Deploying and Configuring Access Point

Access Point 2.7.2, 2.7, 2.6, 2.5
VMware Horizon

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-002165-00

vmware®

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

Deploying and Configuring Access Point

Deploying and Configuring Access Point provides information about designing VMware Horizon®, VMware Identity Manager®, and VMware AirWatch® deployment that uses Access Point for secure external access to your organization's applications, including Windows applications, software as a service (SaaS) applications, 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. The information is written for experienced Linux and Windows 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.

Introduction to Access Point 1

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

Access Point appliances typically reside within a network demilitarized zone (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 virtual desktops, application hosts, and servers 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 virtual appliances also ensure that the traffic for an authenticated user can be directed only to desktop and application resources to which the user is actually entitled. This level of protection involves specific inspection of desktop protocols and coordination of potentially rapid changing policies and network addresses, and so on, to be able to accurately control access.

With Access Point 2.6 and 2.7, the Access Point appliance can also serve as a reverse proxy for VMware Identity Manager.

With Access Point 2.7, the Access Point appliance integrates and provides secure gateway to AirWatch applications.

Compatibility Matrix: The product interoperability matrix table provides the list of Access Point releases that support appropriate solutions. Verify that you install the correct version of Access Point for your product to have seamless integration.

Table 1-1. Product Interoperability Matrix

Access Point Version	Horizon Air	View	Horizon	Horizon Air Hybrid-Mode	VMware Identity Manager	AirWatch
2.0, 2.0.2/2.0.3	15.3	6.2, 6.2.x				
2.5 , 2.5.x	16.4	6.2.3	7.0.2, 7.0.1, 7.0	1.0		
2.6					On-Premise 2.6	
2.7					2.7	8.4
2.7.2	16.6	6.2.2, 6.2.3	7.0.2, 7.0.1, 7.0	1.1	2.7	8.4.2

Access Point is a hardened security appliance designed specifically for DMZ. The following hardening settings are implemented.

- Up to date Linux Kernel and software patches

- Multiple NIC support for internet and intranet traffic
- Disabled SSH
- Disabled FTP, Telnet, Rlogin or Rsh services
- Disabled unwanted services

If you choose to use a Virtual Private Network (VPN), View fully supports remote access to desktops and applications through a VPN. A VPN meets the requirement of ensuring the traffic into the internal network is forwarded only on behalf of a strongly authenticated user. In this respect, Access Point and a commercial-grade VPN are similar. However, there are some considerations to consider for Access Point.

- Access Control Manager. Access Point applies access rules automatically. Access Point recognizes not only the user's entitlements, but also the addressing required to connect internally, which can change quickly.

  A VPN does the same, because most VPNs allow an administrator to configure network connection rules for every user or group of users individually. At first, this works well with a VPN, but requires significant administrative effort maintain the required rules. An administrator manages either too many authorized resources that are blocked or unauthorized resources end up being allowed. The easy response for a VPN administrator is to allow unchecked access to any resource on the internal network, authenticate to the VPN, and you have complete access to the corporate network. This is easy for the administrator, but a concern for corporate security. Thus it is a low-cost operational approach.

- User Interface. A VPN requires that you must set up the VPN software first and authenticate separately before launching the Horizon Client. This may be secure, but is an extra step. Access Point does not alter the straightforward Horizon Client user interface at all, and eliminates the extra (VPN) step. When you launch the Horizon Client, and as long as the authentication is successful, you are into their View environment, and have precisely controlled access to the desktops and applications.

- Performance. VPNs are implemented as SSL VPNs. These certainly meet security requirements and with Transport Layer Security (TLS) enabled, are usually considered secure, but the underlying protocol with SSL/TLS is just TCP-based. With modern video-remoting protocols exploiting connectionless UDP-based transports, the performance benefits can be significantly eroded when forced over a TCP-based transport. This does not apply to all VPN technologies, as those that can also operate with DTLS or IPsec instead of SSL/TLS can work well with View desktop protocols. Access Point is specifically designed to maximize security and maximize performance. With Access Point, PCoIP, HTML access, and WebSocket protocols are secured without requiring additional encapsulation.

