Deploying and Configuring Access Point

Access Point 2.0
VMware Horizon 6

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

EN-001879-02

vmware®

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

Deploying and Configuring Access Point

Deploying and Configuring Access Point provides information about designing a View deployment that uses Access Point for secure external access to Horizon 6 servers and desktops. This guide also provides instructions for deploying Access Point virtual appliances and changing the configuration settings after deployment, if desired.

Intended Audience

This information is intended for anyone who wants to deploy and use Access Point appliances in a Horizon 6 environment. The information is written for experienced Linux system administrators who are familiar with virtual machine technology and datacenter operations.

VMware Technical Publications Glossary

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

1 Introduction to Access Point

Access Point functions as a secure gateway for users who want to access Horizon 6 desktops and applications from outside the corporate firewall.

Access Point appliances typically reside within a DMZ and act as a proxy host for connections inside your company's trusted network. This design provides an additional layer of security by shielding View virtual desktops, application hosts, and View Connection Server instances from the public-facing Internet.

Access Point directs authentication requests to the appropriate server and discards any un-authenticated request. The only remote desktop and application traffic that can enter the corporate data center is traffic on behalf of a strongly authenticated user. Users can access only the resources that they are authorized to access.

Access Point appliances fulfill the same role that was previously played by View security servers, but Access Point provides additional benefits:

- An Access Point appliance can be configured to point to either a View Connection Server instance or a load balancer that fronts a group of View Connection Server instances. This design means that you can combine remote and local traffic.
- Configuration of Access Point is independent of View Connection Server instances. Unlike with security servers, no pairing password is required to pair each security server with a single View Connection Server instance.
- Access Point appliances are deployed as hardened virtual appliances, which are based on a Linux appliance that has been customized to provide secure access. Extraneous modules have been removed to reduce potential threat access.
- Access Point uses a standard HTTP(S) protocol for communication with View Connection Server. JMS, IPsec, and AJP13 are not used.

The following authentication mechanisms are available, and for all of these authentication mechanisms except smart card, authentication is proxied to View Connection Server:

- Active Directory credentials
- RSA SecurID
- RADIUS
- Smart cards (Note that for this release smart card authentication is a Tech Preview feature.)
- SAML (Security Assertion Markup Language)

This chapter includes the following topics:

Firewall Rules for DMZ-Based Access Point Appliances

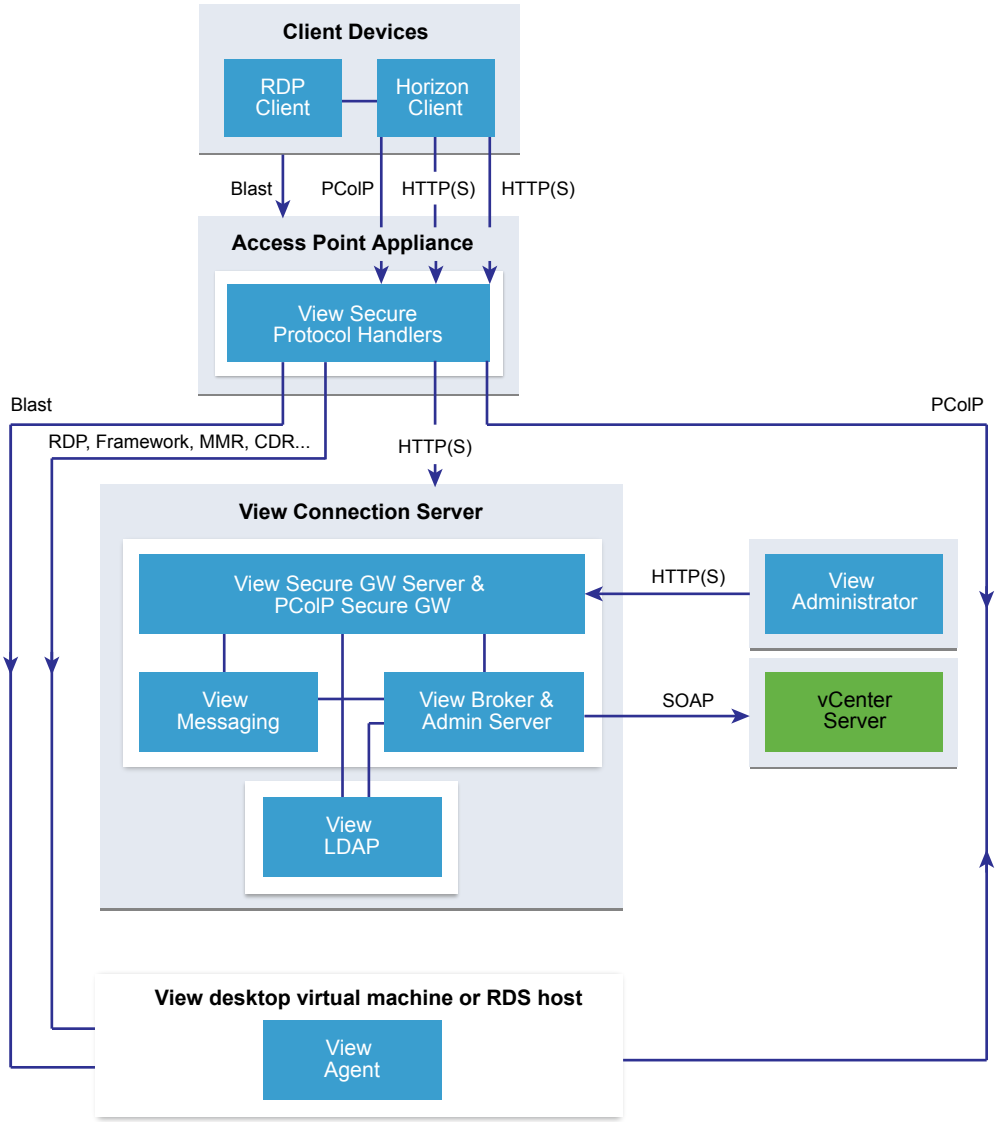
DMZ-based Access Point appliances require certain firewall rules on the front-end and back-end firewalls. During installation, Access Point services are set up to listen on certain network ports by default.

A DMZ-based Access Point appliance deployment usually includes two firewalls.

- An external network-facing, front-end firewall is required to protect both the DMZ and the internal network. You configure this firewall to allow external network traffic to reach the DMZ.
- A back-end firewall, between the DMZ and the internal network, is required to provide a second tier of security. You configure this firewall to accept only traffic that originates from the services within the DMZ.

The following figure illustrates the protocols that each View component uses for communication. This configuration might be used in a typical WAN deployment.

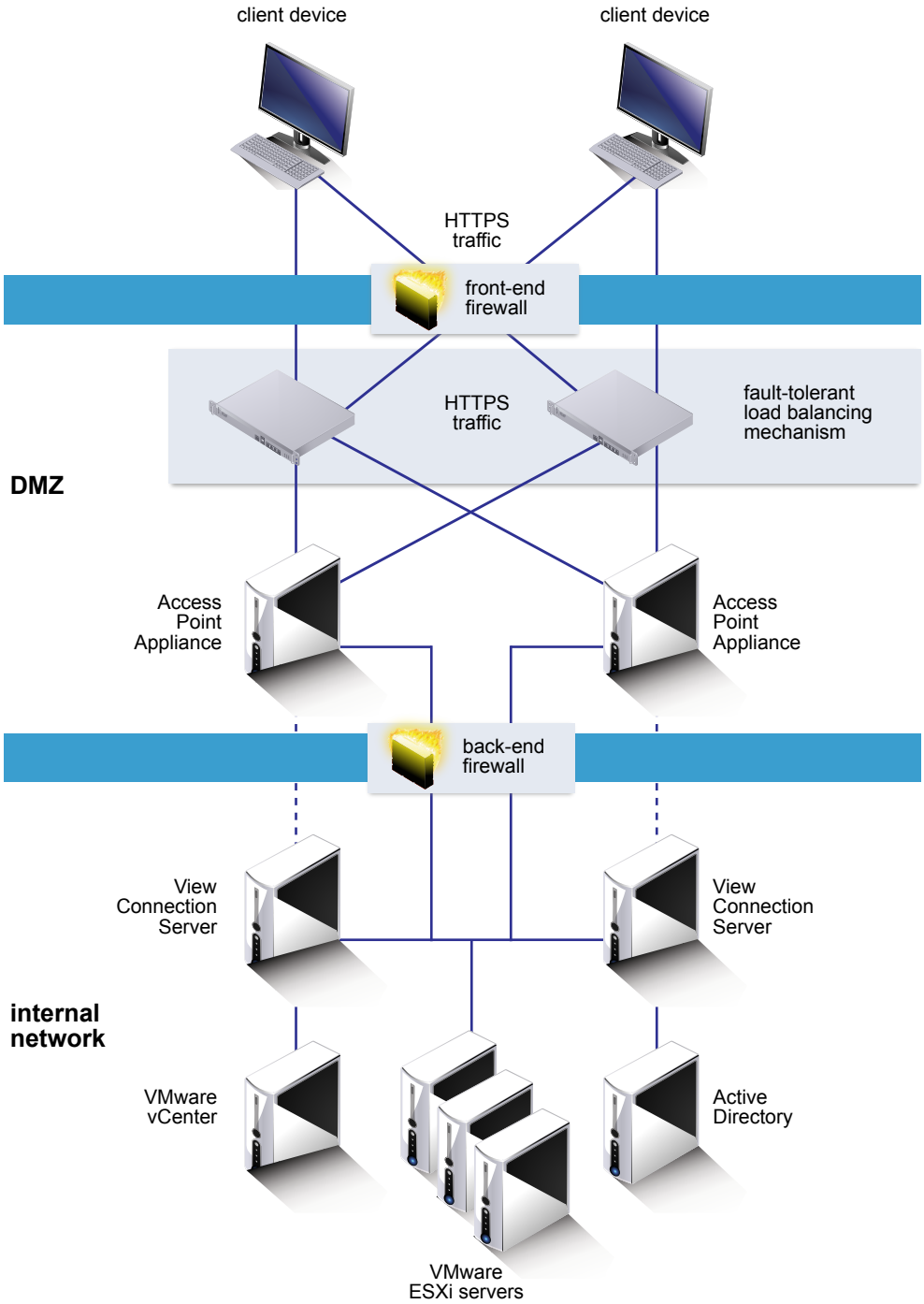
Figure 1-1. View Components and Protocols with Access Point



Firewall policy strictly controls inbound communications from DMZ services, which greatly reduces the risk of compromising your internal network.

The following figure shows an example of a configuration that includes front-end and back-end firewalls.

Figure 1-2. Dual Firewall Topology



Front-End Firewall Rules

To allow external client devices to connect to an Access Point appliance within the DMZ, the front-end firewall must allow traffic on certain TCP and UDP ports.

Table 1-1. Front-End Firewall Rules

Source	Default Port	Protocol	Destination	Destination Port	Notes
Horizon Client	TCP Any	HTTP	Access Point appliance	TCP 80	(Optional) External client devices connect to an Access Point appliance within the DMZ on TCP port 80 and are automatically directed to HTTPS. For information about the security considerations related to letting users connect with HTTP rather than HTTPS, see the *View Security* guide.
Horizon Client	TCP Any	HTTPS	Access Point appliance	TCP 443	External client devices connect to an Access Point appliance within the DMZ on TCP port 443.
Horizon Client	TCP Any UDP Any	PCoIP	Access Point appliance	TCP 4172 UDP 4172	External client devices connect to an Access Point appliance within the DMZ on TCP port 4172 and UDP port 4172 to communicate with a remote desktop or application over PCoIP.
Access Point appliance	UDP 4172	PCoIP	Horizon Client	UDP Any	Access Point appliances send PCoIP data back to an external client device from UDP port 4172. The destination UDP port is the source port from the received UDP packets. Because these packets contain reply data, it is normally unnecessary to add an explicit firewall rule for this traffic.
Client Web browser	TCP Any	HTTPS or Blast	Access Point appliance	TCP 8443	If you use HTML Access, the external Web client connects to an Access Point appliance within the DMZ on HTTPS port 8443 to communicate with remote desktops.

