Installing and Configuring the Connector

Horizon Connector 1.5.0

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-000875-00

vmware®

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

Installing and Configuring the Connector

Draft comment filepath: GUID-ABA8925D-4AA7-4D09-B97F-B65D4546E3CE.xml

This information describes how to install, configure, and maintain the Connector. The Connector software is the interface between Application Manager and your Microsoft Active Directory server. The Connector can also provide users access to Windows applications captured as VMware ThinApp packages.

Intended Audience

Draft comment filepath: GUID-ABA8925D-4AA7-4D09-B97F-B65D4546E3CE.xml

This information is intended for organization administrators. The information is written for experienced Windows and Linux system administrators who are familiar with VMware virtual machine technology, identity management, entitlement, and directory services. SUSE Linux is the underlying operating system for the Connector virtual appliance. Knowledge of Linux is essential to configure the Connector directly and to perform system-level functions, such as configuring network settings, time settings, and log files. Knowledge of other technologies, such as VMware ThinApp and RSA SecurID, is helpful if you plan to implement those features.

The Connector Installation and Configuration Overview

Draft comment filepath: GUID-ABA8925D-4AA7-4D09-B97F-B65D4546E3CE.xml

Before you can install the Connector, an operator creates your account and provides you with the authentication code. If you are using Application Manager as an on-premise appliance, you or someone else in your enterprise is fulfilling the operator role. If you are using Application Manager as a hosted service, someone outside your enterprise is fulfilling the operator role. Regardless of the Application Manager version, you must obtain the Connector virtual appliance in order to install and configure the Connector. The process involves a variety of tasks and you can deploy Application Manager in several different ways. A key distinction in deployments is in the mode of authentication you choose. See Chapter 1, "Introduction to Application Manager," on page 9. An important deployment factor depends on if you choose to provide users with access to Windows applications captured as ThinApp packages. The flowcharts that follow illustrate two Application Manager deployments at different levels of specificity. Together, the flowcharts provide a sense of the variety involved in deploying Application Manager.

- Figure 1: The installation and configuration flow of a generalized deployment of the Connector
- Figure 2: The installation and configuration flow of a deployment of the Connector integrated with ThinApp

Installation and Configuration Flow of the Connector

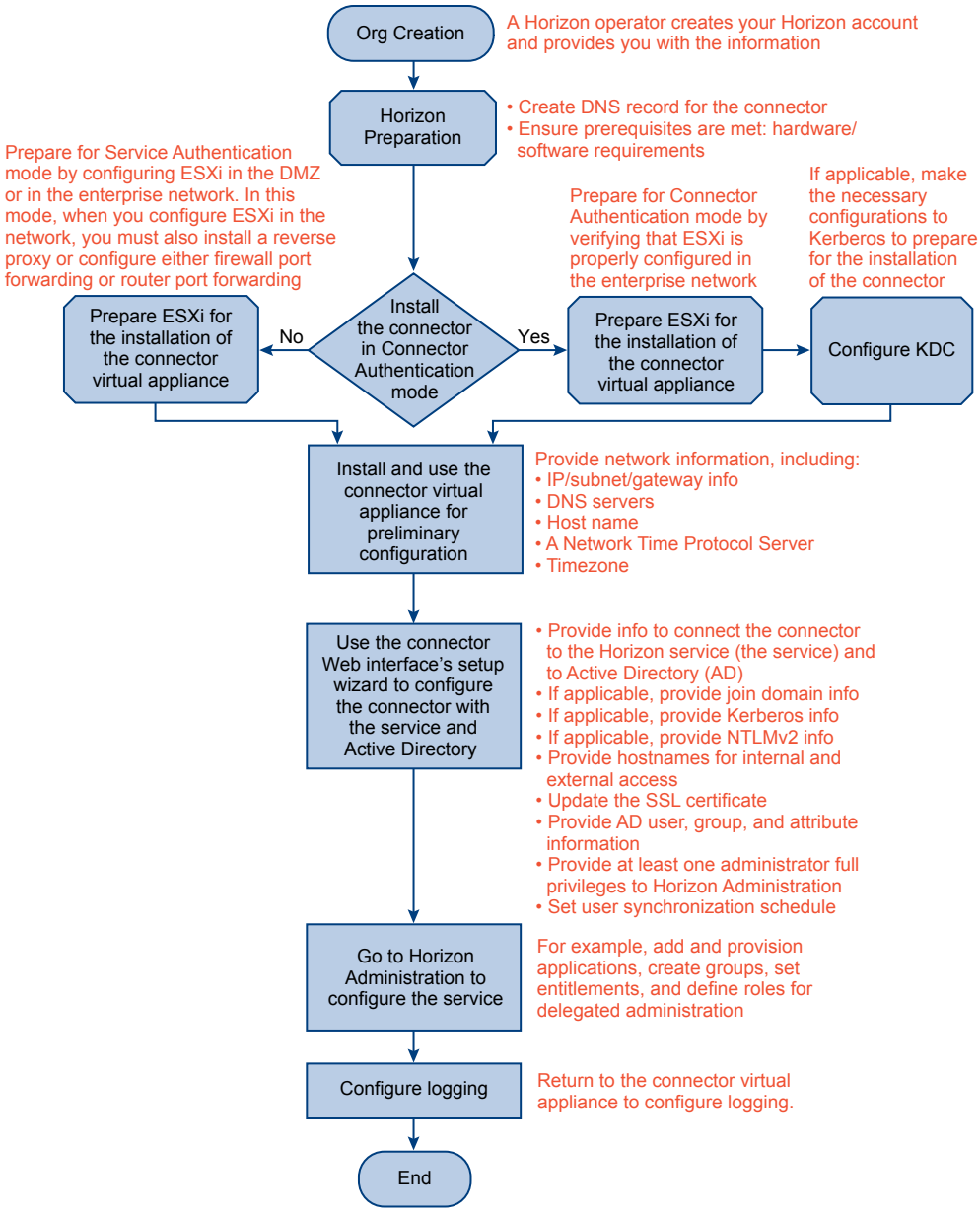
Draft comment filepath: GUID-ABA8925D-4AA7-4D09-B97F-B65D4546E3CE.xml

See "Installation and Configuration Flow of the Connector Integrated with ThinApp," on page 7 for information about installing and configuring the Connector integrated with ThinApp.

Figure 1 provides a broad overview of the tasks involved in installing and configuring the Connector. Early in the installation process, you must choose to install the Connector in Service Authentication mode or Connector Authentication mode. Choose Connector Authentication mode if you want Kerberos to authenticate interactions between users' browsers and the User Portal.

In the Connector Web interface, you can make most configurations using the setup wizard as indicated in the flowchart. However, you have the option of skipping many of those configurations, such as for Kerberos, until after you have completed the setup wizard. Then, on the **Advanced** tab of the Connector Web interface, you can configure the features you skipped and you can edit configurations you made previously.

Figure 1. The Connector Installation and Configuration Flowchart



Installation and Configuration Flow of the Connector Integrated with ThinApp

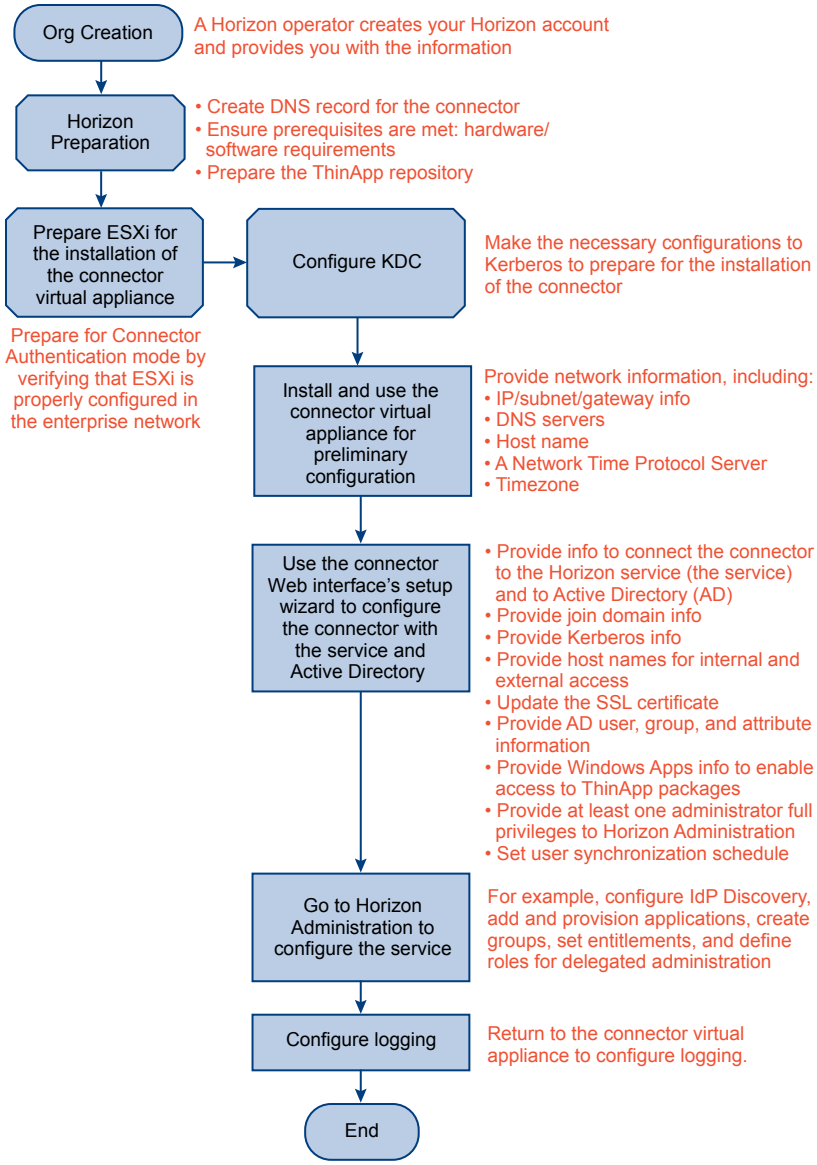
Figure 2 provides an overview of the tasks involved in integrating the Connector with ThinApp. Review this flow if you want to provide users with access to Windows applications captured as ThinApp packages. See "ThinApp Packages," on page 16 for an introduction to integrating an Application Manager deployment with ThinApp.

In the Connector Web interface, you can make most configurations using the setup wizard as indicated in the flowchart. However, you have the option of skipping many of those configurations, such as for Kerberos, until after you have completed the setup wizard. Then, on the **Advanced** tab of the Connector Web interface, you can configure the features you skipped and you can edit configurations you made previously.

Providing Application Manager users with access to ThinApp packages requires a variety of configurations. Some of those configurations do not directly involve the Connector. The following configurations are required to integrate an Application Manager deployment with ThinApp:

- Capture Windows applications as ThinApp packages. See ThinApp 4.7 or later documentation, such as *Using VMware Horizon Application Manager to Manage Deployment and Entitlement of ThinApp Packages* (ThinApp Horizon Integration Guide) and ThinApp User's Guide.
- Create the Windows applications network share to store the ThinApp packages. See "Create a Windows Applications Network Share for ThinApp Packages," on page 24
- Configure the Join Domain page of the Connector Web interface. See "Configure Join Domain," on page 32
- Configure the Windows Authentication page in the Connector Web interface. See "Overview of Configuring Windows Authentication (Kerberos) for the Connector," on page 41 and "Enabling Windows Authentication," on page 33.
- Configure the Windows Apps page of the Connector Web interface. See "Configure Windows Apps," on page 34
- Enable IdP Discovery by configuring IP address ranges for the Connector instance using the Application Manager Administrator Web interface. See *Application Manager Administrator Help*.
- Verify that the Horizon Agent is properly configured on users' Windows system. See *Application Manager User Help*.

Figure 2. The Connector with ThinApp Installation and Configuration Flowchart



1 Introduction to Application Manager

Draft comment filepath: GUID-C2EA1CFA-8AE0-478B-8BB4-593D843FBD54.xml

Application Manager is an identity and access management service or virtual appliance that unifies your software as a service (SaaS) applications and Windows applications (captured as ThinApp packages) into a single catalog for entitlement.

NOTE This document uses the following Application Manager URL example https://*MyCompany*.horizonmanager.com, which is an example URL for the hosted service. If you are using the Application Manager on-premise virtual appliance instead, replace the preceding example URL with this example URL: https://*MyOrg*.*MyDomain*.com.

Table 1-1. Application Manager Component Terminology

Application Manager Component	Other Terms Used	Description
Application Manager deployment	■ None	The entire Application Manager deployment, including Application Manager, the Connector, the related interfaces to access those components, and all other components necessary to enable users to access applications.
Application Manager ■ Application Manager ■ Application Manager Appliance	None ■ hosted service ■ on-premise appliance	Two versions of Application Manager exist: the hosted service and the on-premise virtual appliance. As a generalization, both versions are referred to as the service. If you have the hosted service, it is maintained for you. If you have the on-premise appliance, you install and maintain it yourself. Application Manager stores entitlement, SaaS, policy, and ThinApp package information and communicates with your Connector instances to access Active Directory information.
Application Manager virtual appliance interface	■ virtual appliance interface	The interface of the Application Manager virtual appliance. You use this interface to perform the initial configuration of Application Manager on premise. You also use this interface to access the command-line interface of the underlying Linux operating system.

