

Installing and Configuring Horizon Connector

Horizon Connector 1.3.0

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-000753-00

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

Copyright © 2012 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

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

Contents

Installing and Configuring Horizon Connector	5
1 Introduction to Horizon	9
2 Security Concerns and System Requirements for the Connector	17
Connector Recommendations and Requirements	17
3 Preparing to Install the Connector	21
Prepare to Install the Connector	21
Create a Windows Applications Network Share for ThinApp Packages	22
Prepare Kerberos for the Connector	23
Convert the Virtual Appliance File Format	24
4 Installing the Connector	25
Start the Connector Virtual Appliance	25
Configure the Connector with the Connector Virtual Appliance Interface	26
Access the Connector with the Web Interface	27
Using the Initial Configuration Wizard	28
Configuring the Connector with the Setup Wizard	29
5 Configuring the Connector	35
Configure the Connector for Logging	35
Configure Directory Sync Safeguards	36
Overview of Configuring SecurID	36
Overview of Configuring Kerberos for the Connector	39
Overview of Configuring NTLMv2 for the Connector	39
Configure Internet Explorer to Access the User Portal	40
Configure Firefox to Access the User Portal	41
Configure the Chrome Browser to Access the User Portal	42
Provide User Access to the Service	42
Trusted SSL Certificates on the Connector	43
6 Testing the Connector	45
Test Your Directory Server with the Connector	45
7 Troubleshooting the Connector	47
Inaccurate IP Address Displayed for the Connector	47
Connector Inaccessible	47
Sync Safeguard Message Appears When Creating New Connector Instance	48
Troubleshoot Missing Connector Password	48
Troubleshoot Kerberos	49

Index 51

Installing and Configuring Horizon Connector

This information describes how to install, configure, and maintain Horizon Connector. The connector software is the interface between the Horizon online identity and access management service and your onsite Microsoft Active Directory server. The connector can also provide Horizon users access to Windows applications captured as VMware ThinApp packages.

Intended Audience

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 Horizon features.

Horizon Connector Installation and Configuration Overview

Before you can install the connector, an operator creates your account and provides you with the authentication code. You then obtain the connector virtual appliance in order to install and configure the connector. The process involves a variety of tasks and you can deploy Horizon in several different ways. A key distinction in deployments is in the mode of authentication you choose. See [Chapter 1, "Introduction to Horizon,"](#) on page 9. An important deployment factor depends on if you choose to provide Horizon users with access to Windows applications captured as ThinApp packages. The flowcharts that follow illustrate two Horizon deployments at different levels of specificity. Together, the flowcharts provide a sense of the variety involved in deploying Horizon.

- [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

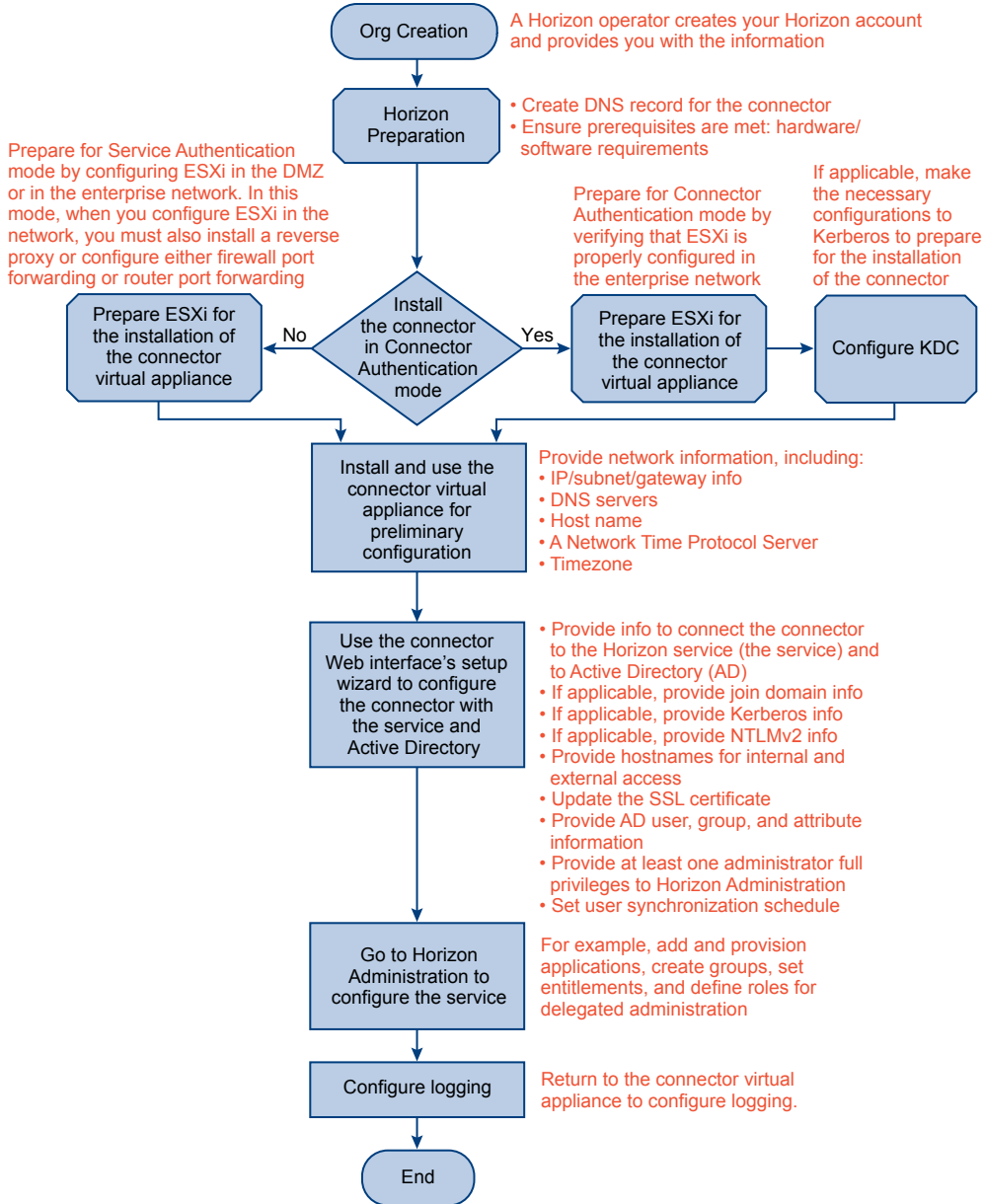
Installation and Configuration Flow of the Connector

See ["Installation and Configuration Flow of the Connector Integrated with ThinApp,"](#) on page 6 for information about installing and configuring Horizon 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 either Kerberos or NTLMv2 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. Horizon 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 15 for an introduction to integrating Horizon with ThinApp.