Back-End Firewall Rules

To allow an Access Point appliance to communicate with a View Connection Server instance or load balancer that resides within the internal network, the back-end firewall must allow inbound traffic on certain TCP ports. Behind the back-end firewall, internal firewalls must be similarly configured to allow remote desktops applications and View Connection Server instances to communicate with each other.

Table 1-2. Back-End Firewall Rules

Source Port	Default Port	Protocol	Destination	Destination Port	Notes
Access Point appliance	TCP Any	HTTPS	View Connection Server or load balancer	TCP 443	Access Point appliances connect on TCP port 443 to communicate with a View Connection Server instance or load balancer in front of multiple View Connection Server instances.
Access Point appliance	TCP Any	RDP	Remote desktop	TCP 3389	Access Point appliances connect to remote desktops on TCP port 3389 to exchange RDP traffic.
Access Point appliance	TCP Any	MMR or CDR	Remote desktop	TCP 9427	Access Point appliances connect to remote desktops on TCP port 9427 to receive MMR (multimedia redirection) or CDR (client drive redirection) traffic.
Access Point appliance	TCP Any UDP Any	PCoIP	Remote desktop or application	TCP 4172 UDP 4172	Access Point appliances connect to remote desktops and applications on TCP port 4172 and UDP port 4172 to exchange PCoIP traffic.
Remote desktop or application	UDP 4172	PCoIP	Access Point appliance	UDP Any	Remote desktops and applications send PCoIP data back to an Access Point appliance from UDP port 4172 . The destination UDP port will be the source port from the received UDP packets and so as this is reply data, it is normally unnecessary to add an explicit firewall rule for this.

Table 1-2. Back-End Firewall Rules (Continued)

Source Port	Default Port	Protocol	Destination	Destination Port	Notes
Access Point appliance	TCP Any	USB-R	Remote desktop	TCP 32111	Access Point appliances connect to remote desktops on TCP port 32111 to exchange USB redirection traffic between an external client device and the remote desktop.
Access Point appliance	TCP Any	HTTPS	Remote desktop	TCP 22443	If you use HTML Access, Access Point appliances connect to remote desktops on HTTPS port 22443 to communicate with the Blast agent.

NOTE Access Point optionally listens on TCP port 9443 for the admin REST API traffic and optionally sends Syslog events on a default UDP port of 514. If there is a firewall in place for this communication, these ports must not be blocked.

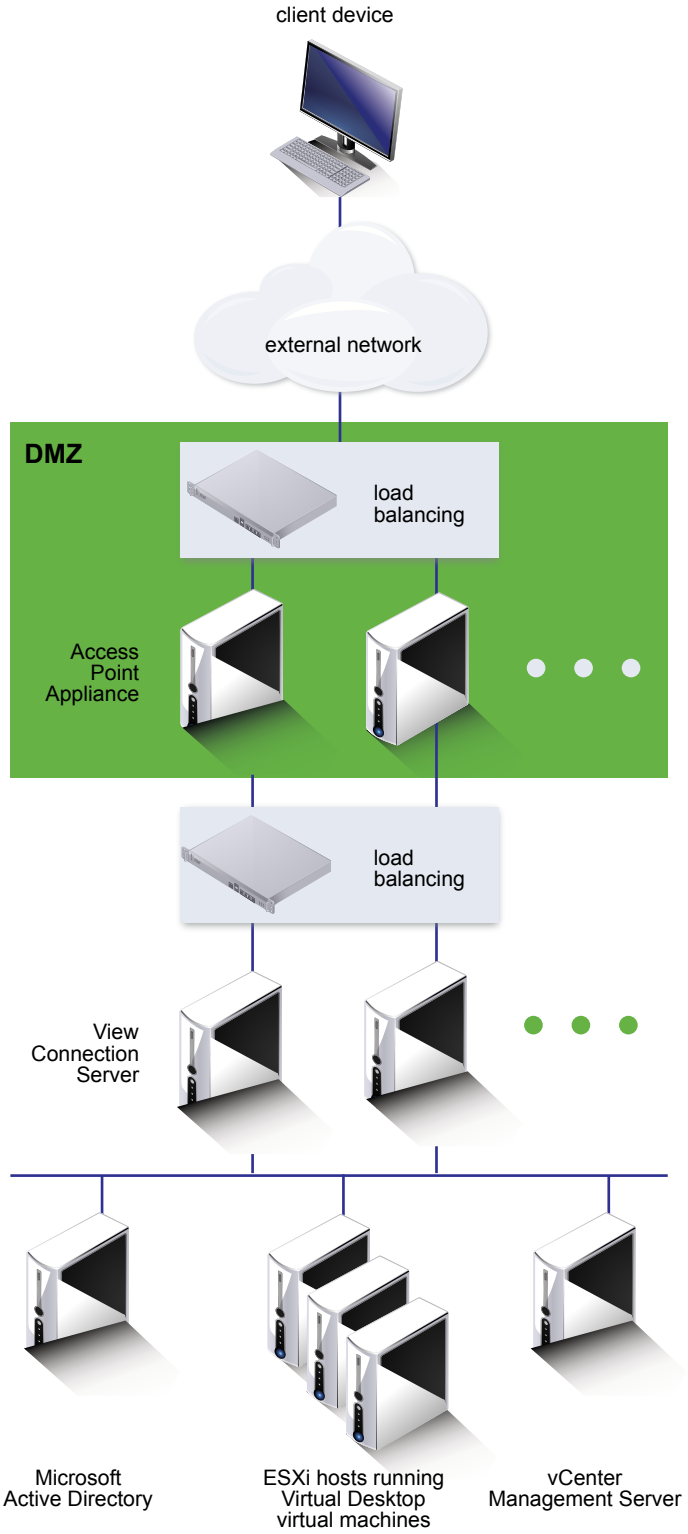
Access Point Topologies

You can implement any of several different topologies.

An Access Point appliance in the DMZ can be configured to point to either a View Connection Server instance or a load balancer that fronts a group of View Connection Server instances. Access Point appliances work with standard third-party load balancing solutions that are configured for HTTPS.

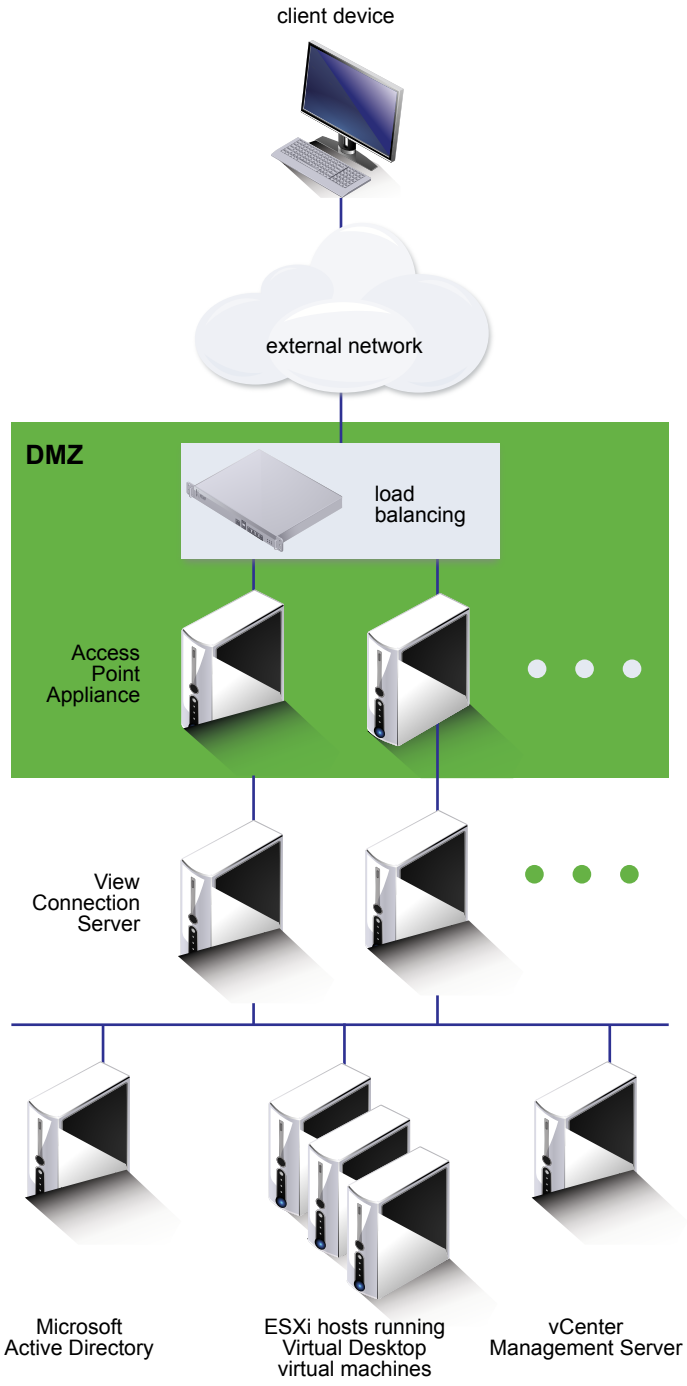
If the Access Point appliance points to a load balancer in front of the View Connection Server instances, the selection of the View Connection Server instance is dynamic. For example, the load balancer might make a selection based on availability and the load balancer's knowledge of the number of current sessions on each View Connection Server instance. The View Connection Server instances inside the corporate firewall usually already have a load balancer in order to support internal access. With Access Point, you can point the Access Point appliance to this same load balancer that is often already being used.

Figure 1-3. Access Point Appliance Pointing to a Load Balancer



You can alternatively have one or more Access Point appliances point to an individual View Connection Server instance, just as was previously done with View security servers. In both approaches, use a load balancer in front of two or more Access Point appliances in the DMZ.

Figure 1-4. Access Point Appliance Pointing to a View Connection Server Instance



System Requirements and Deployment 2

You deploy an Access Point appliance in much the same way that you deploy other VMware virtual appliances.

This chapter includes the following topics:

Access Point System Requirements

To deploy the Access Point appliance, ensure your system meets the hardware and software requirements.

Software Requirements

Access Point 2.0 is designed to be part of the Horizon 6 version 6.2 release.

- Horizon 6 servers: During an upgrade of these components, make sure the View Connection Server instances are upgraded to 6.2 before using Access Point appliances. Access Point is not designed to interoperate with earlier versions of Connection Server.
- vSphere ESX/ESXi hosts and vCenter Server: Access Point appliances must be deployed on a version of vSphere that is the same as a version supported for Horizon 6.2.

  For details about which versions of View are compatible with which versions of vCenter Server and ESXi, see the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
- Horizon Client: Although VMware recommends that you upgrade to the latest version of the clients to get new features and performance improvements, Access Point 2.0 is designed to work with all client versions that are supported with View Connection Server 6.2 and View Agent 6.2.