Table 1-1. Application Manager Component Terminology (Continued)

Application Manager Component	Other Terms Used	Description
Application Manager Operator Web interface	■ Operator Web interface	The browser-based interface of the on-premise version of Application Manager that individuals with operator privileges access to manage organizations and the Operator application catalog. Application Manager provides multi-tenancy. This interface provides an overview of all the organizations managed by Application Manager.
Application Manager Administrator Web interface	■ Administrator Web interface	The browser-based interface of Application Manager that you, as an administrator of a specific organization, use to manage user access and entitlements to SaaS and ThinApp-packaged applications. This interface provides an overview of a single organization.
Application Manager User Web interface	■ Workspace ■ User Web interface	The browser-based interface of Application Manager that users access to use SaaS or ThinApp-packaged applications. This interface includes the User Portal, which provides users easy access to applications.
Application Manager internal database server	■ internal database server	The default database server, vPostgres 9.1, that ships with the on-premise version of Application Manager. You can use this internal database server during the proof-of-concept phase of deployment. For production, you should disable the internal database server and use a supported external database server, such as PostgreSQL 9.1.
Application Manager Operator application catalog	■ Operator application catalog ■ Operator catalog	The master catalog of applications, which is accessible using the operator Web interface. Operators can create application in this catalog. Operators can assign applications to all organizations in the system or only to specific organizations.
Application Manager Administrator application catalog ■ Administrator source application catalog ■ Administrator active application catalog	■ Administrator application catalog ■ Administrator catalog	A catalog of applications accessible using the Administrator Web interface. You, as an organization administrator, manage the applications assigned to you by operators. To make applications available to users, you must move them from the Administrator source application catalog to the Administrator active application catalog.
Application Manager User application catalog	■ User application catalog ■ User catalog	A catalog of applications accessible using the User Web interface. Users access and use the applications assigned to them by you as an organization administrator.

Table 1-1. Application Manager Component Terminology (Continued)

Application Manager Component	Other Terms Used	Description
Connector	■ Connector Appliance ■ Connector instance	The virtual appliance you install in your enterprise network to connect Application Manager to Active Directory and to the ThinApp package repository.
Connector virtual appliance interface	■ None	The interface of the Connector virtual appliance. You use this interface to make the initial configurations of the Connector. You also use this interface to access the command-line interface of the underlying Linux operating system.
Connector Web interface	■ None	The browser-based interface you use to configure and manage the Connector after using the Connector virtual appliance to make the initial Connector configurations.
ThinApp Repository	■ Windows applications network share	A shared folder that you create to store Windows applications captured as ThinApp packages. You then provide users access to these applications.
Horizon Agent	■ Agent	A ThinApp-specific component installed on user's Windows systems that allows users to access Windows applications captured as ThinApp packages.

Application Manager Authentication Modes

Draft comment filepath: GUID-C2EA1CFA-8AE0-478B-8BB4-593D843FBD54.xml

Application Manager facilitates username and password validation by communicating with your Active Directory server. You install the Connector as a virtual appliance that communicates with your local directory using LDAP. You can use LDAP over SSL.

The Connector can operate in different modes of authentication, which indicate the flow of user authentication to access Application Manager. While the Application Manager Appliance supports Connector Authentication mode, the Application Manager service (the hosted version of Application Manager) supports both Service Authentication mode and Connector Authentication mode. The Connector also supports both Connector Authentication mode and Service Authentication mode. Be aware that Service Authentication mode is being deprecated and will not be supported in future releases. See "Service Authentication Mode," on page 14 for the list of configurations that allow Application Manager to access the Connector in Service Authentication mode. Also, your Application Manager deployment can operate in both modes simultaneously.

In Connector Authentication mode, once users are logged in to the internal network, they are usually not prompted for their credentials when attempting to access Application Manager. In specific situations where users are prompted for their credentials to access Application Manager, the Connector presents the login page. In Service Authentication mode, users are always prompted for their credentials when attempting to access Application Manager, in which case Application Manager presents the login page.

You must understand the details involved in each mode of authentication before deciding the mode or modes in which to configure your deployment.

Connector Authentication Mode

Draft comment filepath: GUID-C2EA1CFA-8AE0-478B-8BB4-593D843FBD54.xml

You must Configure your deployment in Connector Authentication mode if you want to use Kerberos (Windows authentication). For Connector Authentication mode, the user authentication process is, in effect, outsourced to the Connector, where the Connector acts as an identity provider. Therefore, for this mode of authentication, the Connector is the starting point for user authentication.

Table 1-2. Providing User Access to Application Manager in Connector Authentication Mode

User Access From Inside the Enterprise Network	User Access From Outside the Enterprise Network
■ Configure Kerberos authentication or username/password authentication.	■ Install both the Application Manager and Connector virtual appliances in a manner that provides Internet access. Kerberos authentication is not available outside the network. Therefore, the best practice is to use RSA SecurID authentication, though username/password authentication is available as well. ■ You can install the Connector and Application Manager virtual appliances without Internet access. However, to provide user access from outside the enterprise network, users will need a VPN connection.

If you decide to enable Internet access to Application Manager and the Connector to provide users outside the enterprise network access to Application Manager, configure them in one of the following ways:

- Install Application Manager and the Connector inside the DMZ.
- Install a reverse proxy server in the DMZ pointing to Application Manager and the Connector installed behind the firewall.
- Configure firewall port forwarding or router port forwarding to point to Application Manager and the Connector installed behind the firewall.

For Connector Authentication mode, if you do not configure IdP discovery, you must provide users access to specific URLs that direct the authentication flow through the Connector. These URLs contain the appropriate information to direct users through the Connector directly to Application Manager. You must provide users access to such URLs.

IMPORTANT Configuring IdP discovery eliminates the need to use the long URLs provided in the following table. See "IdP Discovery," on page 15.

Table 1-3. Connector Authentication Mode: URL Examples

Target	URL Example	Information
Application Manager User Portal	https://*MyCompany*.horizonmanager.com/SAAS/API/1.0/GET/federation/request?i=*IDP#*&s=0	When your deployment is production ready, provide this URL to users to give them access to the User Portal. Replace *MyCompany* with the correct account name and replace *IDP#* with the IdP ID available on the Connector Internal Access page.
	https://*ConnectorHost*.*DomainName*/login/	Use this URL for testing and troubleshooting purposes if Kerberos is not configured. Replace *ConnectorHost* and *DomainName* with the appropriate values.

Table 1-3. Connector Authentication Mode: URL Examples (Continued)

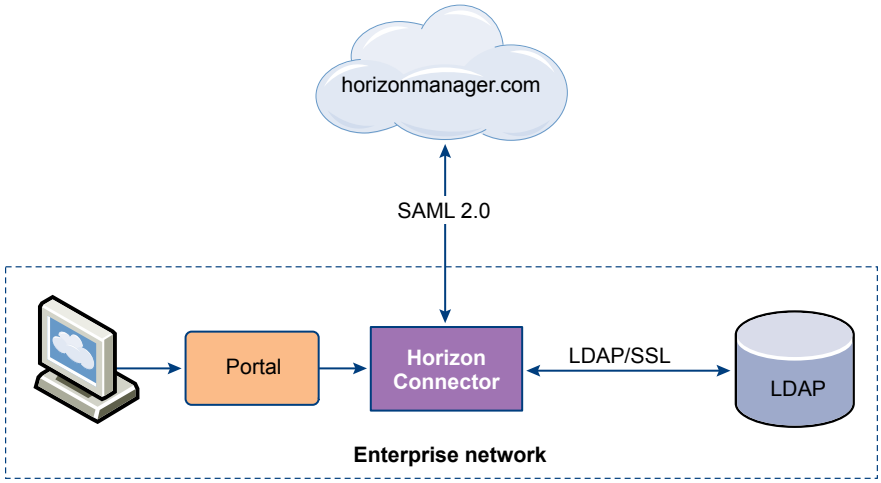
Target	URL Example	Information
	https://*ConnectorHost*.*DomainName*/authenticate/	Use this URL for troubleshooting and testing purposes if Kerberos is configured. Replace *ConnectorHost* and *DomainName* with the appropriate values.
Specific Applications	https://*MyCompany*.horizonmanager.com/SAAS/API/1.0/GET/federation/request?i=*IDP#*&s=*SP#*	When your deployment is production ready, provide this URL to users to give them one-click access to a specific application. Replace the placeholders. For example, replace *SP#* with the ID number for a specific application. The application ID numbers are available from the Application Catalog in Application Manager.

For deployments where Kerberos is configured, the Connector validates user desktop credentials using Kerberos tickets distributed by the key distribution center (KDC).

In Connector Authentication mode, the Connector acts as a federation server within your network, creating an in-network federation authority that communicates with Application Manager using SAML 2.0 assertions. The Connector authenticates the user with Active Directory within the enterprise network (using existing network security).

A troubleshooting-related aspect of Connector Authentication mode is that users can still be authenticated even when Kerberos fails. In fact, users can still be authenticated when Kerberos is not configured. In such cases, an Application Manager redirect takes place causing the Connector to present users with a login page. This Connector-supplied login page prompts users to provide their usernames and passwords again for access to Application Manager. The Connector then validates users against Active Directory. The following figure is of a deployment of Application Manager as a hosted service, not as an on-premise appliance.

Figure 1-1. The Connector Installed in Connector Authentication Mode



Connector Authentication Mode and RSA SecurID

Draft comment filepath: GUID-C2EA1CFA-8AE0-478B-8BB4-593D843FBD54.xml

After you install the Connector in Connector Authentication mode, you can configure SecurID to provide additional security. For an overview of using RSA SecurID with the Connector, see "Overview of Configuring SecurID," on page 39.

You can configure SecurID with or without Kerberos. However, the most common use case is to use SecurID to authenticate users outside the enterprise network, while Kerberos authentication is not available outside the network. See "IdP Discovery," on page 15 for more information about configuring two Connector instances, one instance for users inside the enterprise network and the other for users outside the network.

RSA SecurID with	Result
Kerberos configured	Kerberos authentication takes precedence. Users are only prompted for their SecurID passcode if Kerberos authentication fails.
username-password verification as part of Connector Authentication mode	SecurID takes precedence and username password verification is disabled. Users are prompted for their SecurID passcode. They are never prompted for their Active Directory credentials.

For various reasons, both intentional and unintentional, Kerberos authentication might not function. For example, you might intentionally prevent specific users from accessing the enterprise network. Also, non-Windows machines do not support Kerberos authentication. When Kerberos and SecurID are both configured, but Kerberos authentication fails, users are prompted for their SecurID passcode.

Service Authentication Mode

Draft comment filepath: GUID-C2EA1CFA-8AE0-478B-8BB4-593D843FBD54.xml

CAUTION Service Authentication mode is being deprecated and will not be supported in future releases.

Service Authentication mode provides users with a consistent experience when accessing Application Manager from inside or outside the enterprise network. Application Manager is the starting point for user authentication in this mode and multi-factor authentication is enforced in all situations.

You can use Service Authentication mode as the sole authentication flow for providing users access to Application Manager. For this type of access, since Application Manager must have a way of accessing the Connector, configure access in one of the following ways:

- Install the Connector inside the DMZ.
- Install a reverse proxy server in the DMZ pointing to the Connector installed behind the firewall.
- Configure firewall port forwarding or router port forwarding to point to the Connector installed behind the firewall.

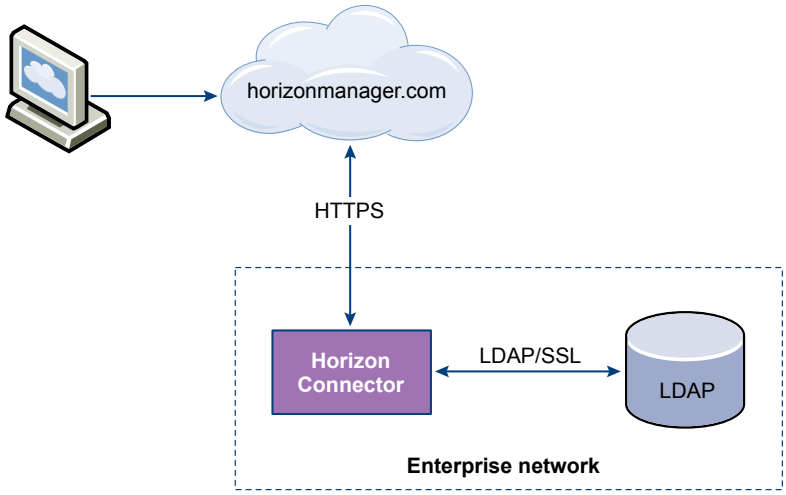
Then, you must provide users with a URL directly to Application Manager.