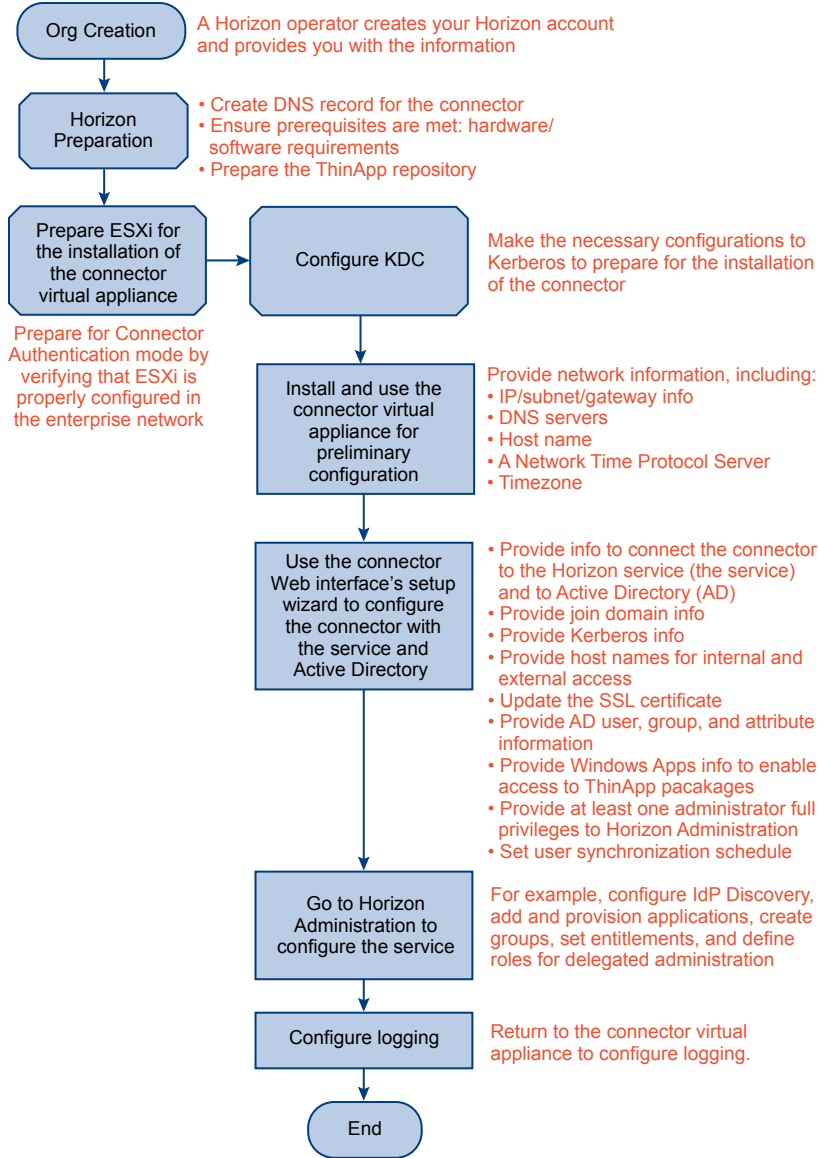
In the connector Web interface, you can make most configurations using the setup wizard as indicated in the flowchart. However, you have the option of skipping many of those configurations, such as for Kerberos, until after you have completed the setup wizard. Then, on the **Advanced** tab of the connector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

Providing Horizon-user 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 Horizon 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 22
- Configure Kerberos in Active Directory. See [“Prepare Kerberos for the Connector,”](#) on page 23
- Configure the Join Domain page of the connector Web interface. See [“Configure Join Domain,”](#) on page 30
- Configure the Kerberos page in the connector Web interface. See [“Configure Kerberos,”](#) on page 30
- Configure the Windows Apps page of the connector Web interface. See [“Configure Windows Apps,”](#) on page 31
- Enable IdP Discovery by configuring IP address ranges for the connector instance using Horizon Administration in the service. See *Horizon Administration Help*.
- Verify that the Horizon Agent is properly configured on users' Windows system. See *Horizon User Help*.

The preceding list of tasks are not required for Horizon to function, but they are required to properly integrate Horizon with ThinApp.

Figure 2. Horizon Connector with ThinApp Installation and Configuration Flowchart



Introduction to Horizon

Horizon is an online identity and access management service, an IT management service that unifies your software as a service (SaaS) applications and Windows applications (captured as ThinApp packages) into a single catalog for entitlement.

Table 1-1. Horizon Component Terminology

Horizon Component	Other Terms Used	Description
Horizon	<ul style="list-style-type: none"> ■ Horizon deployment 	The entire Horizon deployment, including the connector, the service, the related interfaces to access those components, and all other components necessary to enable user access to the service.
Horizon Connector	<ul style="list-style-type: none"> ■ The connector 	The software piece installed in your enterprise network as a virtual appliance. The connector communicates between the service and Active Directory and between the service and the ThinApp package repository.
Horizon Connector virtual appliance interface	<ul style="list-style-type: none"> ■ The connector CLI ■ The connector virtual appliance interface 	The command-line interface of the connector virtual appliance. You use this interface to make basic connector configurations when you first install the connector. You also use this interface to make changes to the connector at the operating system level using Linux commands.
Horizon Connector Web interface	<ul style="list-style-type: none"> ■ The connector Web interface 	The browser-based interface you use to configure and manage the connector after using the connector CLI to make the initial CLI configurations.
The service	<ul style="list-style-type: none"> ■ None 	The online service that stores entitlement, SaaS, and ThinApp package information and communicates with your connector instances on site to access Active Directory information.
Horizon Application Manager	<ul style="list-style-type: none"> ■ The service user Web interface 	The browser-based interface of the service that users use to access SaaS or ThinApp-packaged applications. This interface includes the User Portal and the Application Catalog.

Table 1-1. Horizon Component Terminology (Continued)

Horizon Component	Other Terms Used	Description
Horizon Administration	<ul style="list-style-type: none"> ■ The service administrator Web interface 	The browser-based interface of the service that you use to manage user access and entitlements to SaaS and ThinApp-packaged applications.
Horizon Agent	<ul style="list-style-type: none"> ■ None 	A ThinApp-specific component installed on user's Windows systems that allows users to access Windows applications captured as ThinApp packages.

The service facilitates username and password validation by using your Active Directory server on site. 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. The modes of authentication indicate the flow of user authentication to access the service. The connector can operate in Connector Authentication mode, which requires you to install the connector inside the enterprise network, or the connector can operate in Service Authentication mode, which requires you to install the connector either inside the DMZ or using an equivalent configuration. See “[Service Authentication Mode](#),” on page 12 for the list of configurations that allow the service to access the connector in Service Authentication mode. Also, the connector can operate in Hybrid mode, which is a combination of both Connector Authentication mode and Service Authentication mode.