Hardware Requirements

The OVF package for the Access Point appliance automatically selects the virtual machine configuration that Access Point requires. Although you can change these settings, VMware recommends that you not change the CPU, memory, or disk space to smaller values than the default OVF settings.

Networking Requirements

You can use one, two, or three network interfaces, and Access Point requires a separate static IP address for each. Many DMZ implementations use separated networks to secure the different traffic types. Configure Access Point according to the network design of the DMZ in which it is deployed.

- One network interface is appropriate for POCs (proof of concept) or testing. With one NIC, external, internal, and management traffic are all on the same subnet.
- With two network interfaces, external traffic is on one subnet, and internal and management traffic are on another subnet.
- Using three network interfaces is the most secure option. With a third NIC, external, internal, and management traffic all have their own subnets.

IMPORTANT Verify that you have assigned an IP pool to each network. The Access Point appliance can then pick up the subnet mask and gateway settings at deployment time. To add an IP pool, in vCenter Server, if you are using the native vSphere Client, go to the **IP Pools** tab of the data center. Alternatively, if you are using the vSphere Web Client, you can create a network protocol profile. Go to the **Manage** tab of the data center and select the **Network Protocol Profiles** tab. For more information, see Configuring Protocol Profiles for Virtual Machine Networking.

Preparing View Connection Server for Use with Access Point

Administrators must perform specific tasks to ensure that View Connection Server works correctly with Access Point.

- If you plan to use a secure tunnel connection for client devices, disable the secure tunnel for View Connection Server. In View Administrator, go to the Edit View Connection Server Settings dialog box and deselect the check box called **Use secure tunnel connection to machine**. By default, the secure tunnel is enabled on the Access Point appliance.
- Disable the PCoIP secure gateway for View Connection Server. In View Administrator, go to the Edit View Connection Server Settings dialog box and deselect the check box called **Use PCoIP Secure Gateway for PCoIP connections to machine**. By default, the PCoIP secure gateway is enabled on the Access Point appliance.
- Disable the Blast secure gateway for View Connection Server. In View Administrator, go to the Edit View Connection Server Settings dialog box and deselect the check box called **Use Blast Secure Gateway for HTML Access to machine**. By default, the Blast secure gateway is enabled on the Access Point appliance.
- To use two-factor authentication with Horizon Client, such as RSA SecurID or RADIUS authentication, you must enable this feature on View Connection Server. See the topics about two-factor authentication in the *View Administration* document.

Deploy the Access Point Appliance

The simplest way to deploy the Access Point appliance is by logging in to vCenter Server and using the Deploy OVF Template wizard. Logging in directly to an ESXi host to use the deployment wizard is not supported.

If you would rather use the command-line VMware OVF Tool to deploy the appliance, see "Using VMware OVF Tool to Deploy the Access Point Appliance," on page 20. With this tool, you can set advanced properties that are not available in the deployment wizard.

NOTE For production environments, VMware recommends that you use VMware OVF Tool rather than the deployment wizard so that you can ensure a repeatable installation through scripting. This method also allows advanced settings such as the configuration of the external URLs and the TLS/SSL server certificate to be applied at deployment time. The interactive deployment wizard does not include these advanced settings.

Prerequisites

- Familiarize yourself with the deployment options available in the wizard. See "Access Point Deployment Properties," on page 24. The following options are required: static IP address for the Access Point appliance, IP address of the DNS server, password for the root user, and the URL of the View Connection Server instance or load balancer that this Access Point appliance will point to.
- Determine how many network interfaces and static IP addresses to configure for the Access Point appliance. See "Networking Requirements," on page 16.

  IMPORTANT If you use the vSphere Web Client, you can also specify the DNS server, gateway, and netmask addresses for each network. If you use the native vSphere Client, verify that you have assigned an IP pool to each network. To add an IP pool, in vCenter Server, if you are using the native vSphere Client, go to the **IP Pools** tab of the data center. Alternatively, if you are using the vSphere Web Client, you can create a network protocol profile. Go to the **Manage** tab of the data center and select the **Network Protocol Profiles** tab. For more information, see Configuring Protocol Profiles for Virtual Machine Networking.

- Verify that you can log in to vSphere Client or vSphere Web Client as a user with **system administrator** privileges. For example, you might log in as the user administrator@vsphere.local.

  If you use vSphere Web Client, use a supported browser. See the "Client Integration Plug-In Software Requirements" topic in the vSphere documentation center for your version of vSphere.
- Verify that the data store you plan to use for the appliance has enough free disk space and meets other system requirements. The download size of the virtual appliance is 1.4GB. By default, for a thin-provisioned disk, the appliance requires 2.5GB, and a thick-provisioned disk requires 20GB. Also see "Access Point System Requirements," on page 15.
- Download the `.ova` installer file for the Access Point appliance from the VMware Web site at https://my.vmware.com/web/vmware/downloads, or determine the URL to use (example: `http://example.com/vapps/euc-access-point-2.0.0.0-xxxxxxx_OVF10.ova`).
- If you plan to use the vSphere Web Client, verify that the Client Integration plug-in is installed. For more information, see the vSphere documentation. For example, for vSphere 6, see Install the Client Integration Plug-in. If you do not install this plug-in before you start the deployment wizard, the wizard prompts you to install the plug-in, which requires closing your browser and exiting the wizard.

Procedure

1 Use the native vSphere Client or the vSphere Web Client to log in to a vCenter Server instance.

2 Select a menu command for launching the Deploy OVF Template wizard.

Option	Menu Command
vSphere Client	Select **File > Deploy OVF Template**.
vSphere Web Client	Select any inventory object that is a valid parent object of a virtual machine, such as a datacenter, folder, cluster, resource pool, or host, and from the **Actions** menu, select **Deploy OVF Template**.

3 On the Select Source page of the wizard, browse to the location of the `.ova` file that you downloaded or enter a URL and click **Next**.

A details page appears, which tells how much disk space the appliance requires.

4 Follow the wizard prompts, and take the following guidelines into consideration as you complete the wizard.

Text on each wizard page explains each control. In some cases, the text changes dynamically as you select various options.

NOTE If you use the vSphere Web Client, for assistance you can also click the context-sensitive help button, which is a question mark (**?**) icon in the upper-right corner of the wizard.

Option	Description
Select a deployment configuration	You can use one, two, or three network interfaces (NICs), and Access Point requires a separate static IP address for each. Many DMZ implementations use separated networks to secure the different traffic types. Configure Access Point according to the network design of the DMZ in which it is deployed.
Disk format	For evaluation and testing environments, select the Thin Provision format. For production environments, select one of the Thick Provision formats. Thick Provision Eager Zeroed is a type of thick virtual disk format that supports clustering features such as fault tolerance but takes much longer to create than other types of virtual disks.
VM storage policy	(vSphere Web Client only) This option is available if storage policies are enabled on the destination resource.

Option	Description
Setup Networks/Network Mapping	If you are using vSphere Web Client, the Setup Networks page allows you to map each NIC to a network and specify protocol settings. a Select the first row in the table (**Internet**) and then click the down arrow to select the destination network. After you select the row, you can also enter IP addresses for the DNS server, gateway, and netmask in the lower portion of the window. b If you are using more than one NIC, select the next row (**ManagementNetwork**), select the destination network, and then you can enter the IP addresses for the DNS server, gateway, and netmask for that network. If you are using only one NIC, all the rows are mapped to the same network. c If you have a third NIC, also select the third row and complete the settings. If you are using only two NICs, for this third row (**BackendNetwork**), select the same network that you used for **ManagementNetwork**. With the vSphere Web Client, a network protocol profile is automatically created after you complete the wizard if one does not already exist. If you use the native vSphere Client (rather than the Web Client), the Network Mapping page allows you to map each NIC to a network, but there are no fields for specifying the DNS server, gateway, and netmask addresses. As described in the prerequisites, you must already have assigned an IP pool to each network or created a network protocol profile.
Customize template	The text boxes on this page are specific to Access Point and might not be required for other types of virtual appliances. Text in the wizard page explains each setting. If the text is truncated on the right side of the wizard, resize the window by dragging from the lower-right corner. You must enter values in the following text boxes: ■ **External IP address** ■ **DNS server addresses** ■ **Management network IP address** if you specified 2 NICs, and **Backend network IP address** if you specified 3 NICs ■ **Password for the root user of this VM** ■ **Horizon server URL** ■ **Horizon server thumbprints** if the Horizon server does not already have a server certificate that is issued by a trusted certificate authority All other settings are either optional or already have a default setting entered. VMware strongly recommends that you also specify a password for the **Admin credentials for REST API** text box. Note the password requirements listed on the wizard page.

5 On the Ready to Complete page, select **Power on after deployment**, and click **Finish**.

A Deploy OVF Template task appears in the vCenter Server status area so that you can monitor deployment. You can also open a console on the virtual machine to view the console messages that are displayed during system boot. A log of these messages is also available in the file `/var/log/boot.msg`.

6 When deployment is complete, verify that end users will be able to connect to the appliance by opening a browser and entering the following URL:

`https://FQDN-of-AP-appliance`

In this URL, *FQDN-of-AP-appliance* is the DNS-resolvable, fully qualified domain name of the Access Point appliance.

If deployment was successful, the Horizon Web Portal appears. If deployment was not successful, you can delete the appliance virtual machine and deploy the appliance again. The most common error is not entering certificate thumbprints correctly.

7 To verify that the admin credentials for accessing the REST API were set correctly, open a browser, enter the following URL, and enter the credentials for the admin user.

`https://FQDN-of-AP-appliance:9443/rest/swagger.yaml`

A page containing the Access Point REST API specification appears. If you get an error message, you can either deploy the appliance again and be sure to follow the requirements for the password, or you can log in to the Access Point virtual machine and set the admin password using the REST API.

The Access Point appliance is deployed and starts automatically.

What to do next

Configure security certificates for Access Point. If you did not set the admin credentials correctly for the REST API, you can set them by using the procedure "Reset the admin Password for the Access Point REST API," on page 28.

IMPORTANT Configure the clock (UTC) on the Access Point appliance so that the appliance has the correct time. For example, verify that the ESXi host's time is synchronized with an NTP server, and verify that VMware Tools, which is running in the appliance virtual machine, synchronizes the time on the virtual machine with the time on the ESXi host.

Using VMware OVF Tool to Deploy the Access Point Appliance

As an alternative to using the deployment wizard, you can use this command-line tool to deploy Access Point. Using this tool allows you to set more configuration options than are available in the deployment wizard.

For production environment deployments, VMware recommends using OVF Tool for a scripted, unattended deployment that predictably deploys and fully configures the appliance. You can download the VMware OVF Tool and its documentation by going to https://www.vmware.com/support/developer/ovf/. Besides the standard commands described in the OVF Tool documentation, you can use Access Point-specific options. For a list of the available properties and options, see "Access Point Deployment Properties," on page 24.

Prerequisites for Access Point Deployment

- Familiarize yourself with the deployment options available. See "Access Point Deployment Properties," on page 24. The following options are required: static IP address for the Access Point appliance, IP address of the DNS server, password for the root user, and the URL of the View Connection Server instance or load balancer that this Access Point appliance will point to.
- Determine how many network interfaces and static IP addresses to configure for the Access Point appliance. See "Networking Requirements," on page 16.

  IMPORTANT Verify that you have assigned an IP pool to each network. The Access Point appliance can then pick up the subnet mask and gateway settings at deployment time. To add an IP pool, in vCenter Server, if you are using the native vSphere Client, go to the **IP Pools** tab of the data center. Alternatively, if you are using the vSphere Web Client, you can create a network protocol profile. Go to the **Manage** tab of the data center and select the **Network Protocol Profiles** tab. For more information, see Configuring Protocol Profiles for Virtual Machine Networking.