Table 1-4. Service Authentication Mode: URL Examples

Target	URL Example	Information
Application Manager User Portal	https://*MyCompany*.horizonmanager.com/	Provide this URL to users to give them access to the User Portal. Replace *MyCompany* with the correct account name.
Specific Applications	https://*MyCompany*.horizonmanager.com/SAAS/launchUsersApplication.do?aid=*SP#*	Provide this URL to users to give them access to a specific application. Replace the placeholders. For example, replace *SP#* with the ID number for a specific application. The application ID numbers are available from the Application Catalog in Application Manager.

For Service Authentication mode, Application Manager enforces multi-factor authentication. Therefore, when users attempt to access Application Manager, they are prompted for their Active Directory credentials and for answers to their security questions. They are also provided with a confirmation image. Application Manager collects the Active Directory credentials and passes them to the Connector to validate with Active Directory. When the validation is complete and users have answered the security questions, they have one-click access to the applications available in Application Manager. The following figure is of a deployment of Application Manager as a hosted service, not as an on-premise appliance.

Figure 1-2. The Connector Installed in Service Authentication Mode



Both Modes

Draft comment filepath: GUID-C2EA1CFA-8AE0-478B-8BB4-593D843FBD54.xml

You can implement both Connector Authentication mode and Service Authentication mode in a single deployment.

IdP Discovery

Draft comment filepath: GUID-C2EA1CFA-8AE0-478B-8BB4-593D843FBD54.xml

You configure the IdP Discovery feature in the Application Manager Administrator Web interface. See *Application Manager Administrator Help*. The IdP Discovery feature works in conjunction with Connector Authentication mode. IdP Discovery refers to the discovery of identity providers. The Connector acts as an identity provider. Therefore, even though users access a URL directly to Application Manager, such as https://MyCompany.horizonmanager.com/, when IdP Discovery is properly configured, it finds (discovers) and redirects users to the specific Connector instance. With a single URL, you can provide all users access to the User Portal.

For the IdP Discovery feature to function, you must configure IP address ranges in Application Manager. When you have multiple Connector instances, the order in which the corresponding Connector records are listed in Application Manager is important if the IP ranges overlap. In such cases, the first Connector record to include an IP address is given precedence.

CAUTION When you remove or reset a Connector instance, you must remove the corresponding Connector record from the list of Connector records accessible with the Application Manager Administrator Web interface.

The IdP Discovery feature typically applies when users attempt to access Application Manager from inside the enterprise network and when they are on the same domain as the Active Directory instance.

When users within the specified IP address ranges access the provided URL, their request is processed in Connector Authentication mode and the request is redirected to the Connector. Assuming that Kerberos is configured, a SAML assertion generated by the Connector is used for authentication and users are granted access to the User Portal without being prompted for their username and password. If Kerberos is not configured, users must provide their username and password on the Connector login page to gain access. When users outside the specified IP address range use the provided URL, their request is processed in Service Authentication mode, if you have it enabled, requiring them to provide their username and password on the Application Manager login page to gain access.

You can deploy Application Manager with IdP Discovery in a variety of ways, two of which are summarized in the examples that follow.

Example of IdP Discovery With Both Modes of Operation Configured

This is one possible way to configure IdP Discovery when Application Manager is deployed in both Service Authentication mode and Connector Authentication mode. For this deployment, you configure two Connector instances, one in Service Authentication mode and one in Connector Authentication mode.

- Connector instance in Service Authentication mode: You do not add any IP address ranges for this Connector instance.
- Connector instance in Connector Authentication mode: You configure IP address ranges in Application Manager to include users within the enterprise network.

The result of this configuration is that users attempting to access the User Portal within the network are authenticated in Connector Authentication mode by Kerberos or username/password authentication, while users outside the network are authenticated in Service Authentication mode.

External RSA SecurID and Internal Kerberos Authentication Example of IdP Discovery

This is one possible way to configure IdP Discovery and SecurID in the same Application Manager deployment. For an overview of configuring RSA SecurID with the Connector, see "Overview of Configuring SecurID," on page 39. For this deployment, you configure two Connector instances, both in Connector Authentication mode.

- Internal - First Connector instance in Connector Authentication mode: You do not configure SecurID for this Connector instance. In Application Manager, you configure IP address ranges to include users within the enterprise network.
- External - Second Connector instance in Connector Authentication mode: You configure SecurID for this Connector instance. In Application Manager, you configure a single IP address range that includes all possible users. Therefore, you set the IP address range from 0.0.0.0 to 255.255.255.255.

The result of this configuration is that users attempting to access the User Portal are authenticated in Connector Authentication mode. Users inside the enterprise network are authenticated by Kerberos or username/password authentication. Users outside the enterprise network are authenticated by SecurID authentication.

ThinApp Packages

ThinApp package access requires Connector Authentication mode. See "Installation and Configuration Flow of the Connector Integrated with ThinApp," on page 7 for information about integrating the Connector with ThinApp.

Evaluation and Quick Access to Application Manager

Draft comment filepath: GUID-C2EA1CFA-8AE0-478B-8BB4-593D843FBD54.xml

For evaluation purposes, you can access the User Portal as an administrative user with minimum configuration. This quick-access configuration works in Connector Authentication mode only. Using the Connector Web interface, you run the initial configuration wizard, stopping before running the setup wizard. The initial configuration wizard requires you to provide your activation code and information for Active Directory. The Active Directory information is not used for Directory Sync because quick-access configuration does not enable directory synchronization. The Active Directory information is required for the following purposes:

- To establish a connection to Active Directory, which is used to verify your administrative user credentials when you attempt to log in to Application Manager.
- To allow you to log in to the Application Manager. You use the username associated with the Bind DN user account and respective password as the credentials to log in to Application Manager as an administrator.

With quick-access configuration, you cannot configure Kerberos authentication, nor can you access Windows applications captured as ThinApp packages. Also, with the quick-access configuration, you can use the default internal database, instead of configuring an external database. The purpose of quick-access configuration is to provide easy access to the basic functionality of Application Manager, which you can evaluate.

Security Considerations and System Requirements for the Connector

2

Draft comment filepath: GUID-8430CCA1-C4C0-47C6-A5DD-09A396D5BD46.xml

When you install and configure the Connector, you install the Connector virtual appliance and use both the Connector virtual appliance interface and the Connector Web interface for configuration purposes. You must manage the Web interface with care to avoid security issues.

Consider the Connector system requirements within the context of the following security concerns:

- The Connector virtual appliance interface is accessible to anyone with access to the machine on which vShere and the virtual appliance is hosted. Protection relies on firewalling and enforcing authentication to the vShere host.
- The Connector Web interface listens on HTTP port 8443 for administration and port 443 for user authentication.

Connector Recommendations and Requirements

Draft comment filepath: GUID-7363695F-0DF3-4A60-998A-0B3E71C5628D.xml

To synchronize your Active Directory data effectively with Application Manager, ensure that the environment for the Connector virtual appliance meets the minimum requirements.

The following components are required:

- The Connector virtual appliance VMware provides as an Open Virtual Appliance `.ova` file.
- VMware vSphere as the host of the virtual appliance. See the release notes for the currently supported vSphere versions.
- A virtual machine client that provides access to the Connector virtual appliance interface.
- The appropriate VMware licenses.
- A conversion tool, if your VMware hypervisor does not open OVA files directly. VMware offers a free tool for Windows and Linux. See "(Optional) Convert the Virtual Appliance File Format," on page 25.

Hardware Requirements for the Connector Virtual Appliance Host

Draft comment filepath: GUID-7363695F-0DF3-4A60-998A-0B3E71C5628D.xml

Ensure that the environment for the host, the vSphere instance, to run the Connector virtual appliance meets the minimum hardware requirements.

Table 2-1. Minimum Connector Hardware Requirements

Component	Minimum Requirement
Processor	One Intel Xeon Dual Core, 3.0GHz, 4MB Cache
Random-access memory	6GB DDR2 667 MHz, ECC and registered

Table 2-1. Minimum Connector Hardware Requirements (Continued)

Component	Minimum Requirement
On-board LAN	One 10/100/1000Base-TX port
Storage	15GB

Resource Requirements and Recommendations for the Connector Virtual Appliance

Ensure that the resources allocated to the Connector virtual appliance meet the minimum requirements.

Table 2-2. Connector Resource Requirements and Recommendations

Component	Required	Recommended
Processor	2 vCPU	4 vCPU for higher performance
Random-access memory	1GB	2GB
Storage	15GB	20GB

Network Configuration Requirements for Connector Deployment

The network configuration requirements vary slightly depending on whether you configure the Connector in Service Authentication mode or Connector Authentication mode.

Table 2-3. Network Configuration Requirements by Mode of Operation

Mode of Operation	Network Requirement
Service Authentication mode only	■ Application Manager Hosted Service - Inbound firewall port 443 opened from Application Manager to the Connector. Datacenter IP addresses: 206.80.50.32 and 209.34.94.96 . ■ Application Manager Appliance - Port 443 opened on the path from Application Manager to the Connector.
Connector Authentication mode only	If necessary, port 88 opened on the path between the Connector and Active Directory to enable Kerberos authentication. However, when you follow the recommended deployment of the Connector in Connector Authentication mode, a firewall does not exist on that path.
Connector Authentication mode only	If necessary, port 443 opened on the path between users and the Connector for Connector Authentication mode.
Connector Authentication mode, outside access only	Inbound firewall port 443 opened from users outside the enterprise network to the Connector.
Both modes	■ Application Manager Hosted Service - Outbound firewall port 443 opened from the Connector to the Internet. ■ Application Manager Appliance - Port 80 and 443 opened on the path from the Connector to Application Manager.

Table 2-3. Network Configuration Requirements by Mode of Operation (Continued)

Mode of Operation	Network Requirement
Both modes	Port opened on the path from the Connector to Active Directory, typically port 389 or 636. The default global catalog ports are 3268 and 3269.
Both modes	Access to a Network Time Protocol (NTP) server made available in one of the following ways: ■ To allow the Connector to access an external NTP server, you must ensure the outbound firewall port 123 (NTP Protocol) is opened from the Connector to the Internet. ■ If you do not want a firewall port open for the NTP server, you must ensure that the NTP configuration is pointing to an internal NTP server. You perform this action when you configure the Connector using the Connector virtual appliance interface.

Preparing to Install the Connector

3

Draft comment filepath: GUID-75ECC762-7AC7-4C6C-B34B-A1FF980BE2E3.xml

Preparing to install the Connector involves creating the DNS name; obtaining the Connector virtual appliance; and configuring the hardware, resource, and network settings of the Connector host. Other preinstallation tasks might be required depending on the specifics of your deployment.

Procedure

1 Prepare to Install the Connector on page 23

You must prepare your environment for the installation of the Connector.

2 Create a Windows Applications Network Share for ThinApp Packages on page 24

If you want to enable the VMware ThinApp management capabilities of Application Manager and allow users to access ThinApp packages from the User application catalog, you must create a network file share and store your ThinApp packages in that shared folder.

3 (Optional) Convert the Virtual Appliance File Format on page 25

You can convert the virtual appliance file format from the OVA format to the VMX format by using the VMware OVF tool. Perform this file format conversion only if the hypervisor does not support the OVA format.

Prepare to Install the Connector

Draft comment filepath: GUID-679BB7F3-0205-4B4E-937C-3275404B48A9.xml

You must prepare your environment for the installation of the Connector.

Prerequisites

- Decide whether you are installing this Connector instance in Connector Authentication mode or Service Authentication mode. See Chapter 1, "Introduction to Application Manager," on page 9. This decision influences the physical location of the vSphere host that will host the Connector.
- If you are installing the Connector in Connector Authentication mode and also want to provide Kerberos authentication, no configuration of Kerberos is necessary as long as Active Directory is properly configured. See "Overview of Configuring Windows Authentication (Kerberos) for the Connector," on page 41 for an overview of integrating Kerberos with the Connector.
- If you are installing the Connector in Connector Authentication mode and also want to provide RSA SecurID security, familiarize yourself with the process of integrating SecurID server with the Connector. See "Overview of Configuring SecurID," on page 39.

- If you want users to have access to Windows applications captured as ThinApp packages, create a network file share in which to store the ThinApp packages. See "Create a Windows Applications Network Share for ThinApp Packages," on page 24 for information specific to creating a network file share. See "Installation and Configuration Flow of the Connector Integrated with ThinApp," on page 7 for an overview of integrating Application Manager with ThinApp.
- Ensure that all the hardware, network, and resource requirements are met. See "Connector Recommendations and Requirements," on page 19.

Procedure

1 Create the Domain Name System (DNS) record for the Connector virtual appliance host.

The DNS name must be available for the Connector hostname to be recognized. Depending on your organization, creating the DNS record might take several days. Provide an enough time to ensure that the DNS name is available when required.

IMPORTANT If you are installing the Connector in Service Authentication mode, make the DNS name accessible externally.