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," on page 9
- "Deploying Access Point Appliance," on page 11
- "Firewall Rules for DMZ-Based Access Point Appliances," on page 22
- "Access Point Topologies," on page 23

Access Point System Requirements

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

VMware Software Requirements

You must use specific versions of VMware products with specific versions of Access Point. Refer to the product release notes for the latest information about compatibility, and refer to the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php. Information in the release notes and interoperability matrix supersede information in this guide.

VMware AirWatch 8.4

VMware AirWatch 8.4.x is qualified to support Access Point 2.7.2.

VMware Identity Manager 2.7

VMware Identity Manager 2.7.x is qualified to support Access Point 2.7.2.

Horizon 7 version 7.0.2

Horizon 7 version 7.0.2 is qualified to support Access Point 2.7.2.

During an upgrade, make sure the View Connection Server instances are upgraded to 6.2 or later before using Access Point appliances. Access Point is not designed to interoperate with earlier versions of Connection Server.

VMware Horizon Air Hybrid-Mode 1.0/1.1

Horizon Air Hybrid-Mode 1.1 has been qualified to support Access Point 2.7.2.

VMware vSphere 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 the Horizon products and versions you are using.

Horizon Client

Although VMware recommends that you upgrade to the latest version of the clients to get new features and performance improvements, Access Point is designed to work with all client versions that are supported with the supported versions of Horizon servers.

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.

Log Retention Requirements

The log files are configured by default to use a certain amount of space which is smaller than the total disk size in the aggregate. The logs for Access Point roll by default. You must use syslog to preserve these log entries.

System Requirements to Deploy Access Point Using PowerShell

To deploy Access Point using PowerShell script, you must use specific versions of VMware products.

1. vSphere ESX host with a vCenter Server is needed.

   You must select the vSphere datastore and the network to use. A vSphere Network Protocol Profile must be associated with every referenced network name. his Network Protocol Profile specifies network settings such as IPv4 subnet mask, gateway etc. The deployment of Access Point uses these values so make sure the values are correct.

2. The PowerShell script runs on Windows 8.1 or later machines or Windows Server 2008 R2 or later.

   The machine can also be a vCenter Server running on Windows or a separate Windows machine.

3. The Windows machine running the script must have VMware OVF Tool command installed.

   You must install OVF Tool 4.0.1 or later from https://www.vmware.com/support/developer/ovf/.

Deploying Access Point Appliance

You can deploy the Access Point appliance using PowerShell. You can also deploy using Deploy OVF Template wizard or the OVF command line tool. Logging in directly to an ESXi host to use the deployment wizard is not supported.

For production environments, VMware recommends that you use the sample PowerShell scriptAccess Point. Using the PowerShell script to deployAccess Point overcomes the main difficulties of using OVF Tool directly on the command line. The script calls the OVF Tool command but validates the settings and automatically constructs the correct command line syntax. This method allows advanced settings such as configuration of the TLS/SSL server certificate to be applied at deployment time.

Using PowerShell to Deploy Access Point Appliance

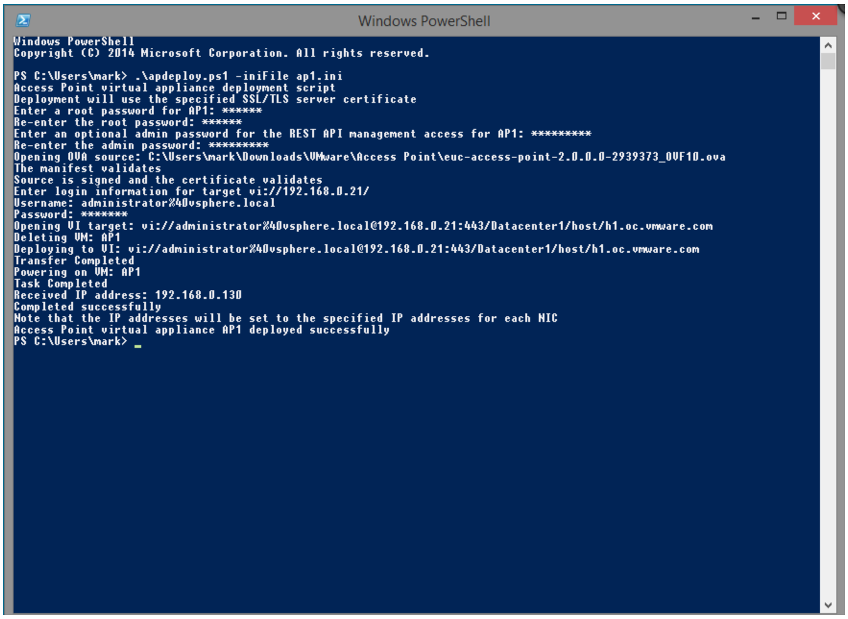
PowerShell scripts prepare you environment with all the configuration settings. When you run the PowerShell script to deploy Access Point, the solution is ready for production on first system boot.