- Verify that the data store you plan to use for the appliance has enough free disk space and meets other system requirements. The download size of the virtual appliance is 1.4GB. By default, for a thin-provisioned disk, the appliance requires 2.5GB, and a thick-provisioned disk requires 20GB. Also see "Access Point System Requirements," on page 15.
- Download the `.ova` installer file for the Access Point appliance from the VMware Web site at https://my.vmware.com/web/vmware/downloads, or determine the URL to use (example: `http://example.com/vapps/euc-access-point-2.0.0.0-xxxxxxx_OVF10.ova`).

Example OVF Tool Command That Uses Access Point Deployment Properties

Following is an example of a command for deploying an Access Point appliance using OVF Tool on a Windows client machine:

```
ovftool --X:enableHiddenProperties ^
--powerOffTarget ^
--powerOn ^
--overwrite ^
--vmFolder=folder1 ^
--net:Internet="VM Network" ^
--net:ManagementNetwork="VM Network" ^
--net:BackendNetwork="VM Network" ^
-ds=PERFORMANCE-X ^
--name=name1 ^
--ipAllocationPolicy=fixedPolicy ^
--deploymentOption=onenic ^
--prop:ip0=10.20.30.41 ^
--prop:DNS=192.0.2.1 ^
--prop:adminPassword=P@ssw0rd ^
--prop:rootPassword=vmware ^
--prop:viewDestinationURL=https://192.0.2.2 ^
--prop:viewDestinationURLThumbprints="sha1=b6 77 dc 9c 19 94 2e f1 78 f0 ad 4b ec 85 d1 7a f8 8b
dc 34" ^
euc-access-point-2.0.0.0-xxxxxxx_OVF10.ova ^
vi://root:password@vc.example.com/ExampleDC/host/ap
```

NOTE The caret characters at the ends of the lines are escape characters for line continuation on Windows, which can be used in a BAT script. You can alternatively just type the entire command on one line.

Following is an example of a command for deploying an Access Point appliance using OVF Tool on a Linux client machine:

```
ovftool --X:enableHiddenProperties \
--powerOffTarget \
--powerOn \
--overwrite \
--vmFolder=folder1 \
--net:Internet="VM Network" \
--net:ManagementNetwork="VM Network" \
--net:BackendNetwork="VM Network" \
-ds=PERFORMANCE-X \
--name=name1 \
--ipAllocationPolicy=fixedPolicy \
--deploymentOption=onenic \
--prop:ip0=10.20.30.41 \
--prop:DNS=192.0.2.1 \
--prop:adminPassword=P@ssw0rd \
--prop:rootPassword=vmware \
--prop:viewDestinationURL=https://192.0.2.2 \
```

```
--prop:viewDestinationURLThumbprints="sha1=b6 77 dc 9c 19 94 2e f1 78 f0 ad 4b ec 85 d1 7a f8 8b
dc 34" \
euc-access-point-2.0.0.0-xxxxxxx_OVF10.ova \
vi://root:password@vc.example.com/ExampleDC/host/ap
```

NOTE The backslashes at the ends of the lines are escape characters for line continuation on Linux, which can be used in a Linux shell script. You can alternatively just type the entire command on one line.

If you use this command, you can then use the Access Point admin REST API to configure additional settings such as the security certificate and secure gateways. Alternatively, you can use the `settingsJSON` property to configure these settings at deployment time.

Example Using the settings.JSON Property

In addition to the deployment properties shown in the previous example, you can use the `settingsJSON` property to pass a JSON string directly to the `EdgeServiceSettings` resource in the Access Point admin REST API. In this manner, you can use the OVF Tool to set configuration properties during deployment that must otherwise be set by using the REST API after deployment.

The following example shows how to use the `settingsJSON` property to enable the View edge service, so that Access Point can point to and use a Horizon server. In addition to specifying the Horizon server URL and the View Connection Server thumbprint, the `settingsJSON` property sets the external URLs for the secure gateways. This example uses escape characters for running the command on a Windows client machine.

```
ovftool --X:enableHiddenProperties ^
--powerOffTarget ^
--powerOn ^
--overwrite ^
--vmFolder=folder1 ^
--net:Internet="VM Network" ^
--net:ManagementNetwork="VM Network" ^
--net:BackendNetwork="VM Network" ^
-ds="PERFORMANCE-X" ^
--name=name1 ^
--ipAllocationPolicy=fixedPolicy ^
--deploymentOption=onenic ^
--prop:ip0=10.20.30.41 ^
--prop:DNS=192.0.2.1 ^
--prop:adminPassword=P@ssw0rd ^
--prop:rootPassword=vmware ^
--prop:settingsJSON="{\"edgeServiceSettingsList\": { \"edgeServiceSettingsList\": [ ^
{ ^
\"identifier\": \"VIEW\", ^
\"enabled\": true, ^
\"proxyDestinationUrl\": \"https://192.0.2.2\", ^
\"proxyDestinationUrlThumbprints\": \"sha1=b6 77 dc 9c 19 94 2e f1 78 f0 ad 4b ec 85 d1 7a f8 8b
dc 34\", ^
\"pcoipEnabled\": true, ^
\"pcoipExternalUrl\": \"10.20.30.40:4172\", ^
\"blastEnabled\": true, ^
\"blastExternalUrl\": \"https://ap1.example.com:8443\", ^
\"tunnelEnabled\": true, ^
\"tunnelExternalUrl\": \"https://ap1.example.com:443\", ^
```

```
\"proxyPattern\":\"/\" } ] }^
}" ^
euc-access-point-2.0.0.0-xxxxxxx_OVF10.ova ^
vi://root:password@vc.example.com/ExampleDC/host/ap
```

The following example uses escape characters for running the command on a Linux client machine. This example also shows how to use the `settingsJSON` property to enable the View edge service, so that Access Point can point to and use a Horizon server. In addition to specifying the Horizon server URL and the View Connection Server thumbprint, the `settingsJSON` property sets the external URLs for the secure gateways.

```
ovftool --X:enableHiddenProperties \
--powerOffTarget \
--powerOn \
--overwrite \
--vmFolder=folder1 \
--net:Internet="VM Network" \
--net:ManagementNetwork="VM Network" \
--net:BackendNetwork="VM Network" \
-ds=PERFORMANCE-X \
--name=name1 \
--ipAllocationPolicy=fixedPolicy \
--deploymentOption=onenic \
--prop:ip0=10.20.30.41 \
--prop:DNS=192.0.2.1 \
--prop:adminPassword=P@ssw0rd \
--prop:rootPassword=vmware \
--prop:settingsJSON='{"edgeServiceSettingsList": { "edgeServiceSettingsList": [ \
{ \
"identifier": "VIEW", \
"enabled": true, \
"proxyDestinationUrl": "https://192.0.2.2", \
"proxyDestinationUrlThumbprints": "sha1=b6 77 dc 9c 19 94 2e f1 78 f0 ad 4b ec 85 d1 7a f8 8b dc
34", \
"pcoipEnabled": true, \
"pcoipExternalUrl": "10.20.30.40:4172", \
"blastEnabled": true, \
"blastExternalUrl": "https://ap1.example.com:8443", \
"tunnelEnabled": true, \
"tunnelExternalUrl": "https://ap1.example.com:443", \
"proxyPattern":"/"  } ] } \
}' \
euc-access-point-2.0.0.0-xxxxxxx_OVF10.ova  \
vi://root:password@vc.example.com/ExampleDC/host/ap
```

Important You must configure the external URLs for the secure tunnel, the PCoIP Secure Gateway, and the Blast Secure Gateway at deployment time. You can do this configuration either by using OVF Tool or through the REST API. This configuration step must be done before you can use Access Point for View traffic. For more information about these URLs, see "Configuring the Secure Gateways," on page 36.

For a list of the REST API properties for configuring Access Point, see "REST API Properties for Access Point," on page 29.

Access Point Deployment Properties

For your convenience, almost all deployment properties can be set using either the deployment wizard or the OVF Tool command-line interface.

For information about how to specify these properties by using the deployment wizard, see "Deploy the Access Point Appliance," on page 17. To specify the properties by using the OVF Tool command-line interface, see "Using VMware OVF Tool to Deploy the Access Point Appliance," on page 20.

Table 2-1. Deployment Options Access Point

Deployment Property	OVF Tool Option	Description
Deployment configuration	`--deploymentOption {onenic|twonic|threenic}`	Specifies how many network interfaces are available in the Access Point virtual machine. By default, this property is not set, which means that one NIC is used.
External (Internet-facing) IP address	`--prop:ip0=`*external-ip-address*	(Required) Specifies public IPv4 address used for accessing this virtual machine on the Internet. **NOTE** The computer name is set through a DNS query of this Internet IPv4 address. Default: none.
Management network IP address	`--prop:ip1=`*management-ip-address*	Specifies the IP address of the interface that is connected to the management network. If not configured, the administration server listens on the Internet-facing interface. Default: none.
Back-end network IP address	`--prop:ip2=`*back-end-ip-address*	Specifies the IP address of the interface that is connected to the back-end network. If not configured, network traffic sent to the back-end systems is routed through the other network interfaces. Default: none.
DNS server addresses	`--prop:DNS=`*ip-of-name-server1*[*ip-of-name-server2* ...]	(Required) Specifies one or more space-separated IPv4 addresses of the domain name servers for this virtual machine (example: 192.0.2.1 192.0.2.2). You can specify up to three servers. By default, this property is not set, which means that the system uses the DNS server that is associated with the Internet-facing NIC. **CAUTION** If you leave this option blank and if no DNS server is associated with the Internet-facing NIC, the appliance will not be deployed correctly.
Password for the root user	`--prop:rootPassword=`*password*	(Required) Specifies the password for the root user of this virtual machine. The password must be a valid Linux password. Default: none.
Password for the admin user	`--prop:adminPassword=`*password*	If you do not set this password, you will not be able to access the REST API on the Access Point appliance. Passwords must be at least 8 characters long, contain at least one uppercase and one lowercase letter, one digit, and one special character, which includes ! @ # $ % * ( ). Default: none.

Table 2-1. Deployment Options Access Point (Continued)

Deployment Property	OVF Tool Option	Description
Locale to use for localized messages	`--prop:locale=`*locale-code*	(Required) Specifies the locale to use when generating error messages. ■ **`en_US`** for English ■ **`ja_JP`** for Japanese ■ **`fr_FR`** for French ■ **`de_DE`** for German ■ **`zh_CN`** for Simplified Chinese ■ **`zh_TW`** for Traditional Chinese ■ **`ko_KR`** for Korean Default: en_US.
Syslog server URL	`--prop:syslogUrl=`*url-of-syslog-server*	Specifies the Syslog server used for logging Access Point events. This value can be a URL or a host name or IP address. The scheme and port number are optional (example: syslog://server.example.com: 514). By default, this property is not set, which means that no events are logged to a syslog server.
Horizon server URL	`--prop:viewDestinationURL=`*URL*	(Required) Specifies the destination URL of the load balancer or View Connection Server that the Access Point appliance directs traffic to. The destination URL must contain the protocol, host name or IP address, and port number (example: https://load-balancer.example.com: 443) Default: none.
Horizon Connection Server thumbrpints	`--prop:viewDestinationURLThumbprints=` *thumbprint-list*	If you do not provide a comma-separated list of thumbrpints, the server certificates must be issued by a trusted CA. The format includes the algorithm (sha1 or md5) and the hexadecimal thumbprint digits (example: sha1=b6 77 dc 9c 19 94 2e f1 78 f0 ad 4b ec 85 d1 7a f8 8b dc 34). To find these properties, browse to the View Connection Server, click the lock icon in the address bar, and view the certificate details. Default: none.