---

2 Configure the network and firewall settings for the Connector host according to the mode of operation you have chosen.

3 Download the .ova file for the Application Manager virtual appliance from the VMware Download Center and deploy it.

You can download the `.ova` file directly to the vSphere host or you can download it to another machine.

Create a Windows Applications Network Share for ThinApp Packages

Draft comment filepath: GUID-6BB6851D-38A4-4665-88F5-640098A8A986.xml

If you want to enable the VMware ThinApp management capabilities of Application Manager and allow users to access ThinApp packages from the User application catalog, you must create a network file share and store your ThinApp packages in that shared folder.

The Connector synchronizes with the Windows applications network file share regularly to communicate ThinApp package metadata to Application Manager.

Prerequisites

You should be familiar with ThinApp package related tasks, such as capturing Windows applications as ThinApp Packages. Before you can access ThinApp packages, you must capture Windows applications that can be managed with Application Manager. See *Using VMware Horizon Application Manager to Manage Deployment and Entitlement of ThinApp Packages* (ThinApp Horizon Integration Guide).

Procedure

1 Create a shared folder as the Windows applications network share.

Verify that the shared folder meets the following conditions:

- The shared folder is accessible using a Uniform Naming Convention (UNC) path from each system running the Horizon Agent. For example, a Windows applications network share named `appshare` on a host named `server` should be accessible using the UNC path `\\server\appshare`.
- The fully qualified host name of the shared folder is resolvable from the Connector.
- The host of the shared folder is joined to the same Microsoft Active Directory domain as the Connector.
- The Connector Active Directory computer account and users have read access to the shared folder.

- The Active Directory groups Authenticated Users and Domain Computers have read-only access to the shared folder. If you prefer, access can be more specific to allow only the Connector computer account and Application Manager users.

2 Within the Windows applications network share, create a shared subfolder for each ThinApp package.

Verify that the subfolders for each ThinApp package meet the following condition:

- For each ThinApp package, the shared folder is an application-named subfolder of the Windows applications network share. For example, if the application is called `abceditor`, the folder for the ThinApp package is available at `\\server\appshare\abceditor`. Once you have copied the ThinApp EXE and DAT files to the application-named subfolder as described in the ThinApp Horizon Integration Guide, the folder will include files such as the following:
  - `\\server\appshare\abceditor\abceditor.exe`
  - `\\server\appshare\abceditor\abceditor.dat`

What to do next

Populate the application-named subfolders with the appropriate ThinApp packages. See ThinApp Horizon Integration Guide.

(Optional) Convert the Virtual Appliance File Format

Draft comment filepath: GUID-3EC77DB6-9E81-4F42-9D57-8DC5F0037141.xml

You can convert the virtual appliance file format from the OVA format to the VMX format by using the VMware OVF tool. Perform this file format conversion only if the hypervisor does not support the OVA format.

The Open Virtualization Format (OVF) tool is a free command-line utility that can convert file formats of virtual machines. You install the virtual appliance on a VMware hypervisor that supports the VMX format and convert the OVA format to the VMX format.

Procedure

1 Download the VMware OVF tool from the VMware Web site and install it.

Follow the installer instructions to install the tool.

2 Create and name a directory in your hypervisor's data store, which is the directory where virtual machines reside.

Provide the name for the directory.

3 Move to that directory.

The converter tool deposits output files in the current directory.

4 Start the converter tool with the following command: *`path-to-ovftool`* `-tt=VMX` *`ova-file-name VMX-file-name`*

For example: `/usr/bin/ovftool -tt=VMX virtualappliance-1.1.0.ova virtualappliance`

The command might take a few minutes to complete. The following is sample output:

```
Opening OVA source:
../virtualappliance-1.1.0.ova
Opening VMX target: central-virtualappliance
Target: central-virtualappliance.vmx
Disk progress: 36%
…
Disk Transfer Completed
Completed successfully
```

Example: File Conversion Output

Draft comment filepath: GUID-3EC77DB6-9E81-4F42-9D57-8DC5F0037141.xml

Two items appear in your current directory as a result of this task: a `.vmdk` disk image file and a `.VMX` virtual machine configuration file, as the following example shows:

```
-rw------- 1 root root 1.6G 2011-05-17 14:46 central-virtualappliance-disk1.vmdk
-rw-r--r-- 1 root root 1.1K 2011-05-17 14:46 central-virtualappliance.vmx
```

What to do next

Install the virtual appliance on your hypervisor.

4 Installing the Connector

Draft comment filepath: GUID-5478B220-290E-4863-909B-E33930072CDD.xml

After you install the Connector, you can use it to access and configure Application Manager.

Installing the Connector includes the following tasks:

- Use vSphere Client to install the Connector virtual appliance.
- Start and configure the virtual appliance.
- Use the Connector Web interface to perform the initial configuration of the Connector necessary to access the Application Manager Administrator Web interface.

The steps to prepare the virtual appliance can vary. For specific instructions, see the vSphere documentation.

This chapter includes the following topics:

Start the Connector Virtual Appliance

Draft comment filepath: GUID-5FF5D042-DA2D-4C0E-BC02-061CF3D051C7.xml

The Connector is a virtual appliance running in a virtual machine. Starting the virtual appliance gives you access to the Connector virtual appliance interface, including command-line access to the underlying Linux operating system of the virtual appliance.

You perform the preliminary configuration of the Connector with the virtual appliance interface. The underlying operating system for the Connector is SUSE Linux Enterprise Server (SLES 11 SP1). You can configure the operating system files directly from the Connector virtual appliance interface. Use caution when editing the operating system files since changes can have unanticipated affects on the deployment.

Procedure

1 Use vSphere Client to install the Connector virtual appliance by choosing the Deploy OVF Template option.

   See VMware vSphere documentation.

2 Power on the virtual appliance.

   This action boots the virtual appliance's SLES operating system, starts the Connector processes, and connects to a DHCP server, if present, to acquire an IP address.

During start up, the virtual machine displays messages in the Connector virtual appliance interface. You can usually ignore the messages until you are prompted to change the UNIX passwords. You can perform the initial configuration of the Connector as described in "Configure the Connector with the Connector Virtual Appliance Interface," on page 28.

Configure the Connector with the Connector Virtual Appliance Interface

Draft comment filepath: GUID-43547321-93A9-42FA-963F-9B851B899F99.xml

Use the Connector virtual appliance interface to make the initial configurations to the Connector, such as network and time-related configurations.

You can use the Connector virtual appliance interface to update these settings or to perform other configurations to the SLES operating system. You use the Connector Web interface to perform most Connector configurations.

You configure the Connector virtual appliance interface after you start the appliance and are prompted to change your UNIX password.

Prerequisites

- Configure the Connector virtual appliance interface after you have installed the virtual appliance on vSphere. See "Start the Connector Virtual Appliance," on page 27.
- Verify that you followed the steps to prepare for the installation of the Connector. See "Prepare to Install the Connector," on page 23.
- If applicable, open a firewall port for an external Network Time Protocol (NTP) server. For more information about the network requirements for configuring an NTP server, see Table 2-3.

Procedure

1 At the UNIX password prompts, type the password to use to access the SLES operating system of the Connector.

2 Select **Configure Network**.

Option	Action
Respond to the IPv6 prompt.	Type **y** if you have an IPv6 network. If you do not have an IPv6 network, type **n**.
Respond to the DHCPv4 prompt.	NOTE The recommended practice is to use a static IP address. If you have a static IP address, type **n**. Continue responding to the subprompts related to a static IP address. If you have a DHCPv4 address, type **y** and continue responding to the subprompts related to DHCP and a proxy server. If you respond with **n**, continue responding to the subprompts related to a static IP address, including subprompts about IPv4 address, netmask, gateway, DNS servers, hostname, and proxy server. Configure a proxy server IP address if your network requires all outbound HTTP or HTTPS connections to go through a network proxy. IMPORTANT If you configure a proxy server IP address, reboot the Connector virtual appliance after you finish configuring the Connector to ensure that the proxy settings take effect. NOTE If you are configuring the Connector with join domain functionality, list Active Directory as the DNS server. You must configure join domain functionality if you plan to provide users with access to ThinApp packages.

When you are finished configuring the network settings, the main screen of the Connector virtual appliance interface reappears.

3 If necessary, configure a Network Time Protocol server.

By default, the Connector virtual appliance points to specific external NTP servers, as listed in the `/etc/ntp.conf` file. However, networking or DNS issues might prevent the virtual appliance from reaching the external NTP servers. Also, you might want to use NTP servers other than the default settings. When you properly configure the Application Manager deployment, the time for all systems is maintained within a range of one minute.

CAUTION Failure to follow the NTP recommendations can prevent user access to the Application Manager Web interface since both the SAML and Kerberos protocols rely on an accurate system clock. The protocols used between Application Manager and the Connector and between the Connector and Active Directory require that the time synchronization of these systems falls within a narrow range.

a Select **Login** and log in to the Linux operating system.

b Using Linux commands configure the Connector's time settings.

See Timekeeping best practices for Linux guests (KB 1006427) for information about time settings for SLES 11. Consult the section on NTP recommendations.

c Exit the command line to return to the main page of the Connector virtual appliance interface.

4 Confirm the Network Time Protocol configuration.

You should check this screen in the following situations:

- When you first install the Connector virtual appliance interface.
- Any time in the future when you modify the networking environment that can affect the ability to contact the NTP server or when you change the NTP configuration.
- As a troubleshooting option when users experience an access issue.

See the troubleshooting section for information about the possible messages on this screen.

5 Set the time zone for the Connector.

a Select **Set Timezone**.

b Continue selecting location options to select your specific time zone.

6 Use the command line to restart the Apache Tomcat server for the time zone configuration to take effect.

a From the Connector virtual appliance interface, select **Login** and log in to the Linux operating system.

b Run the following command to restart the Web server: `/etc/rc.d/tcserver-c2 restart`.

What to do next

Use the Web interface to configure the Connector.

Access the Connector with the Web Interface

Draft comment filepath: GUID-31D243AC-B06D-470C-8E58-9F00A9EAB8EE.xml

When the Connector has a host name, you can use a browser to access the Web interface.

Until you update the SSL certificate, the Connector uses a default self-signed certificate. Your browser has no information on this certificate and, therefore, displays a page indicating that a potential security issue exists. Bypass such browser messages to access the Connector Web interface. In the Connector Web interface, you can update the certificate, which can prevent such browser messages in the future.

CAUTION Use the Connector hostname, not the IP address, to access the Connector Web interface. Using the Connector IP address instead of the hostname negatively affects Kerberos authentication when you or users access Application Manager through the Connector.

Prerequisites

Verify that the following conditions are met:

- You configured the Connector virtual appliance interface. See "Configure the Connector with the Connector Virtual Appliance Interface," on page 28.
- Verify that you have access to a supported browser. The Connector supports Firefox and Internet Explorer.

Procedure

1 Use a supported browser to access the Connector Web interface and, if necessary, bypass any warnings about trusting the site.

See the current release notes for information on supported browsers.

The URL for accessing the Connector follows the format https://*ConnectorHost*.*DomainName*:8443/.

For example: https://ConnectorHost.mycompany.com:8443/.

Your browser prompts you for a new password.

2 Select a password as prompted and click **Next**.

The first page of the initial configuration wizard appears in your browser.

What to do next

Complete the initial configuration wizard.

Using the Initial Configuration Wizard

Draft comment filepath: GUID-6475527E-7C19-4ECE-8852-5224E771AE5F.xml

Use the initial configuration wizard to activate your Connector instance and to establish a connection to Active Directory.

The initial configuration wizard allows quick-access configuration of the Connector. See "Evaluation and Quick Access to Application Manager," on page 17. To fully configure the Connector, you must run the setup wizard after you complete the initial configuration wizard.

Start the Initial Configuration Wizard

Draft comment filepath: GUID-1DEBE4FA-1BEB-48B1-8243-60C44AA3F688.xml

You start the initial configuration wizard by providing the activation code on the first page of the wizard.

The Configuration page is the first page of the initial configuration wizard. If you previously saved a configuration of the Connector, you can import that configuration now instead of running the initial configuration wizard.

Prerequisites

Verify that the following conditions are met:

- You have the authentication code for the Connector.
- You have the relevant information about your Active Directory server.

Procedure

1 In the Activation Code text box, paste your account activation code.

2 If you want to use SSL protocol for user authentication, check the **Use SSL** checkbox.

During the proof-of-concept phase of configuration, you might not want to configure SSL.

3 Click **Next** to continue to the next page of the initial configuration wizard.

NOTE If an error message appears indicating that the Connector cannot connect to a specified URL, see "Error Message Appears After You Provide the Connector Activation Code," on page 54.

When you complete the initial configuration wizard, if you deployed Application Manager in Connector Authentication mode, you, as the administrator have quick-access to the Connector. See "Evaluation and Quick Access to Application Manager," on page 17. You can keep the configuration in the quick-access state or you can run the setup wizard from the **About** page to fully configure the Connector.