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 the service. In specific situations where users are prompted for their credentials to access the service, the connector presents the login page. In Service Authentication mode, users are always prompted for their credentials when attempting to access the service, in which case the service 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

Configure your deployment in Connector Authentication mode if you want to use Kerberos, NTLMv2, or both. Connector Authentication mode refers to access to the service where the connector is the starting point for user authentication. Since Kerberos is required to provide users with ThinApp package access, you must configure Connector Authentication mode to provide access to Windows applications captured as ThinApp packages.

For Connector Authentication mode, users must be in the same domain as the Active Directory instance. Also, all user authentications occur within the enterprise network. Users outside the network can be authenticated when using a VPN connection to the enterprise. Other users outside the network are denied access to the service. Denying access from outside the network in this manner is extremely limiting. Therefore, the best practice when configuring your deployment for Connector Authentication mode is to configure your deployment as a hybrid of both Connector Authentication mode and Service Authentication mode.

For Connector Authentication mode, the service does not enforce multiple authentication factors, but instead accepts the SAML assertion from the connector. Therefore, after users log in to their internal network, they do not have to provide their credentials to access the service. For Connector Authentication mode, users access specific URLs that direct the authentication flow through the connector. These URLs contain the appropriate information to direct users through the connector directly to the service. You must provide users access to such URLs.

Table 1-2. Connector Authentication Mode: URL Examples

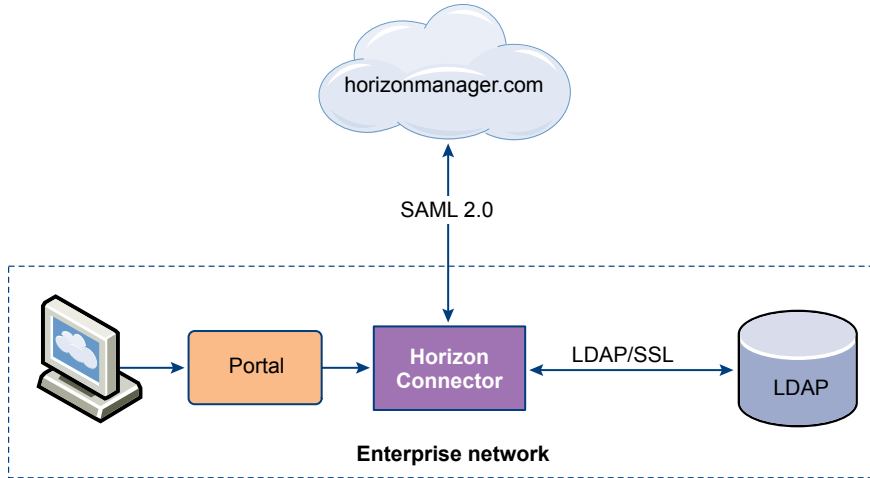
Target	URL Example	Information
Horizon User Portal	https:// <i>MyCompany</i> .horizonmanager.com/SAAS/API/1.0/GET/federation/request?i= <i>IDP#</i> &s=0	When your deployment is production ready, provide this URL to users to give them access to the User Portal. Replace <i>MyCompany</i> with the correct account name and replace <i>IDP#</i> with the IdP ID available on the connector Internal Access page.
	https:// <i>ConnectorHost.DomainName</i> /login/	Use this URL for troubleshooting and testing purposes if Kerberos is not configured. Replace <i>ConnectorHost</i> and <i>DomainName</i> with the appropriate values.
	https:// <i>ConnectorHost.DomainName</i> /authenticate/	Use this URL for troubleshooting and testing purposes if Kerberos is configured. Replace <i>ConnectorHost</i> and <i>DomainName</i> with the appropriate values.
Specific Applications	https:// <i>MyCompany</i> .horizonmanager.com/SAAS/API/1.0/GET/federation/request?i= <i>IDP#</i> &s= <i>SP#</i>	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 <i>SP#</i> with the ID number for a specific application. The application ID numbers are available from the Application Catalog in Horizon Application Manager.

For deployments where Kerberos is configured, the connector validates user desktop credentials using Kerberos tickets distributed by the key distribution center (KDC). For deployments where NTLMv2 is configured, the connector validates user desktop credentials using a challenge-response authentication.

For Connector Authentication mode, you must install the connector inside the enterprise network, where it acts as a federation server within your network, creating an in-network federation authority that communicates with the service using SAML 2.0 assertions. The connector authenticates the user with Active Directory within the enterprise network (using existing network security). When users within the enterprise network access an application URL that you have provided them, they are redirected to the connector, which authenticates users with Active Directory and generates a SAML assertion that the connector sends to the service. The user credentials never leave the corporate network.

A troubleshooting-related aspect of Connector Authentication mode is that users can still be authenticated even when either Kerberos or NTLMv2 fail. In fact, users can still be authenticated when neither Kerberos nor NTLMv2 are configured. In such cases, a service 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 the service. The connector then validates users against Active Directory.

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



Connector Authentication Mode and RSA SecurID

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 36.

You can configure SecurID with or without Kerberos. However, NTLMv2 authentication and username-password verification do no function when SecurID is configured.

RSA SecurID with	Result
Kerberos configured	Kerberos authentication takes precedence. Users are only prompted for their SecurID passcode if Kerberos authentication fails.
NTLMv2 configured (No benefit to enabling NTLMv2 when SecurID is configured)	SecurID takes precedence and NTLMv2 authentication is ignored.
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

Service Authentication mode allows users to access the service outside the enterprise network. Therefore, the service is the starting point for user authentication. You can use Service Authentication mode as the sole authentication flow for providing users access to the service. For this type of access, since the service must have a way of accessing the connector, configure access in one of the following ways:

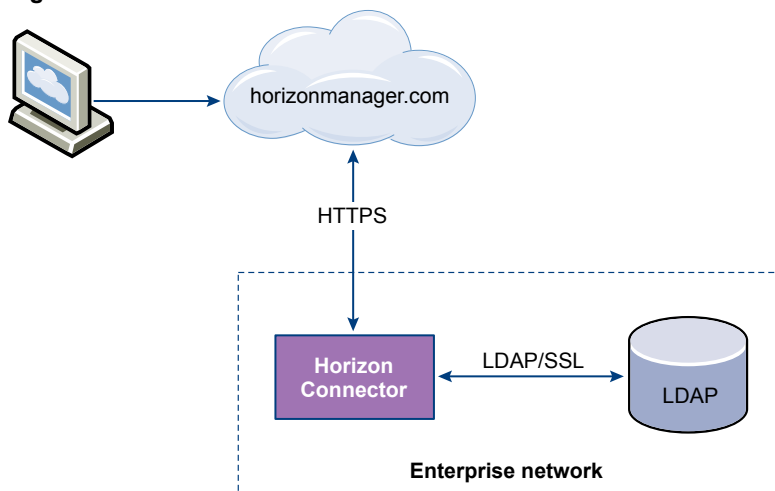
- Install the connector inside the DMZ.
- Install a reverse proxy server in the DMZ pointing to the connector installed behind the firewall.
- Configure firewall port forwarding or router port forwarding to point to the connector installed behind the firewall.

