SaaS, Web, ThinApp, and other applications and virtual desktops.

When VMware Identity Manager is integrated with a Citrix deployment, administrators can use Citrix administration consoles to manage Citrix-published applications and Citrix-published desktops as well as to entitle users to those resources. These Citrix resources and their entitlements can be viewed from the VMware Identity Manager administration console.

VMware Identity Manager provides default global application-delivery settings for Citrix-published resources, for example, to edit the settings that control resource streaming and resource security. Organizations can configure the delivery settings globally for all the Citrix resources in the VMware Identity Manager catalog or for individual Citrix resources.
Monitoring, Troubleshooting, and Reporting
The VMware Identity Manager administration console includes two dashboards to monitor the health of your VMware Identity Manager implementation and to locate problems. For more information, see Monitor System Information and Health in VMware Identity Manager Administration.

System Diagnostics Dashboard
You can use the System Diagnostics dashboard to monitor the following items:

- Password expiration dates – root and sshuser
- Certificates
- Configurator deployment status
- Application manager deployment status
- Connector deployment status
- VMware Identity Manager FQDN status
- Database connectivity
- Analytics and messaging connectivity

User Engagement Dashboard
The User Engagement dashboard provides information in one page on the usage of applications by users.

Figure 10: User Engagement Dashboard
Built-In Reports
VMware Identity Manager built-in reports, accessible from the administration console dashboards, can be helpful for monitoring the health and use of the system. In these reports you can monitor things like Number of Current Logged In Users, List of Connected Clients, and Types of Resources Launched.

Syslog Settings
To enable syslog for VMware Identity Manager application logs, see Enable the Syslog Server in Installing and Configuring VMware Identity Manager. No OS or hardware messages are logged.

SNMP v2 Support
The SNMP v2 feature is enabled through the VMware Identity Manager CLI. It exposes VMware Identity Manager application-specific MIB files. OS or hardware-specific MIB files are not exposed.

Log Collections
You can collect logs by navigating to https://<connector_fqdn>:8443/cfg/logs and supplying the correct FQDN for your VMware Identity Manager server. Opening this link in a supported browser generates and downloads the support log bundle from VMware Identity Manager.

Application-level events from the service can be exported to an external syslog server. Operating system events are not exported. For details, see Enable the Syslog Server in Installing and Configuring VMware Identity Manager and Collecting a Log File Bundle in Upgrading VMware Identity Manager Connector.

---

Figure 11: Log File Locations

You can also initiate a Log File Bundle from the CLI with the following command:

<hostname>:- # /usr/local/horizon/scripts/gatherLogs.hzn
Common Issues and Tips
Table 6 summarizes information about issues that you can resolve.

<table>
<thead>
<tr>
<th>ISSUE</th>
<th>TIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Pre-Configurations Not Completed</td>
<td>Before deploying the VMware Identity Manager VA, complete the networking pre-configurations, especially Forward and Reverse lookup (A and PTR) records and Static IP configurations. DHCP and IPv6 are not supported in VMware Identity Manager.</td>
</tr>
<tr>
<td>Outbound Proxy Exists on Network</td>
<td>Activation of VMware Identity Manager accounts can fail if there is an outbound proxy on the network. For more information, see Configure Proxy Server Settings for the VMware Identity Manager Connector Appliance in Upgrading VMware Identity Manager Connector.</td>
</tr>
<tr>
<td>Accidental Admin Removal</td>
<td>If a domain administrator account is not initially synchronized to VMware Identity Manager, you cannot log in to VMware Identity Manager as a domain administrator. To mitigate this condition, use the local admin account on the VMware Identity Manager VA to resolve the issue, either by promoting another domain user to the VMware Identity Manager Administrator role or by modifying the directory sync configurations to include an AD domain administrator.</td>
</tr>
<tr>
<td>Third-Party Applications Fail to Launch</td>
<td>If third-party applications fail to launch or do not launch correctly, check the Application Parameters and Attribute Mapping sections of the SaaS or Web application to make sure they are configured properly. Other conditions that can prevent applications from launching include certificate trust issues, an application’s inability to support provisioning, or a user account that does not exist in the third-party application. If any of these problems occur, verify that all application configuration parameters are specified correctly.</td>
</tr>
<tr>
<td>SSO from VMware Identity Manager to Hosted Applications or Desktops Fails</td>
<td>SSO to Horizon apps or View desktops can fail if certificate trust is not established or if SSO is not enabled in View. If users see SAML authentication errors, then NTP is not properly set between VMware Identity Manager, View Connection Servers, domain controllers, and ESXi hosts that are running the VMware Identity Manager VAs.</td>
</tr>
<tr>
<td>Applications or Desktops Not Available</td>
<td>If users cannot see their applications or desktops, then the user is either not authorized to use the application, or the application needs manual activation. In the case of View, if the user is authorized, but the application does not appear, then the administrator might need to perform a manual directory sync or have the user wait for the automated sync to occur, if automatic sync has been configured.</td>
</tr>
<tr>
<td>AD Login Fails</td>
<td>If the AD login fails, go to <a href="https://fqdn/SAAS/login/0">https://fqdn/SAAS/login/0</a>. For login credentials, use admin as the username, and the password that was set during the initial appliance installation.</td>
</tr>
</tbody>
</table>
References

Blog posts about VMware Identity Manager

Microsoft knowledge base article, What Are Domains and Forests?

VMware Identity Manager Documentation

VMware Identity Manager Integrations Documentation

VMware Knowledge Base article, How to transfer logins and passwords between instances of SQL Server (918992)

VMware Knowledge Base article, Using embedded vPostgres in Production for VMware Workspace Portal VA 2.1 (and VMware Identity Manager 2.4) (2094258)

VMware Technology Network article, Horizon Workspace - External vFabric Postgres database

About This Paper

The material in this paper was gathered, expanded, and modified by the Technical-Marketing Center of Excellence team, including the following individuals:

• Rick Terlep, End-User-Computing Architect, Technical Marketing, End-User Computing, VMware
• Dean Flaming, End-User-Computing Architect, Technical Marketing, End-User Computing, VMware
• Kevin Sheehan, End-User-Computing Architect, Technical Marketing, End-User Computing, VMware
• Chris White, End-User-Computing Architect, Technical Marketing, End-User Computing, VMware

To comment on this paper, contact the VMware End-User-Computing Technical-Marketing Center of Excellence team at euc_tech_content_feedback@vmware.com.