Configure Active Directory

You configure the Directory page to establish a connection to active Directory, which is used to verify users credentials when they attempt to log in to Application Manager.

NOTE If your deployment uses a multidomain Active Directory Domain Service (AD DS) forest, see "Overview of Configuring the Connector for a Multidomain Active Directory Domain Service Forest," on page 46

Server Host	The text box for the Active Directory host address.
Use SSL	The check box to enable the secure sockets layer (SSL) cryptographic protocol to connect to your Active Directory.
Server Port	The text box for the port number for the Active Directory host. For a single domain Active Directory Domain Service, the default port for LDAP is 389 while the default port for LDAP over SSL is 636. For a multidomain Active Directory Domain Service (AD DS) forest, the default ports for the global catalog are 3268 without SSL and 3269 with SSL.
Search Attribute	The drop-down menu for the Active Directory attribute that contains the username. For a single domain Active Directory Domain Service, the appropriate selection is sAMAccountName. For a multidomain Active Directory Domain Service (AD DS) forest, the appropriate selection is userPrincipalName.
Base DN	For a single domain Active Directory Domain Service, this is the text box for the Distinguished Name (DN) of the starting point for directory server searches. For example: DC=mycompany,DC=com. The Connector starts from this DN to create master lists from which you can later filter out individual users and groups. For a multidomain Active Directory Domain Service (AD DS) forest, the appropriate action is to leave this text box blank.
Bind DN	The text box for the full distinguished name (DN), including common name (CN), of an Active Directory user account that has privileges to search for users. For example: CN=Administrator,CN=Users,DC=mycompany,DC=com. This user account must have at least domain user privileges. **NOTE** The Bind DN user, such as Administrator, is the username associated with the Bind DN user account. The Connector creates a corresponding user account as an administrative user in Application Manager. You use the username for this account to log in to Application Manager as an administrator. For a single domain Active Directory Domain Service, the Bind DN entry must be located in the same branch and below the Base DN. For a multidomain Active Directory Domain Service (AD DS) forest, because you leave the Base DN text box empty, the restrictions that apply for a single domain do not apply for a multidomain forest.
Bind Password	The text box for the Active Directory password for the account that can search for users. **NOTE** The Bind password is the same password used in association with the Bind DN user account.

In the initial setup wizard, when you complete the Directory page, by clicking **Verify**, the About page appears.

If you deployed Application Manager in Connector Authentication mode, the Connector is now in the quick-access state. See "Evaluation and Quick Access to Application Manager," on page 17. At this point, you have access to Application Manager for evaluation purposes. You can start the setup wizard when you are ready to fully configure the Connector.

To fully configure the Connector, for example to enable Directory Sync, click **Setup Wizard**. See "Configuring the Connector with the Setup Wizard," on page 32.

Configuring the Connector with the Setup Wizard

Draft comment filepath: GUID-72A26AB6-7F39-48EB-9B25-11364C1DF8C3.xml

Use the setup wizard to fully configure the Connector and enable features not provided with quick-access configuration, such as Directory Sync. After you use the setup wizard, it is no longer accessible unless you reset the Connector configuration.

The setup wizard helps you to configure the connection between the Connector, Application Manager, and Active Directory. Also, if you want to provide Application Manager users with access to Windows applications captured as ThinApp packages, you can make many of the required configurations in the setup wizard. After you configure these items, you can use the Application Manager Administrator Web interface to configure Application Manager. You can return to the Connector at any time to make further configurations.

Start the Setup Wizard

Draft comment filepath: GUID-A09563F6-D4AA-4F2E-BFA9-B351D64DAEFE.xml

After you complete the initial configuration wizard, you are on the About page, from which you can start the setup wizard. The default behavior of the setup wizard pages is for changes to take effect when you continue to the next page.

Prerequisites

Verify that the following conditions are met:

- If applicable, you have the relevant information about the user in Active Directory who has the right to join machines to the Active Directory domain.
- If applicable, you have the relevant information about your Kerberos key distribution center (KDC).
- If applicable, you have the relevant information about your ThinApp package repository.

Procedure

- On the About page, click **Setup Wizard**.

Once you complete the setup wizard, the key features of the Connector, such as Directory Sync, are configured. However, depending on your deployment, you can expect further configuration to be required, such as for logging and sync safeguards.

Configure Join Domain

Draft comment filepath: GUID-3BD2F13F-1EA8-47E5-BEFA-2570C5708BE6.xml

If you are configuring the Connector in Connector Authentication mode, you can configure the join domain functionality. You have the option of configuring join domain functionality in the setup wizard or you can skip the Join Domain page of the wizard and configure the Join Domain page later on the **Advanced** tab.

You must enable join domain functionality if you want to provide users with access to Windows applications captured as ThinApp packages or to provide single sign-on to the User Portal using Windows authentication (Kerberos). Otherwise, join domain functionality is not needed.

The Active Directory information that you provide for the Join Domain page is for the user who has the right to join machines to the Active Directory domain.

AD FQDN	The text box for the fully qualified domain name of an Active Directory instance. The domain name you enter must be the same Windows domain on which the Connector resides
AD Username	The text box for the username associated with the user account that has the right to join machines to the Active Directory domain
AD Password	The text box for the password associated with the user account has the right to join machines to the Active Directory domain
Join Domain/Leave Domain	The button to join and leave the domain. The wording on the button changes to and from Join Domain and Leave Domain depending on if you last joined or left the domain

Enabling Windows Authentication

Draft comment filepath: GUID-3E4D2C35-0F8A-4E4A-A84F-3C0BE785C5D9.xml

If you are configuring the Connector in Connector Authentication mode, you can enable Windows authentication (Kerberos). You have the option of enabling Windows authentication in the setup wizard or you can skip the Windows Authentication page of the wizard and configure the Windows Authentication page later on the **Advanced** tab.

For an overview of configuring Kerberos with Application Manager, see "Overview of Configuring Windows Authentication (Kerberos) for the Connector," on page 41.

You must enable Windows authentication to allow the Kerberos protocol to secure interactions between users' browsers and Application Manager. Enabling Windows authentication is required if you want to provide Application Manager users access to Windows applications captured as ThinApp packages.

Prior to enabling Windows authentication on this page, you must join the Connector to the Active Directory domain on the Join Domain page.

Enable Windows Authentication	The check box to extend authentication interactions between users' browsers and Application Manager
Enable Redirect	The check box that enables the Connector to redirect users' browsers to the correct Connector instance. Uncheck the Enable Redirect check box if your load balancer supports Kerberos authentication. Windows authentication requires users' browsers to request authentication using the proper hostname. When multiple Connector instances are behind a load balancer, Application Manager uses the hostname of the load balancer in the initial authentication request. If the load balancer is not configured to redirect users' browsers to the selected Connector instance, the Connector instance itself must perform the redirect. Select the Enable Redirect check box to enable the Connector to perform this redirect.

Configure Internal Access

Draft comment filepath: GUID-4240FB9B-A947-452A-9218-3F2F4198F11D.xml

You provide the hostname or IP address of the Connector virtual appliance to allow trust between the Connector and Application Manager, which enables the exchange of SAML metadata.

Use SSL	The box to check to use SSL for end-user authentication. This provides SSL for users authenticated in Connector Authentication mode. For the proof-of-concept phase of deployment, you can leave this box unchecked.
Internal host	The text box for the internal hostname or IP address of the Connector virtual appliance

Configure External Access

Draft comment filepath: GUID-147880E3-ECDF-4846-A6E0-CCBA103DE7F0.xml

Configuring external access includes providing a hostname or IP address that is accessible from the public Internet and configuring the SSL certificate information. The Connector includes a preinstalled self-signed certificate.

During the initial configuration of the Connector on the External Access page of the setup wizard, update the SSL certificate.

Caution If you are deploying the Connector in Service Authentication mode, you can continue to use the self-signed certificate. If you are deploying the Connector in Connector Authentication mode, update the SSL certificate to a certificate signed by a trusted certificate authority to avoid untrusted connection security warnings from appearing in users' browsers.

To use a certificate signed by a trusted certificate authority, see "Overview of Using Trusted SSL Certificates on the Connector," on page 45

External host	The text box for a hostname or IP address that is a public DNS accessible from the public Internet
SSL certificate	The text box for the SSL certificate. If you are using an SSL certificate issued by a trusted certificate authority, you paste the SSL certificate here
Private key	The text box for the private key that corresponds with the SSL certificate. The private key, like the SSL certificate, is applicable to the use of an SSL certificate issued by a trusted certificate authority. You paste the private key here
Generate SSL Certificate	The clickable text that regenerates the SSL certificate and key, ensuring that your Connector instance has a unique SSL certificate. You might choose this option if you want to use a self-signed certificate in production. The new key takes effect when you restart the system

Configure Windows Apps

Draft comment filepath: GUID-08A4660B-0781-4C67-92B9-32485C86F569.xml

In the setup wizard, you can provide Application Manager users with access to Windows applications captured as ThinApp packages. You also have the option of skipping the Windows Applications page in the wizard and configuring the Windows Applications page later on the **Advanced** tab.

Providing Application Manager users access to ThinApp packages requires a variety of other configurations. See "Installation and Configuration Flow of the Connector Integrated with ThinApp," on page 7 for information about the configurations required to integrate Application Manager with ThinApp.

Enable Windows Apps	The check box to enable Application Manager users access to ThinApp packages
Path	The text box for the path to the Windows applications network share. For example: `\\DirectoryHost\ThinAppFileShare` **Caution** For *DirectoryHost*, provide the hostname, not the IP address.
Scheduling	The drop-down list of options for how often the Connector synchronizes the information about ThinApp packages in the Windows applications network share with Application Manager.

Map User Attributes

Draft comment filepath: GUID-4D6C742C-C749-4B45-B089-E6C239D5CEB1.xml

The attribute name for each text box must match the names that Active Directory uses.

Note If your deployment uses a multidomain Active Directory Domain Service (AD DS) forest, see "Overview of Configuring the Connector for a Multidomain Active Directory Domain Service Forest," on page 46

The attribute names used in these text boxes, such as sn for last name, are standard LDAP attribute names.

You use the **Add an attribute** option to create attributes.

CAUTION Do not add multi-valued attributes. Application Manager does not support multi-valued attributes, such as memberOf. However, Active Directory group membership information is synchronized with Application Manager. Refer to "Select Groups," on page 36 for more information on synchronizing Active Directory groups.

If your deployment uses a multidomain Active Directory Domain Service (AD DS) forest, the Active Directory attribute that contains the username is userPrincipalName. On the Map User Attributes page, the Horizon userName attribute should be mapped to the Directory userPrincipalName attribute. This mapping should occur automatically since the userPrincipalName value is carried forward from the Directory page. Do not change this value from userPrincipalName. You can add attributes on this page, but If your deployment uses a multidomain Active Directory Domain Service (AD DS) forest, you should only add attributes that are stored in the global catalog. If you want to synchronize a special user attribute, such as. employeeID with Horizon, you must first add the attribute to the global catalog.

Select Users

Draft comment filepath: GUID-57CBEB92-E957-402B-BBDE-AB1A10DC67F4.xml

You can determine which Active Directory users are synchronized with Application Manager.

NOTE If your deployment uses a multidomain Active Directory Domain Service (AD DS) forest, see "Overview of Configuring the Connector for a Multidomain Active Directory Domain Service Forest," on page 46

Filter Users Tab

Draft comment filepath: GUID-57CBEB92-E957-402B-BBDE-AB1A10DC67F4.xml

The Filter Users tab is the default tab of the Select Users page. Use this tab to select and exclude the Active Directory users that will be transferred to Application Manager during each synchronization.

Enter the DN for Users	The text box for the DN for users. The value you provided as the Base DN on the Directory page of the setup wizard serves as the default value for this text box. You can change the value and you can add distinguished names (DN), with the **Add another** button, to include all of the users to transfer as part of the synchronization process from Active Directory to Application Manager. You can check the results on the **View Results** tab. If your deployment uses a multidomain Active Directory Domain Service (AD DS) forest, this text box is not prepolulated. You must add all the DNs from all the domains from your AD DS forest that you want to include. You can apply filters to include specific users. You have the flexibility of using an inclusion filter instead of using numerous exclusion filters to obtain the same result. Apply an inclusion filter in the following manner: 1 Edit the DN information for users and specify an Inclusion filter. 2 Append a semicolon to the user base DN that you want to filter. For example, if the Base DN for all users in your Active Directory is `ou=Users,DC=testDC,DC=examplecompany,DC=com` and you want to sync users in the Sales department to the Connector, edit the DN information to include the following attributes: `ou=Users,DC=testDC,DC=examplecompany,DC=com; (&(objectClass=user) (objectCategory=person)( department=Sales))`
Apply Filters to Exclude Users	The section for creating filters to exclude users. You can select an Active Directory attribute with which to filter out any names listed on the **View Results** tab that you do not want synchronized between Active Directory and Application Manager. You can apply as many filters as necessary until the desired list of users appears in the **View Results** tab.
Refresh Results	The clickable text that allows you to update the list of users on the **View Results** tab.