Then, you must provide users with a URL directly to the service.

Table 1-3. Service Authentication Mode: URL Examples

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

For Service Authentication mode, the service enforces multi-factor authentication. Therefore, when users attempt to access the service, they are prompted for their Active Directory credentials and for answers to their security questions. They are also provided with a confirmation image. The service 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 from the service.

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

Hybrid Mode

For Hybrid mode, you implement both Connector Authentication mode and Service Authentication mode. You must maintain at least one connector instance inside the enterprise network and at least one connector instance inside the DMZ or an equivalent configuration. See “[Service Authentication Mode](#),” on page 12 for the list of configurations that allow the service to access the connector in Service Authentication mode. The result is that users have the option of connecting to the service through the enterprise network or outside the enterprise network.

IdP Discovery

You configure the IdP Discovery feature in Horizon Administration. See *Horizon Administration Help*. The IdP Discovery feature works in conjunction with Connector Authentication mode or Hybrid mode, taking advantage of Kerberos or NTLMv2 authentication. IdP Discovery enables users to access the service without providing their credentials. 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 the service, 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 the service. When you have multiple connector instances, the order in which the corresponding connector records are listed in the service 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 in Horizon Administration.

The IdP Discovery feature typically applies when users attempt to access the service 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 either Kerberos or NTLMv2 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 neither Kerberos nor NTLMv2 is 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 service login page to gain access.

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

Hybrid Mode Example of IdP Discovery

This is one possible way to configure IdP Discovery when Horizon is deployed in Hybrid 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 the service 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, NTLMv2, or username/password authentication, while users outside the network are authenticated in Service Authentication mode.

RSA SecurID Example of IdP Discovery

This is one possible way to configure IdP Discovery and SecurID in the same Horizon deployment. For an overview of configuring RSA SecurID with the connector, see [“Overview of Configuring SecurID,”](#) on page 36. For this deployment, you configure two connector instances, both in Connector Authentication mode.

- First connector instance in Connector Authentication mode: You do not configure SecurID for this connector instance. In the service, you configure IP address ranges to include users within the enterprise network.
- Second connector instance in Connector Authentication mode: You configure SecurID for this connector instance. In the service, 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, NTLMv2, 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 6 for information about integrating the connector with ThinApp. Users can only access Windows applications captured as ThinApp packages through the enterprise network. Users outside the network have the option of accessing ThinApp packaged applications by using a VPN connection to the enterprise.

Evaluation and Quick Access to the Service

You can provide users with access to the User Portal 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 users credentials when they attempt to log in to the service.
- To allow you to log in to the service. You use the username associated with the Bind DN user account and respective password as the credentials to log in to the service as an administrator.

With quick-access configuration, you cannot configure Kerberos or NTLMv2 authentication, nor can you provide users access to Windows applications captured as ThinApp packages. The purpose of quick-access configuration is to provide easy access to the basic functionality of Horizon, which you and users can evaluate. Because Directory Sync is not required with quick-access configuration, users can self-enroll to the service.

Security Concerns and System Requirements for the Connector

2

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, the command-line interface of the connector, is not encrypted and should not be exposed to public networks.
- The connector virtual appliance interface is accessible to anyone with access to the machine on which ESXi and, therefore, the virtual appliance is hosted. Protection relies on firewalling and enforcing authentication to the ESXi host.
- The connector Web interface listens on HTTP port 8443 for administration and port 443 for user authentication.

Connector Recommendations and Requirements

To synchronize your Active Directory data effectively with the service, ensure that the environment for the connector virtual machine meets the minimum requirements.

The following components are required:

- The connector virtual machine VMware provides as an Open Virtual Appliance .ova file.
- VMware ESXi as the host of the virtual appliance.
- A virtual machine client that provides access to the connector virtual appliance interface, the command-line interface of the virtual appliance.
- A conversion tool, if your VMware hypervisor does not open OVA files directly. VMware offers a free tool for Windows and Linux. See [“Convert the Virtual Appliance File Format,”](#) on page 24.

Hardware Requirements for the Connector Virtual Appliance Host

Ensure that the environment for the host, the ESXi 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	4GB 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 ports
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	1 vCPU	2 or even 4 vCPU for higher performance
Random-access memory	1GB	2GB
Storage	15GB	20GB

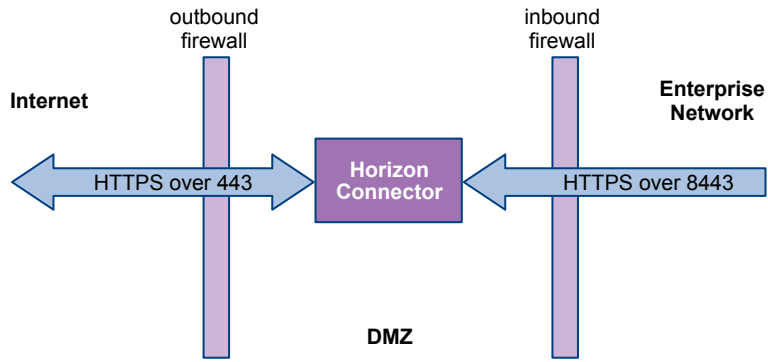
Network Configuration Requirements for Connector Deployment

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	Inbound firewall port 443 opened from the service to the connector. Datacenter IP addresses: 206.80.50.32 and 209.34.94.96
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, SecurID-enabled only	Inbound firewall port 443 opened from users outside the enterprise network to the connector
Both modes	Outbound firewall port 443 opened from the connector to the Internet
Both modes	Port opened on the path from the connector to Active Directory, typically port 389 or 636
Both modes	Ensure access to a Network Time Protocol (NTP) Server in one of the following ways: <ul style="list-style-type: none"> ■ To allow the connector to access an external NTP server, ensure that the outbound firewall port 123 (NTP Protocol) is open from the connector to the Internet ■ If you do not want a firewall port open for the NTP server, when you configure the connector using the connector virtual appliance interface, point the NTP configuration to an internal NTP server