You can also use the `settingsJSON` property to specify other REST API configuration settings using OVF Tool, such as for configuring the external URLs for the secure gateways. For more information, see "Example Using the settings.JSON Property," on page 22.

Configuring Access Point 3

You use the Access Point REST API to configure Access Point.

IMPORTANT After deployment, the first configuration task is to configure the clock (UTC) on the Access Point appliance so that the appliance has the correct time. For example, verify that the ESXi host's time is synchronized with an NTP server, and verify that VMware Tools, which is running in the appliance virtual machine, synchronizes the time on the virtual machine with the time on the ESXi host. Use vCenter Server, rather than the REST API for this configuration task.

This chapter includes the following topics:

Using the Access Point REST API

Although you can configure many settings during appliance deployment, after you deploy the Access Point appliance, you must use the Access Point REST API to change or add configuration settings.

The specification for the Access Point REST API is available at the following URL on the virtual machine where Access Point is installed: `https://access-point-appliance.example.com:9443/rest/swagger.yaml`

You can use any REST client application, such as `curl` or `postman`. For example, the following command uses a `curl` client to retrieve the Access Point configuration:

```
curl -k -u 'admin:P@ssw0rd' https://access-point-appliance.example.com:
9443/rest/v1/config/settings
```

In this example, *P@ssw0rd* is the password for the admin user and *access-point-appliance.example.com* is the fully qualified domain name of the Access Point appliance. As a best practice with regards to security, you can omit the password for the admin user from any scripts. When the password is omitted, the `curl` command prompts you for the password and ensures that no passwords are inadvertently stored in script files.

You also use JSON requests to invoke the Access Point REST API and make configuration changes. The following example shows a configuration JSON for the View edge service:

```
{
  "identifier": "VIEW",
  "enabled": true,
  "proxyDestinationUrl": "https://192.0.2.1",
  "proxyDestinationUrlThumbprints": "sha1=b6 77 dc 9c 19 94 2e f1 78 f0 ad 4b ec 85 d1 7a f8 8b
dc 34",
```

```
  "pcoipEnabled": true,
  "pcoipExternalUrl": "10.20.30.40:4172",
  "blastEnabled": true,
  "blastExternalUrl": "https://ap1.example.com:8443",
  "tunnelEnabled": true,
  "tunnelExternalUrl": "https://ap1.example.com:443"
  "proxyPattern": "/"
}
```

This example shows the following settings:

- The type of edge service being configured (`identifier`) and enabled (`enabled`).

  Setting `identifier` to `VIEW` means that Access Point can communicate with View Connection Server. For this release, `VIEW` is the only choice available.

- The address of the View Connection Server or load balancer (`proxyDestinationUrl`).
- The Horizon server's security certificate thumbprint (`proxyDestinationUrlThumbprints`).
- Settings for enabling the PCoIP Secure Gateway, the Blast Secure Gateway, and the Secure Tunnel Gateway.
- The external URLs for the PCoIP Secure Gateway, the Blast Secure Gateway, and the Secure Tunnel Gateway.
- A setting for enabling HTML Access (`proxyPattern`).

NOTE When you create a JSON request, provide the complete set of properties for that resource. Any parameter that is not specified in the JSON call is reset to the default value. Alternatively, you can first retrieve the parameters and then change the JSON string to the new values.

Reset the admin Password for the Access Point REST API

If the password for the admin user is unknown, or if problems prevent you from logging in to the REST API to reset the password, you can use this procedure to reset the password.

Prerequisites

You must have the password for logging in to the virtual machine as the root user.

Procedure

1 Log in to the operating system of the Access Point appliance as the root user.

2 Enter the following commands:

```
echo 'adminPassword=P@ssw0rd' > /opt/vmware/gateway/conf/firstboot.properties
chown gateway /opt/vmware/gateway/conf/firstboot.properties
supervisorctl restart admin
```

In this example, **`P@ssw0rd`** is a password that is at least 8 characters long, contains at least one uppercase and one lowercase letter, one digit, and one special character, which includes ! @ # $ % * ( ).

When the admin server reboots, it generates the following message in the `/opt/vmware/gateway/logs/admin.log` file: `Successfully set initial settings from firstboot.properties`.

What to do next

You can now log in to the REST administration interface using the user name admin and the password that you just set (for example, P@ssw0rd).

REST API Properties for Access Point

Use the Access Point REST API properties to configure which security certificates, protocols, and cipher suites are used, set up smart card authentication, specify which View Connection Server instance to use, and more.

You can use the properties in the following tables to make configuration changes after the Access Point appliance is deployed, or you can alternatively use the OVF Tool property called `--X:enableHiddenProperties=settingsJSON` with some of these properties to configure the appliance at deployment time. For more information about how to use Access Point with the OVF Tool, see "Access Point Deployment Properties," on page 24.

System Settings

These settings are included in the SystemSettings resource. The URL is

`https://access-point-appliance.example.com:9443/rest/v1/config/system`

In this URL, *access-point-appliance.example.com* is the fully qualified domain name of the Access Point appliance.

Table 3-1. REST API Properties for the SystemSettings Resource

REST API Property	Description and Example	Default Value
`adminPassword`	Specifies the administrator password for accessing the REST API. Passwords must be at least 8 characters long, contain at least one uppercase and one lowercase letter, one digit, and one special character, which includes ! @ # $ % * ( ).	(Not set unless set by the deployment wizard or OVF Tool.)
`cipherList`	Configures the cipher list to restrict the use of certain cryptographic algorithms before establishing an encrypted TLS/SSL connection. This setting is used in conjunction with the settings for enabling various security protocols.	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA, SSL_RSA_WITH_RC4_128_SHA (The same default value as for View Connection Server 6.2.)
`ssl30Enabled`	Specifies whether the SSLv3.0 security protocol is enabled.	FALSE
`tls10Enabled`	Specifies whether the TLSv1.0 security protocol is enabled.	TRUE
`tls11Enabled`	Specifies whether the TLSv1.1 security protocol is enabled.	TRUE
`tls12Enabled`	Specifies whether the TLSv1.2 security protocol is enabled.	TRUE
`locale`	Specifies the local to use for localized messages. ■ **`en_US`** for English ■ **`ja_JP`** for Japanese ■ **`fr_FR`** for French ■ **`de_DE`** for German ■ **`zh_CN`** for Simplified Chinese ■ **`zh_TW`** for Traditional Chinese ■ **`ko_KR`** for Korean	en_US
`syslogUrl`	Specifies the Syslog server used for logging Access Point events. This value can be a URL or a host name or IP address. The scheme and port number are optional (example: syslog://server.example.com:514). .	(Not set unless set by the deployment wizard or OVF Tool.)

Server Certificate

These settings are included in the ServerCertificate resource. The URL is

`https://access-point-appliance.example.com:9443/rest/v1/config/certs/ssl`

In this URL, *access-point-appliance.example.com* is the fully qualified domain name of the Access Point appliance.

Table 3-2. REST API Properties for the ServerCertificate Resource

REST API Property	Description and Example	Default Value
`privateKeyPem`	Specifies the private key for the certificate in PEM format.	(System-generated)
`certChainPem`	Specifies the certificate chain in PEM format	(System-generated)

Edge Service Settings for View

These settings are included in the EdgeServiceSettings resource. The URL is

`https://access-point-appliance.example.com:9443/rest/v1/config/edgeservice/view`

In this URL, *access-point-appliance.example.com* is the fully qualified domain name of the Access Point appliance.

Table 3-3. REST API Properties for the EdgeServiceSettings resource for View

REST API Property	Description and Example	Default Value
`proxyDestinationUrl`	Specifies the URL of the Horizon server (load balancer or View Connection Server) that the Access Point appliance directs traffic to. This URL must contain the protocol, host name or IP address, and port number (example: https://load-balancer.example.com:443).	None
`proxyDestinationUrlThumbprints`	Specifies a list of Horizon Connection Server thumbrpints. If you do not provide a comma-separated list of thumbrpints, the server certificates must be issued by a trusted CA. The format includes the algorithm (sha1 or md5) and the hexadecimal thumbprint digits (example: sha1=b6 77 dc 9c 19 94 2e f1 78 f0 ad 4b ec 85 d1 7a f8 8b dc 34). To find these properties, browse to the View Connection Server, click the lock icon in the address bar, and view the certificate details.	None
`tunnelEnabled`	Specifies whether the View secure tunnel is enabled.	FALSE **NOTE** If you use VMware OVF Tool to specify a value for the `proxyDestinationUrl` property, `tunnelEnabled` gets set to TRUE.
`tunnelExternalUrl`	Specifies an external URL of the Access Point appliance, which clients will use for tunnel connections through the View Secure Gateway. This tunnel is used for RDP, USB, and Multimedia Redirection (MMR) traffic.	https://*appliance*:443 (*appliance* is the fully qualified domain name of the Access Point appliance.)

Table 3-3. REST API Properties for the EdgeServiceSettings resource for View (Continued)

REST API Property	Description and Example	Default Value
`pcoipEnabled`	Specifies whether the PCoIP Secure Gateway is enabled.	FALSE **NOTE** If you use VMware OVF Tool to specify a value for the `proxyDestinationUrl` property, `pcoipEnabled` gets set to TRUE.
`pcoipExternalUrl`	Specifies an external URL of the Access Point appliance, which clients will use for secure connections through the PCoIP Secure Gateway. This connection is used for PCoIP traffic.	*applianceIP*:4172 (*applianceIP* is the IPv4 address of the Access Point appliance.)
`blastEnabled`	Specifies whether the Blast Secure Gateway is enabled.	FALSE **NOTE** If you use VMware OVF Tool to specify a value for the `proxyDestinationUrl` property, `blastEnabled` gets set to TRUE.
`blastExternalUrl`	Specifies an external URL of the Access Point appliance, which allows end users to make secure connections from their Web browsers through the Blast Secure Gateway. This connection is used for the HTML Access feature.	https://*appliance*:8443 (*appliance* is the fully qualified domain name of the Access Point appliance.)
`proxyPattern`	Specifies the regular expression that matches URIs that should be forwarded to the Horizon server URL (proxyDestinationUrl). For View Connection Server, a forward slash (/) is a typical value for providing redirection to the HTML Access Web client when using the Access Point appliance.	None
`authMethods`	Specifies the type of authentication to use. Set this property to `certificate-auth` to change the authentication method to smart card:	By default, authentication is passed through to View Connection Server, which can be configured for AD password, RSA SecurID, RADIUS, or SAML.

Configuring TLS/SSL Certificates for Access Point Appliances

TLS/SSL is required for client connections to Access Point appliances. Client-facing Access Point appliances and intermediate servers that terminate TLS/SSL connections require TLS/SSL server certificates.

TLS/SSL server certificates are signed by a Certificate Authority (CA). A CA is a trusted entity that guarantees the identity of the certificate and its creator. When a certificate is signed by a trusted CA, users no longer receive messages asking them to verify the certificate, and thin client devices can connect without requiring additional configuration.

A default TLS/SSL server certificate is generated when you deploy an Access Point appliance. For production environments, VMware strongly recommends that you replace the default certificate as soon as possible. The default certificate is not signed by a trusted CA. Use the default certificate only in a non-production environment

Selecting the Correct Certificate Type

You can use various types of TLS/SSL certificates with Access Point. Selecting the correct certificate type for your deployment is crucial. Different certificate types vary in cost, depending on the number of servers on which they can be used.