View Results Tab

Draft comment filepath: GUID-57CBEB92-E957-402B-BBDE-AB1A10DC67F4.xml

The View Results tab provides a list of users to be synchronized between Active Directory and Application Manager.

View Errors Tab

Draft comment filepath: GUID-57CBEB92-E957-402B-BBDE-AB1A10DC67F4.xml

The **View Errors** tab provides a list of user entries with errors. User information to be transferred from Active Directory must include username, first name, last name, email address, and any of the required extended attributes. Otherwise, that user entry appears in the View Errors list and is not transferred to Application Manager.

Select Groups

Draft comment filepath: GUID-AD1F3DB0-5A74-4802-8C41-CA207F4015DF.xml

You can select the group information in Active Directory to be imported to Application Manager during synchronization.

NOTE If your deployment uses a multidomain Active Directory Domain Service (AD DS) forest, see "Overview of Configuring the Connector for a Multidomain Active Directory Domain Service Forest," on page 46

Enter DN for Groups	The section that allows you to add Active Directory groups to the Selected Groups section. The value you provided as the Base DN on the Directory page of the setup wizard serves as the default DN from which group searches begin. Edit this value as needed. You must click the Add link next to a group name, to add that group to the Selected Groups list. If your deployment uses a multidomain Active Directory Domain Service (AD DS) forest, this section must contain multiple group DNs. Text boxes for group DNs are automatically pre-populated with values from the Select Users page. You can only use universal groups. If you want to synchronize special local or global group membership information with Application Manager, you must change the scope of the group to universal.
Selected Groups	The section that lists Active Directory groups to be pushed to Application Manager during synchronizations. After you add a group to the Selected Groups list, information for that group is exported to Application Manager each time Active Directory synchronizes with Application Manager. You can edit the Application Manager name for a group as necessary for easy recognition.

Configure Scheduling

Draft comment filepath: GUID-8F092123-78D5-48FC-8EEC-B24D38BBACF7.xml

You can configure how often Active Directory synchronizes with Application Manager.

You can schedule a synchronization to occur as frequently as every hour and as infrequently as once a week.

Push to Application Manager

Draft comment filepath: GUID-D357A4B8-C263-488F-BAD8-034281394292.xml

You can use the Push to Application Manager page to review the number of Active Directory users and groups to be added, updated, or deleted according to the changes you have made in the Connector Web interface.

You click **Save and Continue** to synchronize Active Directory with Application Manager.

When the Setup is complete message appears, you can select your next action.

Log in to Horizon	The link that allows you to continue to Application Manager. To configure Application Manager you must log in as an administrator
View or edit Connector settings	The link that allows you to return to the Connector to view or edit Connector settings

5 Configuring the Connector

Draft comment filepath: GUID-69D37AA1-EA34-4B22-B83D-B953BED919A5.xml

After you configure the Connector and access Application Manager, you can return to the Connector for further configuration.

After you install the Connector and obtain access to Application Manager, certain Connector configurations might still be required to make your Application Manager deployment production ready, such as configuring log files and editing the default Directory Sync safeguards.

This chapter includes the following topics:

Configure the Connector for Logging

Draft comment filepath: GUID-2794071E-89EB-4ECD-8341-855CDEA04097.xml

You can configure logs in the Connector virtual appliance interface. You configure Web server logging behavior in the `log4j.xml` file. To store logging information externally, you can configure an external syslog server.

By default, the Connector logs Web-server related information and ThinApp-package related information as such:

- Web server log file: `/opt/vmware/c2/c2instance/logs/connector.log`.
- ThinApp-package related log file: `/var/log/messages`.

You can edit the log configuration files to control where the Connector stores the log information.

Log Configuration File	Filepath	Information
`log4j.xml`	`/opt/vmware/c2/c2instance/webapps/ROOT/WEB-INF/classes/log4j.xml`	Web server logs rotate with a default size of 50MB as configured in the `log4j.xml` file. By default, these logs are stored in `/opt/vmware/c2/c2instance/logs/connector.log`. For more details about the Web server logging behavior, see the `log4j.xml` file. The Web server logging behavior is preconfigured and might not require any further configuration.
`syslog`	`/etc/syslog-ng/syslog-ng.conf`	Configure the `syslog-ng.conf` file to direct logs to your external syslog server.

The best practice is to store program logs in an external syslog server.

For more information about editing `log4j` files, see Apache documentation on Apache Logging Services.

Prerequisites

Verify that an external syslog server is installed, configured, and accessible.

Procedure

1 Access the Connector virtual appliance interface.

2 Select **Login** and log in to the SLES operating system.

3 Use the appropriate commands to access and configure the `log4j.xml` file to send logs to syslog internally.

4 Use the appropriate commands to access and configure the `syslog-ng.conf` file to send logs to an external syslog server.

After you configure the log configuration files, the new logging behavior takes effect.

Configure Directory Sync Safeguards

Draft comment filepath: GUID-16A4231A-79FD-4FA0-8186-562E3C595714.xml

Once the Connector setup wizard is configured, you can set the directory synchronization safeguards to help prevent unintended changes to Application Manager users and groups.

A change to Application Manager users and groups can be a reflection of changes to Active Directory or to the Connector directory-related Web pages, such as the Select Users page. The safeguards allow you to monitor relatively large changes to Application Manager users and groups. If any directory safeguard trigger condition is met, the directory synchronization is prevented. An alert is issued in such a case that explains why the synchronization did not take place and what your options are. When you first configure the Connector, you should review the default triggers to determine if they are sufficient.

Prerequisites

You must complete the Connector setup wizard before you can edit the default directory sync safeguards.

Procedure

1 In the Connector Web interface, access the Sync Safeguards page on the **Advanced** tab.

2 Review the percentages for each trigger condition and edit as needed.

Overview of Configuring SecurID

Draft comment filepath: GUID-8D29356B-48C5-43AC-A0B4-48D2D1A2D254.xml

Configuring RSA SecurID server (RSA Authentication Manager, formerly ACE/Server) includes a set of tasks for the Connector that involves the RSA SecurID server and the Connector Web interface.

Purpose of using RSA SecurID with Application Manager

Draft comment filepath: GUID-8D29356B-48C5-43AC-A0B4-48D2D1A2D254.xml

After you deploy Application Manager in Connector Authentication mode, you can configure SecurID to provide additional security. See "Connector Authentication Mode and RSA SecurID," on page 13.

Configure the Network

Draft comment filepath: GUID-8D29356B-48C5-43AC-A0B4-48D2D1A2D254.xml

You must ensure your network is properly configured for your Application Manager deployment. For SecurID specifically, you must ensure that the appropriate port is open to enable SecurID to authenticate users outside the enterprise network. See the port information related to SecurID in Table 2-3.

Prepare RSA SecurID Server

Draft comment filepath: GUID-8D29356B-48C5-43AC-A0B4-48D2D1A2D254.xml

After you run the Connector setup wizard, you have all the information necessary to prepare the RSA SecurID server. See "Prepare the RSA SecurID Server for the Connector," on page 39.

Configure SecurID with the Connector Web Interface

Draft comment filepath: GUID-8D29356B-48C5-43AC-A0B4-48D2D1A2D254.xml

After you prepare the RSA SecurID server for the Connector, you use the Connector Web interface to configure the SecurID page. See "Configure SecurID with the Connector Web Interface," on page 40.

Configure the IP Address Range in the Application Manager Administrator Web interface

Draft comment filepath: GUID-8D29356B-48C5-43AC-A0B4-48D2D1A2D254.xml

After you complete the configuration of SecurID with the Connector Web interface, you log in to Application Manager as an administrator to configure IdP Discovery, which involves providing IP address ranges for users' systems. See "IdP Discovery," on page 15 for more information about IdP Discovery, including an example specific to SecurID.

Prepare the RSA SecurID Server for the Connector

Draft comment filepath: GUID-A7233BCC-29D8-4555-B6AD-C38C86F8EE31.xml

If you are deploying the Connector in Connector Authentication mode and you want to provide security with RSA SecurID, prepare the RSA SecurID server for the Connector.

See "Overview of Configuring SecurID," on page 39 for an overview of using RSA SecurID with Application Manager.

Important After you restart the RSA SecurID server, the system takes time to become operational. Wait time can vary, but expect from several minutes to half an hour of delay before the system can process authentication requests from the Connector.

The following steps focus on the Connector-specific information necessary to configure the Connector with RSA SecurID. For detailed information about configuring the RSA SecurID server, see RSA documentation.

Prerequisites

- Verify that one of the following RSA Authentication Manager versions is installed and functioning on the enterprise network to allow communication with the Connector: 6.1.2, 7.1 SP2, or 7.1 SP3.

  Application Manager uses AuthSDK_Java_v8.1.1.312.06_03_11_03_16_51 (Agent API 8.1 SP1), which only supports the preceding versions of RSA Authentication Manager (the RSA SecurID server). For information about installing and configuring RSA Authentication Manager (RSA SecurID server), see RSA documentation.

- Install and configure the Connector. After you install the Connector and use the Connector Web interface to run the setup wizard, you have the information necessary to prepare the RSA SecurID server.

Procedure

1 On a supported version of the RSA SecurID server, add the Connector as an authentication agent.

  You are prompted for the following Connector-related information when you add the Connector as an agent.

Prompt	Enter
Hostname	The hostname of the Connector.
IP address	The IP address of the Connector.
Alternate IP Address	If traffic from the Connector passes through a network address translation (NAT) device to reach the RSA SecurID server, enter the private IP address of the Connector.

  Be prepared to provide this information again in the Connector Web interface, when you configure the SecurID page, which is available on the **Advanced** tab.

2 Download the compressed configuration file and extract the `sdconf.rec` file.

  Download the compressed file from the RSA SecurID server and extract the server configuration file, which by default is named `sdconf.rec`. Be prepared to upload this file later with the Connector Web interface, when you configure the SecurID page, which is available on the **Advanced** tab.

What to do next

Using the Connector Web interface, configure the SecurID page, which is available on the **Advanced** tab.

Configure SecurID with the Connector Web Interface

Draft comment filepath: GUID-28B16D8D-CDBF-4543-BF11-44F036EC825E.xml

Once the Connector setup wizard is configured, you can configure the SecurID page.

Prerequisites

Verify that RSA Authentication Manager (the RSA SecurID server) is installed and properly configured. For more information about configuring SecurID for Application Manager, see "Overview of Configuring SecurID," on page 39.

Procedure

1 Access the SecurID page on the **Advanced** tab.

2 Click the **Enable SecurID** check box.

3 Configure and save the SecurID page.

Information used and files generated on the RSA SecurID server are required when you configure the SecurID page. See "Prepare the RSA SecurID Server for the Connector," on page 39.

Connector Address	Enter the appropriate Connector IP address. The value you enter matches a value you used to configure the RSA SecurID server when you added the Connector as an authentication agent. If your RSA SecurID server has a value assigned to the **Alternate IP Address** prompt, enter that value as the Connector IP address. If no alternate IP address is assigned, enter the value assigned to the **IP Address** prompt instead.
Agent IP Address	Enter the value assigned to the **IP Address** prompt in the RSA SecurID server.
Server Configuration	Upload the server configuration file. First, you must download the compressed file from the RSA SecurID server and extract the server configuration file, which by default is named `sdconf.rec`.
Node Secret	Leaving the node secret blank allows the node secret to autogenerate. Therefore, the recommended action is to clear the node secret file on the RSA SecurID server and to intentionally not upload the node secret file to the Connector. Ensure that the node secret file on the RSA SecurID server and on the Connector always match. If you change the node secret at one location, change it respectively at the other location. For example, if you clear or generate the node secret on the RSA SecurID server, clear or upload the node secret file accordingly on the Connector.

What to do next

Log in to Application Manager Administrator Web interface to configure the IdP Discovery feature. See "IdP Discovery," on page 15.

Overview of Configuring Windows Authentication (Kerberos) for the Connector

Configuring Kerberos for the Connector involves installation, and possibly configuration tasks. Kerberos authentication provides another layer of security for your Application Manager deployment.

Active Directory Configuration

Starting with Application Manager 1.5, you do not need to directly configure Active Directory to make Kerberos function with your Application Manager deployment.

Connector Installation

After you install the Connector, you use the Connector Web interface to enable the Connector to use Kerberos authentication by first joining the domain on the Join Domain page and then by enabling Windows Authentication on the **Windows Authentication** page. You can configure these pages in either the setup wizard or on the **Advanced** tab. See "Configure Join Domain," on page 32 and "Enabling Windows Authentication," on page 33.

Kerberos Authentication Operating System Support

Currently, interactions between users' browsers and Application Manager are authenticated by Kerberos on Windows operating systems only. Accessing Application Manager from other operating systems does not does not take advantage of Kerberos authentication.