Figure 2-1. Network Traffic to and from the Connector



Preparing to Install the Connector

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 21
You must prepare your environment for the installation of the connector.
- 2 [Create a Windows Applications Network Share for ThinApp Packages](#) on page 22
If you want to enable the VMware ThinApp management capabilities of Horizon and allow users to access ThinApp packages from the Horizon Application Catalog, you must create a network file share and store your ThinApp packages in that shared folder.
- 3 [Prepare Kerberos for the Connector](#) on page 23
If you are deploying the connector in Connector Authentication mode, you can perform the preinstallation steps to prepare your system for Kerberos.
- 4 [\(Optional\) Convert the Virtual Appliance File Format](#) on page 24
You can convert the virtual appliance file format from the OVA format to the VAX 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

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 Horizon,”](#) on page 9. This decision influences the physical location of the ESXi machine that will host the connector.
- If you are installing the connector in Connector Authentication mode and also want to provide Kerberos authentication, prepare Kerberos for the connector. See [“Prepare Kerberos for the Connector,”](#) on page 23 for information specific to preparing Kerberos for the connector. See [“Overview of Configuring Kerberos for the Connector,”](#) on page 39 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 36.

- 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 22 for information specific to creating a network file share. See [“Installation and Configuration Flow of the Connector Integrated with ThinApp,”](#) on page 6 for an overview of integrating Horizon with ThinApp.
- Ensure that all the hardware, network, and resource requirements are met. See [“Connector Recommendations and Requirements,”](#) on page 17.

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 On the ESXi instance on which you will install the connector, download the .ova file for the connector virtual appliance from the VMware Download Center.

Create a Windows Applications Network Share for ThinApp Packages

If you want to enable the VMware ThinApp management capabilities of Horizon and allow users to access ThinApp packages from the Horizon 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 the service.

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 Horizon 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 Horizon 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.

Prepare Kerberos for the Connector

If you are deploying the connector in Connector Authentication mode, you can perform the preinstallation steps to prepare your system for Kerberos.

For an overview of configuring Kerberos with Horizon, see [“Overview of Configuring Kerberos for the Connector,”](#) on page 39. Perform this task only if you plan to configure the connector in Connector Authentication mode. If you want to provide Horizon users with access to ThinApp packages, you must configure Kerberos.

Prerequisites

Verify that the following conditions are met:

- The Windows network is functioning.
- The Domain Name System (DNS) server is configured to resolve all machines involved.
- Internal users can sign in to their desktop computers using Active Directory.
- Internal users have access to connector port 443.

Procedure

- 1 On the Active Directory Domain Controller and Key Distribution Center (KDC) host, create a user account with a name that follows the format `HTTP/FullyQualifiedConnectorHost@DomainName` for each connector instance that will connect and authenticate users.

You must use this information again when you configure the connector Web interface. For example, you must specify this user account, or principal, when you configure Kerberos in the connector Web interface. Also, the hostname you use to replace the `FullyQualifiedConnectorHost` placeholder must match the Internal hostname referenced in the Internal Host text box on the Internal Access page of the connector Web interface.

- a Ensure that the legacy user name of the account matches the host name of the connector, for example `ConnectorHost` for `ConnectorHost.DomainName`.
 - b Ensure that the user belongs to the domain users group.
 - c Set the password to never expire. You must specify this password again when you configure Kerberos in the connector Web interface.
- 2 Add the (servicePrincipalName) attribute for the newly created user account by adding these values.
 - `HTTP/ConnectorHost.DomainName`

- `HTTP/ConnectorHost`

One way to add the `servicePrincipalName` attribute is to select the newly created user and navigate through the properties to the attribute editor where you can edit the `servicePrincipalName` attribute. To access the attribute editor, you might need to change the view to display advanced features.

What to do next

If all the preinstallation tasks are completed, install the connector. See [Chapter 4, “Installing the Connector,”](#) on page 25.

(Optional) Convert the Virtual Appliance File Format

You can convert the virtual appliance file format from the OVA format to the VAX 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 connector on a VMware hypervisor that supports the VAX format and convert the connector OVA file to the VAX 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=VAX ova-file-name VAX-file-name`

For example: `/usr/bin/ovftool -tt=VAX connector-1.1.0.ova central-connector`

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

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

Example: File Conversion Output

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

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

What to do next

Install the connector virtual appliance on your hypervisor.

Installing the Connector

After you install the connector, you can use it to access and configure the service.

Installing the connector includes the following tasks:

- Make the connector virtual appliance accessible to the ESXi host.
- Start and configure the virtual appliance.
- Use the connector Web interface to perform the initial configuration of the connector necessary to access Horizon Administration.

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

This chapter includes the following topics:

- [“Start the Connector Virtual Appliance,”](#) on page 25
- [“Configure the Connector with the Connector Virtual Appliance Interface,”](#) on page 26
- [“Access the Connector with the Web Interface,”](#) on page 27
- [“Using the Initial Configuration Wizard,”](#) on page 28
- [“Configuring the Connector with the Setup Wizard,”](#) on page 29

Start the Connector Virtual Appliance

The connector is a virtual appliance running in a virtual machine. Starting the virtual appliance gives you access to the connector virtual appliance interface, which is the connector CLI.

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). 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 Make the connector virtual appliance accessible to the ESXi instance.

See the VMware ESXi documentation.

- 2 In ESXi, start 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 password. You can perform the initial configuration of the connector as described in [“Configure the Connector with the Connector Virtual Appliance Interface,”](#) on page 26.

Configure the Connector with the Connector Virtual Appliance Interface

Use the connector virtual appliance interface, the command-line interface of the connector virtual appliance, 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 ESXi. See [“Start the Connector Virtual Appliance,”](#) on page 25.
- Verify that you followed the steps to prepare for the installation of the connector. See [“Prepare to Install the Connector,”](#) on page 21.
- 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.	<p>If you have a static IP address, type n. Continue responding to the subprompts related to a static IP address.</p> <p>If you have a DHCPv4 address, type y and continue responding to the subprompts related to DHCP and a proxy server.</p> <p>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.</p> <p>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 configure NTLMv2 functionality or if you plan to provide users with access to ThinApp packages. Both configurations rely on the join domain functionality.</p>

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

- 3 Configure a Network Time Protocol server.
 - a Select **Login** and log in to the Linux operating system with root credentials.
 - 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 Set the time zone for the connector.
 - a Select **Set Timezone**.
 - b Continue selecting location options to select your specific time zone.
- 5 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 with root credentials.
 - b Change directories to `/opt/vmware/c2`.

The c2 directory stores the tools for stopping and starting the Apache Tomcat server, which is the underlying Web server for the connector. Because the locations to which Tomcat logs activity varies depending on where commands are run, the best practice is to stop and start the Web server from the c2 directory.
 - c Run the following command to restart the Web server: `./c2instance/bin/tcruntime-ctl.sh restart`.