Follow VMware security recommendations by using fully qualified domain names (FQDNs) for your certificates, no matter which type you select. Do not use a simple server name or IP address, even for communications within your internal domain.

Single Server Name Certificate

You can generate a certificate with a subject name for a specific server. For example: `dept.example.com`.

This type of certificate is useful if, for example, only one Access Point appliance needs a certificate.

When you submit a certificate signing request to a CA, you provide the server name that will be associated with the certificate. Be sure that the Access Point appliance can resolve the server name you provide so that it matches the name associated with the certificate.

Subject Alternative Names

A Subject Alternative Name (SAN) is an attribute that can be added to a certificate when it is being issued. You use this attribute to add subject names (URLs) to a certificate so that it can validate more than one server.

For example, three certificates might be issued for the Access Point appliances that are behind a load balancer: `ap1.example.com`, `ap2.example.com`, and `ap3.example.com`. By adding a Subject Alternative Name that represents the load balancer host name, such as `horizon.example.com` in this example, the certificate will be valid because it will match the host name specified by the client.

Wildcard Certificate

A wildcard certificate is generated so that it can be used for multiple services. For example: `*.example.com`.

A wildcard is useful if many servers need a certificate. If other applications in your environment in addition to Access Point appliances need TLS/SSL certificates, you can use a wildcard certificate for those servers, too. However, if you use a wildcard certificate that is shared with other services, the security of the VMware Horizon product also depends on the security of those other services.

Note You can use a wildcard certificate only on a single level of domain. For example, a wildcard certificate with the subject name `*.example.com` can be used for the subdomain `dept.example.com` but not `dept.it.example.com`.

Certificates that you import into the Access Point appliance must be trusted by client machines and must also be applicable to all instances of Access Point and any load balancer, either by using wildcards or by using Subject Alternative Name (SAN) certificates.

Convert Certificate Files to One-Line PEM Format

To use the Access Point REST API to configure certificate settings, you must convert the certificate into PEM-format files for the certificate chain and the private key, and you must then convert the `.pem` files to a one-line format that includes embedded newline characters.

When configuring Access Point, there are three possible types of certificates you might need to convert.

- You should always install and configure a TLS/SSL server certificate for the Access Point appliance.
- If you plan to use smart card authentication, you must install and configure the trusted CA issuer certificate for the certificate that will be put on the smart card.

- If you plan to use smart card authentication, VMware recommends that you install and configure a root certificate for the signing CA for the SAML server certificate that is installed on the Access Point appliance.

For all of these types of certificates, you perform the same procedure to convert the certificate into a PEM-format file that contains the certificate chain. For TLS/SSL server certificates and root certificates, you also convert each file to a PEM file that contains the private key. You must then convert each `.pem` file to a one-line format that can be passed in a JSON string to the Access Point REST API.

Prerequisites

- Verify that you have the certificate file. The file can be in PKCS#12 (`.p12` or `.pfx`) format or in Java JKS or JCEKS format.
- Familiarize yourself with the `openssl` command-line tool that you will use to convert the certificate. See https://www.openssl.org/docs/apps/openssl.html.
- If the certificate is in Java JKS or JCEKS format, familiarize yourself with the Java `keytool` command-line tool to first convert the certificate to `.p12` or `.pks` format before converting to `.pem` files.

Procedure

1 If your certificate is in Java JKS or JCEKS format, use `keytool` to convert the certificate to `.p12` or `.pks` format.

IMPORTANT Use the same source and destination password during this conversion.

2 If your certificate is in PKCS#12 (`.p12` or `.pfx`) format, or after the certificate is converted to PKCS#12 format, use `openssl` to convert the certificate to `.pem` files.

For example, if the name of the certificate is `sslservercerts.p12`, use the following commands to convert the certificate:

```
openssl pkcs12 –in sslservercerts.p12 –nokeys –out sslservercerts.pem
openssl pkcs12 –in sslservercerts.p12 –nodes –nocerts –out sslservercertskey.pem
```

3 Use the following UNIX command to convert each `.pem` file to a value that can be passed in a JSON string to the Access Point REST API:

```
awk 'NF {sub(/\r/, ""); printf "%s\\n",$0;}' cert–name.pem
```

In this example, *`cert–name`*`.pem` is the name of the certificate file.

The new format places all the certificate information on a single line with embedded newline characters.

4 If you have an intermediate certificate, convert that certificate to one-line format and then add it to the first certificate so that both certificates are on the same line.

You can now create and use a JSON request to configure the certificate.

What to do next

If you converted an TLS/SSL server certificate, see "Replace the Default TLS/SSL Server Certificate for Access Point," on page 34. For smart card certificates, see Chapter 5, "Setting Up Smart Card Authentication," on page 39.

Replace the Default TLS/SSL Server Certificate for Access Point

To store a trusted CA-signed TLS/SSL server certificate on the Access Point appliance, you must convert the certificate to the correct format and use the Access Point REST API to configure the certificate.

For production environments, VMware strongly recommends that you replace the default certificate as soon as possible. The default TLS/SSL server certificate that is generated when you deploy an Access Point appliance is not signed by a trusted Certificate Authority.

IMPORTANT Also use this procedure for periodically replacing a certificate that has been signed by a trusted CA before the certificate expires, which might be every two years.

Prerequisites

- Unless you already have a valid TLS/SSL server certificate and its private key, obtain a new signed certificate from a Certificate Authority. When you generate a certificate signing request (CSR) to obtain a certificate, make sure that a private key is generated also. Do not generate certificates for servers using a KeyLength value under 1024.

  To generate the CSR, you must know the fully qualified domain name (FQDN) that client devices will use to connect to the Access Point appliance and the organizational unit, organization, city, state, and country to complete the Subject name.

- Convert the certificate to PEM-format files and convert the `.pem` files to one-line format. See "Convert Certificate Files to One-Line PEM Format," on page 32.

- Familiarize yourself with the Access Point REST API. The specification for this API is available at the following URL on the virtual machine where Access Point is installed: `https://access-point-appliance.example.com:9443/rest/swagger.yaml`.

Procedure

1 Create a JSON request for submitting the certificate to the Access Point appliance.

```
{
  "privateKeyPem": "string",
  "certChainPem": "string"
}
```

In this example, the *string* values are the JSON one-line PEM values that you created as described in the prerequisites.

2 Use a REST client, such as `curl` or `postman`, to use the JSON request to invoke the Access Point REST API and store the certificate and key on the Access Point appliance.

The following example uses a `curl` command. In the example, *access-point-appliance.example.com* is the fully qualified domain name of the Access Point appliance, and *cert*.json is the JSON request you created in the previous step.

```
curl -k -d @- -u 'admin' -H "Content-Type: application/json" -X PUT https://access-point-appliance.example.com:9443/rest/v1/config/certs/ssl < ~/cert.json
```

What to do next

If the CA that signed the certificate is not well known, configure clients to trust the root and intermediate certificates.

Change the Security Protocols and Cipher Suites Used for TLS/SSL Communication

Although in almost all cases, the default settings do not need to be changed, you can configure the security protocols and cryptographic algorithms that are used to encrypt communications between clients and the Access Point appliance.

The default setting includes cipher suites that use either 128-bit or 256-bit AES encryption, except for anonymous DH algorithms, and sorts them by strength. By default, TLS v1.0 , TLS v1.1, and TLS v1.2 are enabled. (SSL v3.0 and SSL v2.0 are disabled.)

Prerequisites

- Familiarize yourself with the Access Point REST API. The specification for this API is available at the following URL on the virtual machine where Access Point is installed: `https://access-point-appliance.example.com:9443/rest/swagger.yaml`.
- Familiarize yourself with the specific properties for configuring the cipher suites and protocols: `cipherSuites`, `ssl30Enabled`, `tls10Enabled`, `tls11Enabled`, and `tls12Enabled`. See "REST API Properties for Access Point," on page 29.

Procedure

1 Create a JSON request for specifying the protocols and cipher suites to use.

The following example has the default settings.

```
{
"cipherSuites":
"TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,SSL_RSA_WITH_RC4_128_SHA",
  "ssl30Enabled": "false",
  "tls10Enabled": "true",
  "tls11Enabled": "true",
  "tls12Enabled": "true"
}
```

2 Use a REST client, such as `curl` or `postman`, to use the JSON request to invoke the Access Point REST API and configure the protocols and cipher suites.

The following example uses a `curl` command. In the example, *access-point-appliance.example.com* is the fully qualified domain name of the Access Point appliance, and *ciphers*.json is the JSON request you created in the previous step.

```
curl -k -d @- -u 'admin' -H "Content-Type: application/json" -X PUT https://access-point-appliance.example.com:9443/rest/v1/config/system < ~/ciphers.json
```

The cipher suites and protocols that you specified are used.

Configuring the Secure Gateways

By default the secure tunnel, PCoIP Secure Gateway, and Blast Secure Gateway are all enabled on the Access Point appliance. The external URLs need to be set to values that can be used by remote Horizon clients to connect to the Access Point appliance for the tunnel connection, the PCoIP connection, and the Blast connection, respectively.

Table 3-4. Examples of the Secure Gateway Settings

Type of Secure Gateway	Property Name	Example Setting
Secure tunnel	`tunnelExternalUrl`	`https://ap1.example.com:443`
PCoIP Secure Gateway	`pcoipExternalUrl`	`10.20.30.40:4172`
Blast Secure Gateway	`blastExternalUrl`	`https://ap1.example.com:8443`

These properties are described in more detail in "Edge Service Settings for View," on page 30.

The PCoIP external URL must use an IPv4 address. The other URLs can use an IP address or a host name that can be resolved by the client on the external network, which is usually the Internet. These external addresses are used only by the clients. The connection from the client for all three URLs must route to the specific Access Point appliance and must not be load-balanced. In a NAT environment, the addresses must be the external addresses and not the internal NAT'd addresses.

The following example shows a configuration JSON that includes these properties.:

```
{
  "identifier": "VIEW",
  "enabled": true,
  "proxyDestinationUrl": "https://192.0.2.1",
  "proxyDestinationUrlThumbprints": "sha1=b6 77 dc 9c 19 94 2e f1 78 f0 ad 4b ec 85 d1 7a f8 8b
dc 34",
  "pcoipEnabled": true,
  "pcoipExternalUrl": "10.20.30.40:4172",
  "blastEnabled": true,
  "blastExternalUrl": "https://ap1.example.com:8443",
  "tunnelEnabled": true,
  "tunnelExternalUrl": "https://ap1.example.com:443",
  "proxyPattern": "/"
}
```

These settings are included in the EdgeServiceSettings resource. The URL is

`https://`*`access-point-appliance.example.com`*`:9443/rest/v1/config/edgeservice/view`

In this URL, *access-point-appliance.example.com* is the fully qualified domain name of the Access Point appliance.

VMware recommends that you configure these settings at deployment time, by using the VMware OVF Tool. For an example, see "Using VMware OVF Tool to Deploy the Access Point Appliance," on page 20.

Collecting Logs from the Access Point Appliance

4

You can enter a URL in a browser to get a ZIP file that contains logs from your Access Point appliance.

Use the following URL to collect logs from your Access Point appliance.

`https://access-point-appliance.example.com:9443/rest/v1/monitor/support-archive`

In this example, *access-point-appliance.example.com* is the fully qualified domain name of the Access Point appliance.

These log files are collected from the `/opt/vmware/gateway/logs` directory on the appliance.