Browser Configuration

Draft comment filepath: GUID-06C5BDE5-5160-4488-A5DF-B9FFD931EFD6.xml

The following browsers, on Windows only, are supported for accessing Application Manager in Kerberos authentication:

- Firefox: Additional configuration is required for each user's browser. See "Configure Firefox to Access the User Portal," on page 43.
- Internet Explorer: Additional configuration is required for each user's browser. See "Configure Internet Explorer to Access the User Portal," on page 42.
- Chrome: Additional configuration is required for each user's browser. See "Configure the Chrome Browser to Access the User Portal," on page 44.

Kerberos Troubleshooting

Draft comment filepath: GUID-06C5BDE5-5160-4488-A5DF-B9FFD931EFD6.xml

See "Troubleshoot Kerberos," on page 55.

Configure Internet Explorer to Access the User Portal

Draft comment filepath: GUID-18656F18-5A7D-4BB1-AF9B-36DDEFC602BD.xml

You must configure the Internet Explorer browser if Kerberos is configured for your Application Manager deployment and you want to provide users access to the User Portal using Internet Explorer.

Kerberos authentication works in conjunction with Application Manager on Windows operating systems. Do not implement these Kerberos-related steps on other operating systems.

Prerequisites

Configure the Internet Explorer browser, for each user, or provide users with the instructions, after you configure Kerberos. See "Overview of Configuring Windows Authentication (Kerberos) for the Connector," on page 41.

Procedure

1 Verify that you are logged in to Windows as a user in the domain.

2 In Internet Explorer, enable automatic log on.

   a Select **Tools > Internet Options > Security**.

   b Click **Custom level**.

   c Select **Automatic login only in Intranet zone**.

   d Click **OK**.

3 Verify that this instance of the Connector is part of the local intranet zone.

   a Use Internet Explorer to access the Connector login URL at https://*ConnectorHost*.*DomainName*/authenticate/.

   For example, https://ConnectorHost.mycompanyintranet.com/authenticate/.

   b Locate the zone in the bottom right corner on the status bar of the browser window.

   If the zone is Local intranet, Internet Explorer configuration is complete.

4 If the zone is not Local intranet, add the Connector to the intranet zone.

   a Select **Tools > Internet Options > Security > Local intranet > Sites**.

   b Select **Automatically detect intranet network**.

   If this option was not selected, selecting it might be sufficient for adding the Connector to the intranet zone.

   c (Optional) If you selected **Automatically detect intranet network**, click **OK** until all dialog boxes are closed.

   d In the Local Intranet dialog box, click **Advanced**.

   A second dialog box named Local intranet appears.

   e Type the Connector URL in the Add this Web site to the zone text box.

   For example, https://ConnectorHost.mycompanyintranet.com.

   f Click **Add**.

   g Click **Close** to close the second Local intranet dialog box.

   h Click **OK** to close the first Local intranet dialog box.

5 Verify that Internet Explorer is allowed to pass the Windows authentication to the trusted site.

   a In the Internet Options dialog box, click the **Advanced** tab.

   b Select **Enable Integrated Windows Authentication**.

   This option takes effect only after you restart Internet Explorer.

   c Click **OK**.

6 Log in to the Connector login URL at https://*ConnectorHost*.*DomainName*/authenticate/ to check access.

   For example, https://ConnectorHost.mycompanyintranet.com/authenticate/.

   If Kerberos authentication is successful, the test URL goes to the User Portal.

The Kerberos protocol secures all interactions between that Internet Explorer browser instance and Application Manager. Users then have single sign-on access to Application Manager.

Configure Firefox to Access the User Portal

Draft comment filepath: GUID-E55B5C69-05CB-41CA-9EC3-8430BDC8EA1B.xml

You must configure the Firefox browser if Kerberos is configured for your Application Manager deployment and you want to provide users access to the User Portal using Firefox.

Kerberos authentication works in conjunction with Application Manager on Windows operating systems. Do not implement these Kerberos-related steps on other operating systems.

Prerequisites

Configure the Firefox browser, for each user, or provide users with the instructions, after you configure Kerberos. See "Overview of Configuring Windows Authentication (Kerberos) for the Connector," on page 41.

Procedure

1 In the URL text box of the Firefox browser, type **`about:config`** to access the advanced settings.

2 Click **I'll be careful, I promise!**.

3 Double-click **network.negotiate-auth.trusted-uris** in the Preference Name column.

4 Type your Connector URL in the text box.

The URL to the login page is https://*ConnectorHost.DomainName*.

For example, https://ConnectorHost.mycompanyintranet.com.

5 Click **OK.**

6 Double-click **network.negotiate-auth.delegation-uris** in the Preference Name column.

7 Type your Connector URL in the text box.

For example, https://ConnectorHost.mycompanyintranet.com.

8 Click **OK**.

9 Test Kerberos functionality by using the Firefox browser to log in to the Connector login URL.

For example, https://ConnectorHost.mycompanyintranet.com/authenticate/.

If the Kerberos authentication is successful, the test URL goes to the User Portal.

The Kerberos protocol secures all interactions between that Firefox browser instance and Application Manager. Users then have single sign-on access to Application Manager.

Configure the Chrome Browser to Access the User Portal

Draft comment filepath: GUID-85D10E40-6970-4F4D-8AB2-0580C5CEDAFD.xml

You must configure the Chrome browser if Kerberos is configured for your Application Manager deployment and you want to provide users access to the User Portal using the Chrome browser.

Kerberos authentication works in conjunction with Application Manager on Windows operating systems. Do not implement these Kerberos-related steps on other operating systems.

Prerequisites

- Configure Kerberos. See "Overview of Configuring Windows Authentication (Kerberos) for the Connector," on page 41.
- Since Chrome uses the Internet Explorer configuration to enable Kerberos authentication, you must configure Internet Explorer to allow Chrome to use the Internet Explorer configuration. Follow the instructions in "Configure Internet Explorer to Access the User Portal," on page 42.

Procedure

- Test Kerberos functionality by using the Chrome browser to log in to the Connector login URL.

  For example, https://ConnectorHost.mycompanyintranet.com/authenticate/.

  If either Kerberos authentication is successful, the test URL goes to the User Portal.

If all related Kerberos configurations are correct, the relative protocol (Kerberos) secures all interactions between that Chrome browser instance and Application Manager. Users then have single sign-on access to Application Manager.

Provide User Access to Application Manager

Draft comment filepath: GUID-96399511-9399-4810-ACF2-AA21F3F2F76E.xml

After you configure the Connector and Application Manager, you must provide users with a URL to access the User Portal. You can also provide URLs for individual applications that are available in the User application catalog.

See Chapter 1, "Introduction to Application Manager," on page 9 for information about the URLs to provide users. The following sections might apply depending on how you configure the Connector:

- "Connector Authentication Mode," on page 12
- "Service Authentication Mode," on page 14
- "IdP Discovery," on page 15

Overview of Using Trusted SSL Certificates on the Connector

Draft comment filepath: GUID-89CEAD1D-3227-4EBA-BF6A-B5AAFAF10D94.xml

After you complete the setup wizard, you can visit the External Access page on the **Advanced** tab to update the SSL certificate.

Trusted SSL Certificate

Draft comment filepath: GUID-89CEAD1D-3227-4EBA-BF6A-B5AAFAF10D94.xml

If you deploy the Connector in Connector Authentication mode, you must update the SSL certificate to a certificate signed by a trusted certificate authority to avoid untrusted connection security warnings from appearing in users' browsers. You must restart the system for the new key to take effect, allowing users to authenticate to Application Manager. See "Configure External Access," on page 34

Intermediate SSL Certificates

Draft comment filepath: GUID-89CEAD1D-3227-4EBA-BF6A-B5AAFAF10D94.xml

When you use a trusted Certificate Authority, in most cases, at least one intermediate certificate authority (CA) exists between your Connector SSL certificate and the trusted root CA. If one or more intermediate CAs exist for your Connector SSL certificate, you must update the Connector. See "Include Intermediate SSL Certificates Signed by a Trusted Certificate Authority," on page 45

Include Intermediate SSL Certificates Signed by a Trusted Certificate Authority

Draft comment filepath: GUID-CD12233A-8E6B-4EE5-9CC9-7C0F6C1DF453.xml

If you are installing an SSL certificate for the Connector that uses at least one intermediate certificate authority (CA) between your Connector SSL certificate and the trusted root CA, you must manually update the Connector.

This task requires you to combine the certificate and its corresponding chain into a single file. The file with the combined certificate information interacts with the private key in the keystore to allow the Web server to present the appropriate certificate upon request.

Prerequisites

- Obtain the Connector certificate, for example `ConnectorCert.Trusted.pem`, and the certificate chain, for example `CertChain.pem`, that lead to a trusted root CA.
- Use the **External Access** page in the **Advanced** tab to load the Connector SSL certificate and corresponding private key. See "Configure External Access," on page 34. This action loads the private key in the keystore, `tcserver.keystore`.

Procedure

1 In the Connector virtual appliance interface, select Login and log in to the command line of the Linux operating system.

2 Make the combined file available in the Connector virtual appliance.

You can decide where to download and combine the certificates. However, you must make the combined file available in the Connector virtual appliance. For example you can combine files in a temporary directory with the following command: `cat ConnectorCert.Trusted.pem CertChain.pem > FullChain.pem`

IMPORTANT Verify that you combine the certificates in the correct order. The order is meaningful.

3 Use the command line to load the combined certificate file into the keystore.

For example: `keytool –import –trustcacerts –alias tcserver –file FullChain.pem –keystore /opt/vmware/c2/c2instance/conf/tcserver.keystore –storepass changeme`

This combined certificate replaces the certificate you previously loaded with the Connector Web interface.

4 Use the command line to restart the Apache Tomcat Web server.

For example: `/etc/rc.d/tcserver–c2 restart`.

The SSL certificate for the Connector and the intermediate certificates are now combined in a single file. This allows the establishment of trust between the Connector and users' browsers.

Overview of Configuring the Connector for a Multidomain Active Directory Domain Service Forest

Draft comment filepath: GUID-91CAFCD0-301C-4C19-A8F3-E7B96F875D83.xml

If your deployment uses a multidomain Active Directory Domain Service (AD DS) forest, you must base the Connector configuration on the Active Directory global catalog instead of on LDAP.

Active Directory Global Catalog

Draft comment filepath: GUID-91CAFCD0-301C-4C19-A8F3-E7B96F875D83.xml

The global catalog is a distributed data repository that contains a searchable, partial representation of every object in every domain in a multidomain AD DS forest. The global catalog is stored on domain controllers that have been designated as global catalog servers. The global catalog is distributed through multimaster replication.

Searches that are directed to the global catalog are faster because they do not involve referrals to different domain controllers. A global catalog server is a domain controller that, in addition to its full, writable domain directory partition replica, also stores a partial, read-only replica of all other domain directory partitions in the forest. The additional domain directory partitions are partial because only a limited set of attributes is included for each object. By including only the attributes that are most used for searching, every object in every domain in even the largest forest can be represented in the database of a single global catalog server.

The global catalog is built and updated automatically by the AD DS replication system. The attributes that are replicated to the global catalog are identified in the schema as the partial attribute set (PAS) and are defined by default by Microsoft. However, to optimize or extend searching, you can edit the schema by adding or removing attributes that are stored in the global catalog.

Access to a global catalog server is required for successful user authentication. If a global catalog server is not available, the user login fails. The global catalog stores the membership (the member attribute) of only universal groups. You can change the scope of a group from local domain or global to universal.

By using different ports for standard LDAP queries (ports 389, 636) than for global catalog queries (ports 3268. 3269), AD DS effectively separates forest-wide queries that require a global catalog server from local, domain-wide queries that can be serviced by the domain controller in the user's domain.

Users must log in to Application Manager with a user principal name (UPN). When a user account is created, the UPN suffix is generated by default as userName@DnsDomainName, but you as an administrator can change this default setting.

For example, in a forest that has four domains, the UPN suffix might be configured to map to the external DNS name for the organization. The userPrincipalName attribute of the user account in Active Directory identifies the UPN and is replicated to the global catalog.

Connector Installation

The installation and configuration of the Connector is similar for an AD DS forest scenario as it is for a single domain scenario. However, you must configure a few of the Connector Web interface pages differently when your deployment uses an AD DS forest.

You can reference the links that follow for instructions to specific Connector Web interface pages. Instructions specific to an AD DS forest scenario are integrated into each of these topics. Table 5-1 provides an summary of all the instructions specific to an AD DS forest scenario.

- Directory Page. See "Configure Active Directory," on page 31.
- Map User Attributes Page. See "Map User Attributes," on page 34
- Select Users Page. See "Select Users," on page 35
- Select Groups page. See "Select Groups," on page 36

Table 5-1. Connector Web Interface Configurations Specific to an AD DS Forest.