The connector now uses its real IP address and is set to the correct time and time zone. The connector is ready for further configuration.

What to do next

Use the Web interface to configure the connector.

Access the Connector with the Web Interface

When the connector has an IP address, you can use a browser to access the Web interface.

Until you update the SSL certificate, the connector uses a 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 If you are configuring Horizon with Kerberos, use the connector hostname, not the IP address, to access the connector. Using the connector IP address instead of the hostname negatively affects Kerberos authentication when you or users access the service 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 26.
- Verify that you have access to a supported browser. Horizon Connector supports Firefox and Internet Explorer.

Procedure

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

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

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 the Service,”](#) on page 15. To fully configure the connector, you must run the setup wizard after you complete the initial configuration wizard.

Start the Initial Configuration Wizard

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

The Horizon Application Manager 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 Click **Next** to continue to the next page of the initial configuration wizard.

When you complete the initial configuration wizard, if you deployed Horizon in Connector Authentication mode, you have the option of providing users with quick-access to the connector. 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 the service.

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
Server Port	The text box for the port number for the Active Directory host
Search Attribute	The text box for the Active Directory attribute that contains the username
Base DN	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

Bind DN	<p>The text box for the full common name (CN) of an Active Directory user account that has privileges to search for users. The Bind DN entry must be located in the same branch and below the Base DN.</p> <p>For example: CN=Administrator,CN=Users,DC=mycompany,DC=com. This user account must have at least domain user privileges.</p> <p>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 the service. You use the username for this account to log in to the service as an administrator.</p>
Bind Password	<p>The text box for the Active Directory password for the account that can search for users.</p> <p>NOTE The Bind password is the same password used in association with the Bind DN user account.</p>

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

If you deployed Horizon in Connector Authentication mode, the connector is now in the quick-access state, providing users access to the User Portal. See [“Evaluation and Quick Access to the Service,”](#) on page 15. At this point, you and users have access to the service. You do not need to start the setup wizard unless you want 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 29.

Configuring the Connector with the Setup Wizard

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, the service, and Active Directory. Also, if you want to provide Horizon 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 Horizon Administration to configure the service. You can return to the connector at any time to make further configurations.

Start the Setup Wizard

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

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 either configure single sign-on with NTLMv2 or provide users with access to Windows applications captured as ThinApp packages. 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

Configure Kerberos

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

Configure the Kerberos page only after you have configured your system for Kerberos before you install the connector. You receive information during the preinstallation task that you need to configure Kerberos in the connector Web interface. For an overview of configuring Kerberos with Horizon, including info about preparing Kerberos for the connector, see [“Overview of Configuring Kerberos for the Connector,”](#) on page 39.

You must configure Kerberos to enable the Kerberos protocol to secure interactions between users' browsers and the service. Configuring Kerberos is required if you want to provide Horizon users access to Windows applications captured as ThinApp packages.

KDC	The text box for the key distribution hostname or IP address. For example, <code>kdc.mycompany.com</code>
Realm	The text box for the Windows realm name. For example, <code>MYCOMPANY.COM</code>
Principal	The text box for the servicePrincipalName (SPN) of the connector account in Active Directory. For example <code>http/connector.mycompany.com@MYCOMPANY.COM</code>
Password	The text box for the password of the connector user account in Active Directory

For information about all the procedures involved in configuring the connector with Kerberos authentication, see [“Overview of Configuring Kerberos for the Connector,”](#) on page 39.

Configure NTLMv2

If your are configuring the connector in Connector Authentication mode, and you want to provide the security offered by NTLMv2 instead of or in addition to that provided by Kerberos, you can configure NTLMv2 in the setup wizard. You also have the option of skipping the NTLMv2 page in the wizard and configuring the NTLMv2 page later on the **Advanced** tab.

You must configure the Join Domain page as a prerequisite to configuring NTLMv2. For an overview of configuring NTLMv2 with Horizon, see [“Overview of Configuring NTLMv2 for the Connector,”](#) on page 39.

Enable NTLMv2 The check box to enable the NTLMv2 protocol to secure interactions between browsers and the service

Configure Internal Access

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

Internal host The text box for the internal hostname or IP address of the connector virtual appliance

Configure External Access

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.

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 chain. If you are using an SSL certificate issued by a trusted certificate authority, you paste the SSL certificate chain 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 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

In the setup wizard, you can provide Horizon 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 Horizon users access to ThinApp packages requires a variety of other configurations. See [“Installation and Configuration Flow of the Connector Integrated with ThinApp,”](#) on page 6 for information about the configurations required to integrate Horizon with ThinApp.

Enable Windows Apps	The check box to enable Horizon users access to ThinApp packages
Path	The text box for the path to the Windows applications network share
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 the service

Map User Attributes

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

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.

Select Users

You can determine which Active Directory users are synchronized with the service.

Filter Users Tab

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 the service 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) to include all of the users to transfer as part of the synchronization process from Active Directory to the service. You can check the results on the View Results tab
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 the service. 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

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

View Errors Tab

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 the service.

Select Groups

You can select the group information in Active Directory to be imported to the Horizon service during synchronization.

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
Selected Groups	The section that lists Active Directory groups to be pushed to the service during synchronizations. After you add a group to the Selected Groups list, information for that group is exported to the service each time Active Directory synchronizes with the service. You can edit the Horizon name for a group as necessary for easy recognition

Configure Scheduling

You can configure how often Active Directory synchronizes with the Horizon service.

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

Push to Horizon

You can use the Push to Horizon 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.

You click **Save and Continue** to synchronize Active Directory with the service.

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 the service. To configure the service 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

Configuring the Connector

After you configure the connector and access the Horizon service, you can return to the connector for further configuration.

After you install the connector and have access to Horizon Administration, certain connector configurations might still be required to make your Horizon 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,”](#) on page 35
- [“Configure Directory Sync Safeguards,”](#) on page 36
- [“Overview of Configuring SecurID,”](#) on page 36
- [“Overview of Configuring Kerberos for the Connector,”](#) on page 39
- [“Overview of Configuring NTLMv2 for the Connector,”](#) on page 39
- [“Configure Internet Explorer to Access the User Portal,”](#) on page 40
- [“Configure Firefox to Access the User Portal,”](#) on page 41
- [“Configure the Chrome Browser to Access the User Portal,”](#) on page 42
- [“Provide User Access to the Service,”](#) on page 42
- [“Trusted SSL Certificates on the Connector,”](#) on page 43

Configure the Connector for Logging

You can configure logs in the connector virtual appliance interface. You configure Web server logs in the `log4j.xml` file, and configure other program logs in the `syslog` file. To store syslog information, you can configure your own 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/logrotate.d/syslog	Configure the syslog file to direct program logs to your syslog server.