The following tables contain descriptions of the various files included in the ZIP file.

Table 4-1. Files That Contain System Information to Aid in Troubleshooting

File Name	Description
`df.log`	Contains information about disk space usage.
`netstat.log`	Contains information about network connections.
`ap_config.json`	Contains the current configuration settings for the Access Point appliance.
`ps.log`	Includes a process listing.
`ifconfig.log`	Contains information about network interfaces.
`free.log`	Contains information about memory usage.

Table 4-2. Log Files for Access Point

File Name	Description
`esmanager.log`	Contains log messages from the Edge Service Manager process, which listens on ports 443 and 80.
`authbroker.log`	Contains log messages from the AuthBroker process, which handles authentication adapters.
`admin.log`	Contains log messages from the process that provides the Access Point REST API on port 9443.
`admin-zookeeper.log`	Contains log messages related to the data layer that is used to store Access Point configuration information.
`tunnel.log`	Contains log messages from the tunnel process that is used as part of XML API processing.
`bsg.log`	Contains log messages from the Blast Secure Gateway.
`SecurityGateway_*.log`	Contains log messages from the PCoIP Secure Gateway.

The log files that end in "`-std-out.log`" contain the information written to `stdout` of various processes and are usually empty files.

Setting Up Smart Card Authentication 5

By default, Access Point uses pass-through authentication, so that users enter their Active Directory credentials, and these credentials are sent through to a back-end system for authentication. You can, however, configure the Access Point appliance to perform smart card authentication.

With smart card authentication, a user or administrator inserts a smart card into a smart card reader attached to the client computer and enters a PIN. Smart card authentication provides two-factor authentication by verifying both what the person has (the smart card) and what the person knows (the PIN). End users can use smart cards for logging in to a remote View desktop operating system and also for smart-card enabled applications, such as an email application that uses the certificate for signing emails to prove the identity of the sender.

NOTE Smart card authentication is a Tech Preview feature for the Access Point 2.0 release, meaning that the feature is available for you to try out, but it is not recommended for production use, and no support is provided.

With this feature, smart card certificate authentication is performed against Access Point, and Access Point communicates information about the end user's X.509 certificate and the smart card PIN to View Connection Server by using a SAML assertion.

This chapter includes the following topics:

Copy Access Point SAML Metadata to View Connection Server

You must generate SAML metadata on the Access Point appliance and exchange metadata with View Connection Server to establish the mutual trust required for smart card authentication .

The Security Assertion Markup Language (SAML) is an XML-based standard that is used to describe and exchange authentication and authorization information between different security domains. SAML passes information about users between identity providers and service providers in XML documents called SAML assertions.

In this procedure, you generate Access Point SAML metadata by using the Access Point REST API. You copy that metadata and then use the ADSI Edit utility on the View Connection Server host to edit the View LDAP and paste in the metadata. In this way, you manually create an Access Point SAML authenticator on the View Connection Server instance.

Prerequisites

- Configure the clock (UTC) on the Access Point appliance so that the appliance has the correct time. For example, verify that the ESXi host's time is synchronized with an NTP server, and verify that VMware Tools, which is running in the appliance virtual machine, synchronizes the time on the virtual machine with the time on the ESXi host.

  IMPORTANT If the clock on the Access Point appliance does not match the clock on the View Connection Server host, smart card authentication might not work.

- See the Microsoft TechNet Web site for information on how to use the ADSI Edit utility on your Windows operating system version.
- Obtain a SAML signing certificate that you can use to sign the Access Point metadata.

  NOTE VMware recommends that you create and use a specific SAML signing certificate when you have more than one Access Point appliance in your setup. In this case, all appliances must be configured with the same signing certificate so that View Connection Server can accept assertions from any of the Access Point appliances. With a specific SAML signing certificate, the SAML metadata from all of the appliances is the same.

- If you have not done so already, convert the SAML signing certificate to PEM-format files and convert the `.pem` files to one-line format. See "Convert Certificate Files to One-Line PEM Format," on page 32.

Procedure

1 Create a JSON request for generating the SAML metadata for the Access Point appliance.

   - If you do not have a SAML signing certificate for the Access Point appliance, the body of the JSON request is empty brackets:

     ```
     {}
     ```

   - If you do have a SAML signing certificate, use the following syntax:

     ```
     {
       "privateKeyPem": "string",
       "certChainPem": "string"
     }
     ```

     In this example, the *string* values are the JSON one-line PEM values that you created as described in the prerequisites.

2 Use a REST client, such as `curl` or `postman`, to use the JSON request to invoke the Access Point REST API and generate Access Point metadata.

   The following example uses a `curl` command. In the example, *access-point-appliance.example.com* is the fully qualified domain name of the Access Point appliance, and *ap-metadata*.json is the JSON request you created in the previous step.

   ```
   curl -k -d @- -u 'admin' -H "Content-Type: application/json" -X POST https://access-point-appliance.example.com:9443/rest/v1/config/idp-metadata < ~/ap-metadata.json
   ```

3 Use a REST client to get the generated metadata, and then copy the metadata.

   ```
   curl -k -u 'admin' https://access-point-appliance.example.com:9443/rest/v1/config/idp-metadata
   ```

   After you copy the Access Point SAML metadata, you can paste it into View LDAP to create a SAML authenticator on View Connection Server.

4 Start the ADSI Edit utility on your View Connection Server host and connect to View LDAP.

   a In the console tree, select **Connect to**.

   b In the **Select or type a Distinguished Name or Naming Context** text box, type the distinguished name **`DC=vdi, DC=vmware, DC=int`**.

   c In the Computer pane, select or type **`localhost:389`** or the fully qualified domain name (FQDN) of the View Connection Server host followed by port 389.

   For example: **`localhost:389`** or **`mycomputer.example.com:389`**

5 Expand the ADSI Edit tree, expand **OU=Properties**, right-click **OU=Authenticator** and select **New > Object**.

6 In the Create Object wizard, select **pae-SAMLAuthenticator** and click **Next**.

7 In the **Value** text box, enter a name, such as **`ap`** for Access Point, click **Next**, and click **Finish**.

   The object appears in the right pane. For this example, the name of the object is **CN=ap**.

8 Double-click the **CN=*name*** object and edit the following attributes.

Attribute	Description
pae-SAMLLabel	Supply a name of the SAML authenticator. This label will appear in View Connection Server, in the View Connection Server authentication settings.
pae-SAMLMetaDataXml	Paste in the SAML metadata that you generated on the Access Point appliance. Make sure metadata does not contain escape characters before double quotes. For example, the correct format is **`<?xml version="1.0"`** and not **`<?xml version=\"1.0\"`**.
pae-SAMLMetaDataUrl	(Optional) If you specify a URL in this attribute (for example, **`https://access-point.example.com`**), the URL will be displayed in the Manage Authenticators dialog box in View Administrator.

On View Connection Server, the new setting takes effect immediately. You do not need to restart the View Connection Server service or the client computer.

Change the Expiration Period for Service Provider Metadata

If you do not change the expiration period, View Connection Server will stop accepting SAML assertions from the SAML authenticator, such as Access Point or a third-party identity provider, after 24 hours, and the metadata exchange must be repeated.

Use this procedure to specify the number of days that can elapse before View Connection Server stops accepting SAML assertions from the identity provider. This number is used when the current expiration period ends. For example, if the current expiration period is 1 day and you specify 90 days, after 1 day elapses, View Connection Server generates metadata with an expiration period of 90 days.

Prerequisites

See the Microsoft TechNet Web site for information on how to use the ADSI Edit utility on your Windows operating system version.

Procedure

1 Start the ADSI Edit utility on your View Connection Server host.

2 In the console tree, select **Connect to**.

3 In the **Select or type a Distinguished Name or Naming Context** text box, type the distinguished name **`DC=vdi, DC=vmware, DC=int`**.

4 In the Computer pane, select or type **localhost:389** or the fully qualified domain name (FQDN) of the View Connection Server host followed by port 389.

   For example: **localhost:389** or **mycomputer.example.com:389**

5 Expand the ADSI Edit tree, expand **OU=Properties**, select **OU=Global**, and double-click **OU=Common** in the right pane.

6 In the Properties dialog box, edit the **pae-NameValuePair** attribute to add the following values

   ```
   cs-samlencryptionkeyvaliditydays=number-of-days
   cs-samlsigningkeyvaliditydays=number-of-days
   ```

   In this example, *number-of-days* is the number of days that can elapse before a remote View Connection Server stops accepting SAML assertions. After this period of time, the process of exchanging SAML metadata must be repeated.

Copy View Connection Server SAML Metadata to Access Point

After you enable the Access Point SAML authenticator in View Administrator, you can generate View Connection Server metadata and use this metadata to create a service provider on the Access Point appliance.

Prerequisites

- Verify that you can log in to View Administrator as an administrator.
- Verify that you have created an Access Point SAML authenticator by copying the Access Point SAML metadata into View LDAP. See "Copy Access Point SAML Metadata to View Connection Server," on page 39.
- Verify that the expiration period for the metadata is set for the correct number of days. The default is one day. See "Change the Expiration Period for Service Provider Metadata," on page 41.

Procedure

1 Log in to View Administrator and go to **View Configuration > Servers** and click the **Connection Servers** tab.

2 Select the View Connection Server instance and click **Edit**.

3 Click the **Authentication** tab, and in the **Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator)** drop-down list, select **Allowed** or **Required**, as appropriate.

4 From the **SAML Authenticator** list, select the name of the Access Point authenticator you created, and click **OK**.

5 In the System Health section on the View Administrator dashboard, select **Other components > SAML 2.0 Authenticators**, select the SAML authenticator that you added, and verify the details.

   If the configuration is successful, the authenticator's health can be either green or red. An authenticator's health can also display red if the certificate is untrusted, if Access Point is unavailable, or if the metadata URL is invalid. If the health indicator is red, you do not need to click **Verify** to validate and accept the certificate. Clicking **Verify** is only necessary for dynamic SAML authenticators. The Access Point SAML authenticator is a static SAML authenticator.

6 Open a new browser tab and enter the URL for getting the View Connection Server SAML metadata.

   https://*connection-server.example.com*/SAML/metadata/sp.xml

   In this example, *connection-server.example.com* is the fully qualified domain name of the View Connection Server host.

   This page displays the SAML metadata from View Connection Server.

7 Use a **Save As** command to save the Web page to an XML file.

For example, you could save the page to a file named `connection-server-metadata.xml`. The contents of this file begin with the following text:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ...
```

8 Use a REST client, such as `curl` or `postman`, to invoke the Access Point REST API and store the metadata on the Access Point appliance.

The following example uses a `curl` command. In the example, *access-point-appliance.example.com* is the fully qualified domain name of the Access Point appliance, *service-provider-name* is the name to use as the View Connection Server service provider, and *connection-server-metadata.xml* is the metadata file you created in the previous step.