Connector Web Interface Page	Configurations Specific to an AD DS Forest
Directory (The Directory page is available in the initial configuration wizard and in the **Advanced** tab)	■ Server Port: You enter the global catalog port number. The default ports for the global catalog are 3268 without SSL and 3269 with SSL. ■ Search Attribute: You select userPrincipalName from the drop-down menu. ■ Base DN: You leave the Base DN text box empty.
User Attributes (The Map User Attributes page is available in the setup wizard and from the Directory Sync page)	IMPORTANT On the Map User Attributes page, the Horizon userName attribute should be mapped to the Directory userPrincipalName attribute. This mapping should occur automatically since the userPrincipalName value is carried forward from the Directory page. Do not change this value from userPrincipalName. On the Map User Attributes page, you should only add attributes that are stored in the global catalog. If you want to synchronize a special user attribute, such as employeeID, with Application Manager, you must first add the attribute to the global catalog.
Select Users (The Select Users page is available in the setup wizard and from the Directory Sync page)	On the Select Users page, you can add users from multiple domains of the same AD DS forest by clicking **Add another** in the DN section and providing another DN.
Select Groups (The Select Groups page is available in the setup wizard and from the Directory Sync page)	On the Selected Groups page, multiple group DNs can exist. They are automatically pre-populated with values from the Select Users page. You can only use universal groups. If you want to synchronize special local or global group membership information with Application Manager, you must change the scope of the group to universal.

6 Testing the Connector

Draft comment filepath: GUID-867B911E-C9E8-42A9-8085-E53BD95107C8.xml

You can use the Connector Web interface to perform specific tests to verify that the Connector is functioning properly.

You can perform testing directly in the Connector Web interface.

Test Your Directory Server with the Connector

Draft comment filepath: GUID-2BC9C586-3724-436F-B878-B9018A83AA10.xml

You can use the Connector to verify a username and password.

Procedure

1 While you are logged in as a domain user, go to https://*ConnectorHost*.*DomainName*/authenticate/.

The result of visiting this URL depends on the mode of authentication.

Authentication Mode	Result
Connector Authentication mode	You arrive at the User Portal.
Service Authentication mode	You are prompted for your Active Directory credentials.

2 If you are prompted for your Active Directory credentials, provide your user name and password.

You arrive at the User Portal.

What to do next

If you cannot access Application Manager, troubleshoot the appropriate configuration, such as Active Directory or Kerberos.

7 Troubleshooting the Connector

Draft comment filepath: GUID-D94397B2-F7B5-4448-BB77-99001FA970E7.xml

You can troubleshoot some problems with the Connector directly from the Connector Web interface, while some troubleshooting involves other aspects of your Application Manager deployment.

This chapter includes the following topics:

Potential Network Time Protocol Issue

Draft comment filepath: GUID-60A1A470-DC8D-4037-B614-65E37A60F1F5.xml

As a troubleshooting or preventative procedure, you can check the Connector Network Time Protocol (NTP) configuration.

Problem

The protocols used between Application Manager and the Connector and between the Connector and Active Directory require that the time synchronization of these systems falls within a narrow range. The time settings of these systems might not be synchronized or the time settings might drift out of synchronization. When you installed the Connector virtual appliance, you either used the default NTP configuration, or you reconfigured NTP. See "Configure the Connector with the Connector Virtual Appliance Interface," on page 28 for steps specific to NTP configuration. Also see the following VMware Knowledge Base article on the topic: Timekeeping best practices for Linux guests (KB 1006427).

You can follow the Solution section in the following situations to prevent an NTP-related problem from occurring:

- When you first install the Connector virtual appliance.
- When you modify the networking environment that can affect the ability of the Connector to contact the NTP server.

- When you change the NTP configuration

You can also follow the Solution section to troubleshoot, for example when users cannot access Application Manager.

Cause

The time setting of the Connector virtual appliance is not properly synchronized with an NTP server.

Solution

1 In the Connector virtual appliance interface, select **Configure**.

2 If necessary, access the next page of options, at the prompt, type the number to **NTP Status**, and press Enter.

A new screen appears that provides information about the NTP configuration. The NTP status is listed at the top of the page.

Types of Status Messages	Explanation
Time Server Connection Error	If the status indicates that there is a time server connection error, the NTP configuration is incorrect or the Connector instance is not able to reach an NTP server. You must troubleshoot your configuration to find the cause.
Not Synchronized	The status message is in red text and indicates that the Connector virtual appliance time has drifted by a minute (60,000 milliseconds) or more, or has not polled an NTP server in 30 minutes or more. The NTP configuration is incorrect. Example Causes: ■ A firewall is preventing the Connector instance from reaching an NTP server. ■ The DNS cannot resolve the NTP server. You must troubleshoot your configuration to find the cause.
Synchronized	The status message is in green text and indicates that the Connector virtual appliance has not drifted outside the 60,000 ms range and no more than 30 minutes has passed since the NTP server was last polled. Example: ■ 3ms clock drift, last poll 176 seconds ago. Such a status message verifies that polling of the NTP server and the resetting of clock drift is taking place.
Waiting to Stabilize	The status message is in red text and indicates that the NTP status has not stabilized yet. This should be a temporary state. If the message persists, you must troubleshoot your configuration to find the cause.

3 If a recent change is not reflected on the NTP Status page, type the option to **Restart NTP** and press Return.

NTP configurations can occur slowly. Therefore, you might want to implement this step to force the synchronization.

4 If you determine that the time setting of the Connector virtual appliance is not properly synchronized with an NTP server, check the current NTP configuration of the appliance to verify that the configuration conforms to the guidelines in the referenced KB article.

Inaccurate IP Address Displayed for the Connector

Draft comment filepath: GUID-CA91F95F-1924-4D3A-BD08-F201F1C97CB4.xml

An inaccurate IP address is issued in the Connector virtual appliance interface when you first deploy the appliance.

Problem

The IP address appears as 127.0.0.1.

Cause

The IP address, subnet mask, or gateway might be invalid.

Solution

1 In the Connector virtual appliance interface, select **Configure Network**.

2 Respond to the network prompts to correct the network settings error.

Connector Inaccessible

Draft comment filepath: GUID-3F6F4E5B-4FF2-4C87-BB03-AFEA6E82EA3F.xml

If you cannot access the Connector using the Web interface, you can troubleshoot the problem in a number of ways.

Problem

Using a supported browser to access the Connector fails. The Web interface is not accessible.

Cause

A variety of issues can cause this problem. Use the following suggestions to diagnose the problem.

Ping	Send a ping from your client to the Connector to determine if the Connector is reachable.
Restart	If you recently changed the Connector host name or regenerated the Web server SSL certificate, the Web server might stop responding to requests until the Connector is restarted.
Network Settings	Use the Connector virtual appliance interface to verify that the network settings are correct. See "Inaccurate IP Address Displayed for the Connector," on page 52.
DNS (if applicable)	Use the nslookup or dig command-line tool to look up the DNS name of the Connector.
Routing	Use tracert.exe or traceroute tools to check for a routing problem.
Firewall	Verify that ports 443 and 8443 are allowed between your client and the Connector.

Solution

- Correct the issue according to the cause.

  When you identify a problem, such as an unreachable Connector instance, the possible causes are still many and require expertise in that area, such as networking expertise.

Sync Safeguard Message Appears When Creating New Connector Instance

Draft comment filepath: GUID-88A7A7B7-6A4E-4A0B-B6C6-8810CF5A9F81.xml

If a Sync Safeguard message appears when you create a new instance of the Connector, the account is already configured with a Connector instance.

Problem

A sync safeguard message appears as you complete the setup wizard of a new Connector instance.

Cause

Another Connector instance is configured with Directory Sync enabled. A sync safeguard message for a new Connector instance indicates that the new instance has Directory Sync enabled and that you are attempting to push changes out to Application Manager with the new instance. You should not configure Directory Sync on an additional Connector instance because this can lead to serious synchronization issues.

Solution

1 In the new Connector instance, do not override the safeguard, but return to the Select Users page of the setup wizard.

2 Uncheck the Enable Directory Sync checkbox.

3 Complete the configuration of the new Connector instance.

4 In the instance of the Connector that has Directory Sync enabled, make directory-related changes.

Missing Connector Web Interface Password

Draft comment filepath: GUID-8899836F-E529-4EC2-A097-6026CE74210B.xml

If you no longer have the Connector Web interface password, you can use the Linux command line of the Connector virtual appliance to clear the password, which causes the Connector Web interface to prompt you for a new password.

Problem

You cannot access the Connector Web interface.

Cause

You do not have the Connector Web interface password. For example, you have forgotten or misplaced the password.

Solution

1 Access the Connector virtual appliance interface.

2 Select **Login** and log in to the Linux operating system with root credentials.

3 Use the command line to stop the Apache Tomcat Web server, remove the file that contains the Connector password, and start the Web server again.

For example: `/etc/rc.d/tcserver-c2 stop ; config-admin.json file: rm /var/lib/config-admin.json; /etc/rc.d/tcserver-c2 start`

4 Use a browser to access the Connector Web interface.

The following is an example URL for the Connector: https://ConnectorHost.mycompany.com:8443/admin/.

The Change Password page appears, where you are prompted for a new password.

5 Respond to the password prompts and click **Save.**

A temporary message appears informing you that your password has been successfully changed. You remain on the Change Password page after the password has been updated.

Error Message Appears After You Provide the Connector Activation Code

Draft comment filepath: GUID-AE88A3E9-88E5-41E2-ABB5-BABFB0A1D49D.xml

A networking issue or a self-signed SSL certificate issue might result in an error message that the Connector cannot connect to a specified URL.

Problem

When you first configure the Connector with the Connector Web interface, you must provide a Connector authentication code to continue. When you submit the code, you receive an error message that the Connector cannot connect to a specified URL.

Cause

The cause can be a networking issue or an SSL certificate issue.

Solution

- Troubleshoot the cause of the error.

Potential Cause	Action
Self-Signed Certificate (for Application Manager Appliance only)	■ Verify that you generated a self-signed certificate using the Application Manager Web interface and that you copied the certificate to the relative Connector Instance. See *Installing Application Manager*..
Networking	■ Ensure that the activation code was generated for an organization that currently exists. ■ Verify that no other networking issues exist.

Using a Static Address for the Connector with vCenter Sever Results in an Access Issue

Draft comment filepath: GUID-F2ABCA68-5B5E-4C82-980C-55CF9B0BCFCB.xml

If you use vCenter Server to deploy the Connector using a static IP address and an access issue occurs, a specific misconfiguration might exist.

Problem

Either you cannot access the Administrator Web interface, or if you catch the problem earlier, you realize when you configure the Connector virtual appliance that Applicatiion Manager is using a DHCP IP address instead of the static IP address that you provided when you deployed the virtual appliance.

Cause

You did not configure the respective vCenter Server IP pool correctly. This setting overrides the configurations you made while deploying the virtual appliance. Therefore, when you deploy the Connector virtual appliance, even though you set the IP allocation policy to Fixed and provide a static IP address, the Connector uses a DHCP IP address instead.

Solution

1. Return to vCenter Server and Configure the respective IP Pool to use static IP addresses.
2. Deploy the Connector virtual appliance again, setting the IP allocation policy to Fixed and providing the static IP address for the virtual appliance.

Troubleshoot Kerberos

Draft comment filepath: GUID-6712EDBB-AF6E-4DD8-9D96-2C75FFD3EAE2.xml

You can troubleshoot Kerberos if users cannot access Application Manager or are experiencing difficulty with single sign-on (SSO) using their Windows login.

Problem

Users cannot access Application Manager, or single sign-on access is not functioning.

Cause

Familiarize yourself with the process of installing the Connector with Kerberos authentication. See "Overview of Configuring Windows Authentication (Kerberos) for the Connector," on page 41.

One of the following problems might be affecting your ability to access Application Manager:

- You might need to change the browser configuration.
- System clocks might have a synchronization problem.
- A Kerberos ticket problem might affect single sign-on access. The key distribution center (KDC) might not be distributing tickets for the Connector, your system might be rejecting the ticket, you did not log in to the correct domain, or encryption types might be incompatible.

Solution

Cause	Solution
Users' browsers are not properly configured.	■ See "Browser Configuration," on page 42 for information about configuring users' browsers to use Kerberos authentication.
The clocks for the Connector host, the key distribution center (KDC) host, and client desktops are not correctly synchronized. They must be synchronized within a minute of each other.	1 Access a Network Time Protocol (NTP) server. See "Configure the Connector with the Connector Virtual Appliance Interface," on page 28 for more information about the configuration of an NTP server. 2 From a command window on each machine, run the `net` command: `net time /set`. 3 Compare the results and synchronize the time on the machines if necessary.
Your Windows system does not have a Kerberos ticket that matches the Connector URL.	Use Microsoft Kerbtray to perform diagnostics. ■ Verify that the names and the target on the **Names** tab match the WindowsDesktopSSO configuration on the Connector. ■ On the **Times** tab, check that the time stamp is current for the Kerberos ticket that matches the Connector. Invalid times might indicate a misconfiguration of your KDC. ■ Check the encryption type on the **Encryption types** tab. If your system uses the older DES encryption, verify that all systems allow for it. Some service packs and operating systems from Microsoft remove support for DES.

Index