Prerequisites

The best practice is to store program logs in a separate syslog server. Verify that a 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 with root credentials.
- 3 Use Linux commands to access and configure the log4j.xml or syslog files.

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

Configure Directory Sync Safeguards

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

A change to Horizon 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 Horizon 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

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 Horizon

After you deploy Horizon in Connector Authentication mode, you can configure SecurID to provide additional security. See [“Connector Authentication Mode and RSA SecurID,”](#) on page 12.

Configure the Network

You must ensure your network is properly configured for your Horizon 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

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 37.

Configure SecurID with the Connector Web Interface

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 38.

Configure the IP Address Range in Horizon Administration

After you complete the configuration of SecurID in the connector, you log in to Horizon as an administrator to configure IdP Discovery, which involves providing IP address ranges for users' systems. See [“IdP Discovery,”](#) on page 13 for more information about IdP Discovery, including an example specific to SecurID.

Prepare the RSA SecurID Server for the Connector

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 36 for an overview of using RSA SecurID with Horizon.

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.

Horizon 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 Horizon 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 in 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

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 Horizon, see [“Overview of Configuring SecurID,”](#) on page 36.

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 37.

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 <code>sdconf.rec</code> .
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 Horizon Administration to configure the IdP Discovery feature. See [“IdP Discovery,”](#) on page 13.

Overview of Configuring Kerberos for the Connector

Configuring Kerberos for the connector involves preinstallation, installation, and possibly configuration tasks.

Kerberos Configuration

Before you install the connector, you configure Kerberos directly. See [“Prepare Kerberos for the Connector,”](#) on page 23. Kerberos configuration is required if you want to provide Horizon users with access to Windows applications captured as ThinApp packages.

Connector Installation

After you install the connector, you enable the connector to use Kerberos authentication by configuring the Kerberos page in the connector Web interface, either in the setup wizard or on the **Advanced** tab. See [“Configure Kerberos,”](#) on page 30.

Kerberos Authentication Operating System Support

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

Browser Configuration

The following browsers, on Windows only, are supported for accessing the service in Kerberos authentication:

- Firefox: Additional configuration is required for each user's browser. See [“Configure Firefox to Access the User Portal,”](#) on page 41.
- Internet Explorer: Additional configuration is required for each user's browser. See [“Configure Internet Explorer to Access the User Portal,”](#) on page 40.
- Chrome: Additional configuration is required for each user's browser. See [“Configure the Chrome Browser to Access the User Portal,”](#) on page 42.

Kerberos Troubleshooting

See [“Troubleshoot Kerberos,”](#) on page 49.

Overview of Configuring NTLMv2 for the Connector

Configuring NTLMv2 for the connector involves installation and possibly configuration tasks.

NTLMv2 Configuration

NTLMv2 is configured as a part of Active Directory. No further configuration to Active Directory is necessary.

Connector Installation

After you install the connector, you enable the connector to use NTLMv2 authentication by configuring the Join Domain page and the NTLMv2 page in the connector Web interface, either in the setup wizard or on the **Advanced** tab. See [“Configure Join Domain,”](#) on page 30 and [“Configure NTLMv2,”](#) on page 30.

NTLMv2 Authentication Operating System Support

Currently, interactions between users' browsers and the service are authenticated by NTLMv2 on Windows operating systems only. Accessing the service from other operating systems does not take advantage of NTLMv2 authentication.

Browser Configuration

The following browsers, on Windows only, are supported for accessing the service using NTLMv2 authentication:

- Firefox: Additional configuration is required for each user's browser. See [“Configure Firefox to Access the User Portal,”](#) on page 41.
- Internet Explorer: Additional configuration is required for each user's browser. See [“Configure Internet Explorer to Access the User Portal,”](#) on page 40.
- Chrome: Additional configuration is required for each user's browser. See [“Configure the Chrome Browser to Access the User Portal,”](#) on page 42.

Configure Internet Explorer to Access the User Portal

You must configure the Internet Explorer browser if Kerberos or NTLMv2 is configured for your Horizon deployment and you want to provide users access to the User Portal using Internet Explorer.

Kerberos and NTLMv2 authentication work in conjunction with Horizon on Windows operating systems. Do not implement these Kerberos and NTLMv2 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 or NTLMv2. See [“Overview of Configuring Kerberos for the Connector,”](#) on page 39 or [“Overview of Configuring NTLMv2 for the Connector,”](#) on page 39.

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 either Kerberos or NTLMv2 authentication is successful, the test URL goes to the User Portal.

If all related Kerberos or NTLMv2 configurations are correct, the relative protocol (Kerberos or NTLMv2) secures all interactions between that Internet Explorer browser instance and the service. Users then have single sign-on access to the service.

Configure Firefox to Access the User Portal

You must configure the Firefox browser if Kerberos or NTLMv2 is configured for your Horizon deployment and you want to provide users access to the User Portal using Firefox.

Kerberos and NTLMv2 authentication work in conjunction with Horizon on Windows operating systems. Do not implement these Kerberos and NTLMv2 related steps on other operating systems.

Prerequisites

Configure the Firefox browser, for each user, or provide users with the instructions, after you configure Kerberos or NTLMv2. See [“Overview of Configuring Kerberos for the Connector,”](#) on page 39 or [“Overview of Configuring NTLMv2 for the Connector,”](#) on page 39.

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 or NTLMv2 functionality by using the Firefox browser to log in to the connector login URL.
For example, `https://ConnectorHost.mycompanyintranet.com/authenticate/`.
If either Kerberos or NTLMv2 authentication is successful, the test URL goes to the User Portal.

If all related Kerberos or NTLMv2 configurations are correct, the relative protocol (Kerberos or NTLMv2) secures all interactions between that Firefox browser instance and the service. Users then have single sign-on access to the service.

Configure the Chrome Browser to Access the User Portal

You must configure the Chrome browser if Kerberos or NTLMv2 is configured for your Horizon deployment and you want to provide users access to the Horizon User Portal using the Chrome browser.

Kerberos and NTLMv2 authentication work in conjunction with Horizon on Windows operating systems. Do not implement these Kerberos and NTLMv2 related steps on other operating systems.

Prerequisites

- Configure Kerberos or NTLMv2. See [“Overview of Configuring Kerberos for the Connector,”](#) on page 39 or [“Overview of Configuring NTLMv2 for the Connector,”](#) on page 39.
- Since Chrome uses the Internet Explorer configuration to enable Kerberos and NTLMv2 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 40.

Procedure

- ◆ Test Kerberos or NTLMv2 functionality by using the Chrome browser to log in to the connector login URL.
For example, `https://ConnectorHost.mycompanyintranet.com/authenticate/`.
If either Kerberos or NTLMv2 authentication is successful, the test URL goes to the User Portal.