```
curl -k -d @- -u 'admin' -H "Content-Type: text/xml" -X POST https://access-point-appliance.example.com:9443/rest/v1/config/sp-metadata/service-provider-name < connection-server-metadata.xml
```

Access Point and View Connection Server can now exchange authentication and authorization information.

What to do next

To verify that the POST command worked, you can use a GET command with the same URL.

To verify that the Access Point SAML authenticator was successfully configured after you selected it in View Administrator, open the ADSI Edit utility on the View Connection Server host, connect to View LDAP (**`DC=vdi, DC=vmware, DC=int`**), and in the ADSI Edit tree, under **OU=Properties**, select **OU=Server**, and double-click the **CN=*name*** item in the right pane. The **pae-SAMLConfigDN** attribute will be populated with the distinguished name.

Obtain the Certificate Authority Certificates

You must obtain all applicable CA (certificate authority) certificates for all trusted user certificates on the smart cards presented by your users and administrators. These certificates include root certificates and can include intermediate certificates if the user's smart card certificate was issued by an intermediate certificate authority.

If you do not have the root or intermediate certificate of the CA that signed the certificates on the smart cards presented by your users and administrators, you can export the certificates from a CA-signed user certificate or a smart card that contains one. See "Obtain the CA Certificate from Windows," on page 44.

Procedure

- Obtain the CA certificates from one of the following sources.
  - A Microsoft IIS server running Microsoft Certificate Services. See the Microsoft TechNet Web site for information on installing Microsoft IIS, issuing certificates, and distributing certificates in your organization.
  - The public root certificate of a trusted CA. This is the most common source of a root certificate in environments that already have a smart card infrastructure and a standardized approach to smart card distribution and authentication.

Obtain the CA Certificate from Windows

If you have a CA-signed user certificate or a smart card that contains one, and Windows trusts the root certificate, you can export the root certificate from Windows. If the issuer of the user certificate is an intermediate certificate authority, you can export that certificate.

Procedure

1 If the user certificate is on a smart card, insert the smart card into the reader to add the user certificate to your personal store.

If the user certificate does not appear in your personal store, use the reader software to export the user certificate to a file. This file will be used in Step 4.

2 In Internet Explorer, select **Tools > Internet Options**.

3 On the **Content** tab, click **Certificates**.

4 On the **Personal** tab, select the certificate you want to use and click **View**.

If the user certificate does not appear on the list, click **Import** to manually import it from a file. After the certificate is imported, you can select it from the list.

5 On the **Certification Path** tab, select the certificate at the top of the tree and click **View Certificate**.

If the user certificate is signed as part of a trust hierarchy, the signing certificate might be signed by another higher-level certificate. Select the parent certificate (the one that actually signed the user certificate) as your root certificate. In some cases, the issuer might be an intermediate CA.

6 On the **Details** tab, click **Copy to File**.

The Certificate Export Wizard appears.

7 Click **Next > Next** and type a name and location for the file that you want to export.

8 Click **Next** to save the file as a root certificate in the specified location.

Configure Smart Card Settings on the Access Point Appliance

On the Access Point appliance, you must enable smart card authentication, copy in the certificate, and change the authentication type to smart card authentication.

NOTE Smart card authentication is a Tech Preview feature for the Access Point 2.0 release.

Prerequisites

- Get the trusted CA issuer certificate that was used to sign the X.509 certificates for the smart cards. See "Obtain the Certificate Authority Certificates," on page 43. for the certificate that will be put on the smart card.
- Convert the certificate to a PEM-format file that contains the certificate chain. See "Convert Certificate Files to One-Line PEM Format," on page 32. If you have an intermediate certificate, that certificate must immediately follow the first certificate, and both certificates must be on the same one line.
- Verify that you have copied Access Point SAML metadata to View Connection Server and copied View Connection Server SAML metadata to Access Point appliance. See "Copy Access Point SAML Metadata to View Connection Server," on page 39 and "Copy View Connection Server SAML Metadata to Access Point," on page 42.
- Familiarize yourself with the smart card certificate properties and determine which settings to use. See "Smart Card Certificate Properties for Advanced Options," on page 46.

- If you use a load balancer between Access Point and View Connection Server instances, verify that TLS/SSL termination is not done on the load balancer. The load balancer must be configured to pass authentication through to View Connection Server.

Procedure

1 Use a REST client, such as `curl` or `postman`, to invoke the Access Point REST API and get the default certificate settings.

The following example uses a `curl` command. In the example, *access-point-appliance.example.com* is the fully qualified domain name of the Access Point appliance.

```
curl –k –u 'admin' https://access–point–appliance.example.com:
9443/rest/v1/config/authmethod/certificate–auth
```

2 Paste this information into a JSON request for enabling smart card authentication and pasting in the certificate.

The following two properties are the required properties to configure. You can also change the defaults for the other properties.

```
{
"enabled": "true",
"caCertificates": "–––––BEGIN CERTIFICATE–––––– ... ––––––END CERTIFICATE––––––"
}
```

In this example, the ellipses (...) indicates the middle content of the certificate text. The format of certificate text must be one-line format that can be passed in a JSON string to the Access Point REST API, as described in the prerequisites.

For `caCertificates`, you can specify multiple certificates using spaces as separators. When a user initiates a connection to the Access Point appliance, Access Point sends a list of trusted certificate authorities (CAs) to the client system. The client system checks the list of trusted CAs against the available user certificates, selects a suitable certificate, and then prompts the user to enter a smart card PIN. If there are multiple valid user certificates, the client system prompts the user to select a certificate.

3 Use a REST client, such as `curl` or `postman`, to use the JSON request to invoke the Access Point REST API and store the certificate on the Access Point appliance and enable smart card authentication.

The following example uses a `curl` command. In the example, *access-point-appliance.example.com* is the fully qualified domain name of the Access Point appliance, and *smartcard*.json is the JSON request you created in the previous step.

```
curl –k –d @– –u 'admin' –H "Content–Type: application/json" –X PUT https://access–point–
appliance.example.com:9443/rest/v1/config/authmethod/certificate–auth < ~/smartcard.json
```

4 Use a REST client to get the default edge service settings for View Connection Server.

```
curl –k –u 'admin' https://access–point–appliance.example.com:
9443/rest/v1/config/edgeservice/VIEW
```

5 Paste this information into a JSON request for enabling smart card authentication for the View server and add the `authMethods` and `samlSP` properties.

```
{
  "identifier": "VIEW",
  "enabled": true,
  "proxyDestinationUrl": "https://connection–server.example.com",
  "proxyDestinationUrlThumbprints": "sha1=40 e6 98 9e a9 d1 bc 6f 86 8c c0 ad b1 ea ff f7 4a
3b 12 8c",
  "pcoipEnabled": true,
  "blastEnabled": true,
  "tunnelEnabled": true,
```

```
  "proxyPattern": "/",
  "authMethods": "certificate-auth",
  "samlSP": "connection-server-sp"
}
```

In this example, *connection-server.example.com* is the fully qualified domain name of the View Connection Server host. You specified this name when you deployed the Access Point appliance. Also in this example, *connection-server-sp* is the service provider name that you specified when you copied the View Connection Server metadata to the Access Point appliance. The text for `proxyDestinationUrlThumbprints` is an example only. Replace this text with the thumbprint of your destination server.

6 Use a REST client to send the JSON request to the Access Point API and configure the edge service to use smart card authentication.

In the following example, *smartauth*.json is the JSON request you created in the previous step.

```
curl -k -d @- -u 'admin' -H "Content-Type: application/json" -X PUT https://access-point-appliance.example.com:9443/rest/v1/config/edgeservice/VIEW < ~/smartauth.json
```

End users can now use smart cards when logging in to Access Point.

Smart Card Certificate Properties for Advanced Options

Smart card authentication properties provide functionality for certificate revocation, consent forms, and configuring the subject alternative name.

You can prevent users who have revoked user certificates from authenticating with smart cards by configuring certificate revocation checking. Certificates are often revoked when a user leaves an organization, loses a smart card, or moves from one department to another.

Access Point supports certificate revocation checking with certificate revocation lists (CRLs) and with the Online Certificate Status Protocol (OCSP). A CRL is a list of revoked certificates published by the CA that issued the certificates. OCSP is a certificate validation protocol that is used to get the revocation status of an X.509 certificate.

When you configure both types of certificate revocation checking, Access Point attempts to use OCSP first and can be configured to fall back to CRL if OCSP fails. Access Point does not fall back to OCSP if CRL fails. The CA must be accessible from the Access Point host.

When you use the REST API to get the configuration data for smart card authentication, you see a list of the items you can configure. For example, you can use a GET request with the following URL:

```
https://access-point-appliance.example.com:9443/rest/v1/config/authmethod/certificate-auth
```

If you have not changed any configuration settings, the following default settings are returned.

```
  "enableOCSP": null,
  "ocspSigningCert": null,
  "caCertificates": null,
  "displayName": "CertificateAuthAdapter",
  "versionNum": null,
  "enableAlternateUPN": "",
  "className": "com.vmware.horizon.adapters.certificateAdapter.CertificateAuthAdapter",
  "sendOCSPNonce": null,
  "enabled": "false",
  "enableCertCRL": "true",
  "enableOCSPCRLFailover": "true",
  "enableConsentForm": null,
  "ocspURL": null,
  "jarFile": "/opt/vmware/gateway/data/authbroker/certificate-auth-adapter-0.1.jar",
```

```
"enableCertRevocation": "",
"name": "certificate-auth",
"certificatePolicies": null,
"consentForm": null,
"authMethod": "urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient",
"crlLocation": null,
"enableEmail": "",
"crlCacheSize": "100"
```

Table 5-1. Smart Card Certificate Properties That You Can Configure

Property Name	Description	Valid Values
enableOCSP	Specifies whether to use Online Certificate Status Protocol (OCSP) for certificate revocation checking. When this setting is enabled, Access Point sends a request to an OCSP responder to determine the revocation status of a specific user certificate. The default is true.	true or false
ocspSigningCert	Specifies the path to the OCSP responder's certificate, if known.	Path to the file on the OCSP responder host (for example, `/path/to/file.cer`).
caCertificates	(Required) Specifies one or more trusted CA certificates in PEM format.	Each certificate's text has the format "`-----BEGIN CERTIFICATE------ ... -----END CERTIFICATE------`" where the ellipsis points (...) indicate the middle content of the certificate text. Separate multiple certificates with spaces.
enableAlternateUPN	Specifies whether to use alternative fields in the Subject Alternative Name. Smart card logins use the user principal name (UPN) from Active Directory to validate user accounts. If the domain a smart card user resides in is different from the domain that your root certificate was issued from, you must set the user's UPN to the Subject Alternative Name (SAN) contained in the root certificate of the trusted CA.	true or false
sendOCSPNonce	Specifies whether to include a nonce in the OCSP request and require that the nonce be included in the response. A nonce is an arbitrary number used only once in a cryptographic communication.	true or false
enabled	(Required) Specifies whether to use smart card certificate authentication. You must change this setting to true. The default is false.	true or false
enableCertCRL	Specifies whether to use the CRL Distribution Points extension of the certificate.	true or false
enableOCSPCRLFailover	Specifies whether to use a certificate revocation list if OCSP fails. The default is true.	true or false
enableConsentForm	Specifies whether to present users with a consent form window before they log in using certificate authentication.	true or false
ocspURL	Specifies the URL of the OCSP responder to use for the revocation check (for example, http://ocspurl.com).	A URL that begins with http or https.

Table 5-1. Smart Card Certificate Properties That You Can Configure (Continued)

Property Name	Description	Valid Values
enableCertRevocation	Specifies whether to use certificate revocation checking.	true or false
certificatePolicies	Specifies the object Identifier (OID) list that is accepted in the Certificate Policies extension.	An OID
consentForm	Specifies the content of the consent form to be displayed to users.	Text.
crlLocation	Specifies the location of the certificate revocation list to use for the revocation check.	URL or file path (for example, `http://crlurl.crl` or `file:///crlFile.crl`). **NOTE** Do not use `ldap:` URLs.
enableEmail	Specifies whether to use the RFC822 field in Subject Alternative Name if no UPN (user principal name) is found in the certificate.	true or false

Index