If all related Kerberos or NTLMv2 configurations are correct, the relative protocol (Kerberos or NTLMv2) secures all interactions between that Chrome browser instance and the service. Users then have single sign-on access to the service.

Provide User Access to the Service

After you configure the connector and the service, you must provide users with a URL to access the Horizon User Portal. You can also provide URLs for individual applications that are available in Horizon Application Catalog.

See [Chapter 1, “Introduction to Horizon,”](#) 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 10

- [“Service Authentication Mode,”](#) on page 12
- [“IdP Discovery,”](#) on page 13

Trusted SSL Certificates on the Connector

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

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 the service.

Testing the Connector

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

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 Horizon 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 the service, troubleshoot the appropriate configuration, such as Active Directory, Kerberos, or NTLMv2.

Troubleshooting the Connector

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

This chapter includes the following topics:

- [“Inaccurate IP Address Displayed for the Connector,”](#) on page 47
- [“Connector Inaccessible,”](#) on page 47
- [“Sync Safeguard Message Appears When Creating New Connector Instance,”](#) on page 48
- [“Troubleshoot Missing Connector Password,”](#) on page 48
- [“Troubleshoot Kerberos,”](#) on page 49

Inaccurate IP Address Displayed for the Connector

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

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

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 47.
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

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 the service 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.

Troubleshoot Missing Connector Password

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 Change directories to `/opt/vmware/c2`.

The `c2` directory stores the tools for stopping and starting the Apache Tomcat server, which is the underlying Web server for the connector. Because the locations to which Tomcat logs activity varies depending on where commands are run, the best practice is to stop and start the Web server from the `c2` directory.

- 4 Run the following command to stop the Web server: `./c2instance/bin/tcruntime-ctl.sh stop`.
- 5 Run the following command to remove the `config-admin.json` file: `rm /var/lib/config-admin.json`
Removing this file removes the connector password.
- 6 Run the following command to start the Web server: `./c2instance/bin/tcruntime-ctl.sh start`
- 7 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.

- 8 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.

Troubleshoot Kerberos

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

Problem

Users cannot access the service 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 Kerberos for the Connector,”](#) on page 39.

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

- 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.	<ul style="list-style-type: none"> ■ See “Browser Configuration,” on page 39 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.	<ol style="list-style-type: none"> 1 Access a Network Time Protocol (NTP) server. See “Configure the Connector with the Connector Virtual Appliance Interface,” on page 26 for more information about the configuration of an NTP server. 2 From a command window on each machine, run the <code>net time /set</code>. 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.	<p>Use Microsoft Kerbtray to perform diagnostics.</p> <ul style="list-style-type: none"> ■ 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

A

Active Directory
 groups **32**
 synchronization schedule **32**
 user attributes **31**
 users **32**
Active Directory domain controller **23**
Apache Tomcat **48**
Application Catalog **9, 42**
audience **5**

B

Base DN, Active Directory **28**
Bind DN, Active Directory **28**
browser
 Chrome **42**
 Firefox **41**
 Internet Explorer **40**
 support for the connector **27**

C

Chrome browser **42**
CLI interface **25**
command line **48**
command-line interface **26**
configuring
 gateway **26**
 IP address **26**
 netmask **26**
 the connector **35**
configuring Kerberos, setup wizard **30**
connector
 description **9**
 operating system **26**
 supported browsers **27**
Connector Authentication mode **9, 23, 30**
connector CLI interface, description **9**
connector virtual appliance interface **25, 26**
converter tool, OVF **21**

D

DHCP **26**
DHCP server **25**
dig command **47**
directory, synchronization safeguards **36**
DNS **21**

DNS record **21**
Domain Name System **21**

E

ESXi **17**
External Access **31**

F

file share **22**
flowchart, installation and configuration **5**

G

gateway information **26**

H

Horizon Application Manager, description **9**
Horizon Connector, description **9**
Horizon Connector virtual appliance interface,
 description **9**
Horizon Connector Web interface, description **9**
Horizon deployment, description **9**
Hybrid mode **9**
hypervisor **21**

I

initial configuration wizard **28**
internal access **31**
IP address **26**
IP Address, error **47**

J

join domain **30**

K

KDC, See key distribution center
Kerberos, overview **39**
Kerberos support
 browsers **39**
 operating systems **39**
Kerbray **49**
key distribution center **9**
keytab file **23**
ktpass command **23**

L

Linux, SUSE **5**

- Linux system administrators **5**
- logging **35**
- logs
 - syslog **35**
 - ThinApp-package related **35**
 - Web server **35**

M

- mode
 - Connector Authentication **9**
 - Hybrid **9**
 - Service Authentication **9**

N

- network configuration settings **17**
- network file share **22**
- Network Time Protocol, *See* NTP
- nslookup **47**
- NTLMv2, overview **39**
- NTLMv2 support
 - browsers **39**
 - operating systems **39**
- NTP, configuring **17**

O

- OVA **21**
- OVA file format, converting **24**
- overview, installation and configuration **5**
- OVF conversion tool, using **24**

P

- password
 - Active Directory **28**
 - the connector **27, 48**
- port
 - 123 **17**
 - 389 **17**
 - 443 **17**
 - 8443 **17**
 - 88 **17**
- preinstallation **21**

R

- requirements
 - hardware **17**
 - network **17**
 - resource **17**
- RSA SecurID, *See* SecurID
- RSA SecurID server
 - authentication agent **37**
 - configuration file **37**
 - preparing **37**
 - supported versions **37**

S

- SaaS **9**
- safeguards, directory synchronization **36**
- sdconf.rec file, downloading **37**
- SecurID **9, 36, 37**
- SecurID, configuration **38**
- service, description **9**
- Service Authentication mode **9**
- setup wizard
 - configuration **29, 32**
 - introduction **25**
 - synchronizing Active Directory **32**
- SLES **25**
- software as a service, *See* SaaS
- SSL certificate
 - Active Directory **28**
 - self-signed **31, 43**
 - trusted **31, 43**
- subnet **26**
- SUSE Linux **5, 26**
- SUSE Linux Enterprise Server, *See* SLES
- sync safeguards, troubleshooting **48**
- syslog **35**
- system administrator
 - Linux **5**
 - Windows **5**

T

- testing, the connector **45**
- ThinApp packages **22**
- Tomcat, Apache **48**
- traceroute tools **47**
- tracert.exe **47**

U

- user attributes **31**
- User Portal **9**

V

- VAX file format **24**
- verify
 - password **45**
 - username **45**
- virtual appliance, file format **24**
- VMware hypervisor, *See* hypervisor

W

- Web server **48**
- Windows applications network share **22**
- Windows Apps **31**
- Windows system administrator **5**