Prerequisites

- Verify that the system requirements are appropriate and available for use.

Note This is a sample script to deploy Access Point in your environment.

Figure 2-1. Sample PowerShell Script



```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\mark> .\apdeploy.ps1 -iniFile ap1.ini
Access Point virtual appliance deployment script
Deployment will use the specified SSL/TLS server certificate
Enter a root password for AP1: ******
Re-enter the root password: ******
Enter an optional admin password for the REST API management access for AP1: *********
Re-enter the admin password: *********
Opening OVA source: C:\Users\mark\Downloads\VMware\Access Point\euc-access-point-2.0.0.0-2939373_OVF10.ova
The manifest validates
Source is signed and the certificate validates
Enter login information for target vi://192.168.0.21/
Username: administrator%40vsphere.local
Password: *******
Opening VI target: vi://administrator%40vsphere.local@192.168.0.21:443/Datacenter1/host/h1.oc.vmware.com
Deleting VM: AP1
Deploying to VI: vi://administrator%40vsphere.local@192.168.0.21:443/Datacenter1/host/h1.oc.vmware.com
Transfer Completed
Powering on VM: AP1
Task Completed
Received IP address: 192.168.0.130
Completed successfully
Note that the IP addresses will be set to the specified IP addresses for each NIC
Access Point virtual appliance AP1 deployed successfully
PS C:\Users\mark> _
```

Procedure

1 Download Access Point virtual appliance from VMware product download page to the Windows machine.

This appliance is an OVA file. For example: euc-access-point-2.7.2_OVF10.ova.

2 Download the ap-deploy-272.zip files into a folder on the Windows machine.

The zip files are available at https://communities.vmware.com/docs/DOC-30835.

3 Open a PowerShell script and modify the directory to the location of your script.

4 Create a .INI configuration file for the Access Point virtual appliance.

For example: Deploy a new Access Point appliance AP1. The configuration file is named ap1.ini. This file contains all the configuration settings for AP1. You should use the sample .INI files in the apdeploy .ZIP file to create the .INI file and modify the settings appropriately.

Sample .INI File

```
name=AP1
source=C:\APs\euc-access-point-2.7.0.0-3588605_OVF10.ova
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host/esx1.myco.int
ds=Local Disk 1
netInternet=VM Network
netManagementNetwork=VM Network
netBackendNetwork=VM Network

[Horizon/WebReverseProxy/AirwatchTunnel]
proxyDestinationUrl=https://192.168.0.209

# For IPv4, proxydestinationURL=https://192.168.0.209
# For IPv6, proxyDEstinationUrl=[fc00:10:112:54::220]
```

Note You can have unique .INI files for multiple Access Point deployments in your environment. You must change the IP Addresses and the name parameters in the .INI file appropriately to deploy multiple appliances.

5 Ensure that the script execution is unrestricted for the current user.

```
set-executionpolicy -scope currentuser unrestricted
```

You must run this command once and only if it is currently restricted.

If there is a warning for the script, run the command to unblock the warning:

```
unblock-file -path .\apdeploy.ps1
```

6 Run the command to start the deployment. If you do not specify the .INI file, the script defaults to ap.ini.

```
.\apdeploy.ps1 -iniFile ap1.ini
```

7 Enter the credentials when prompted and complete the script.

Note If you are prompted to add the fingerprint for the target machine, enter **yes**.

Access Point appliance is deployed and available for production.

For more information on PowerShell scripts, see https://communities.vmware.com/docs/DOC-30835.

Using the OVF Template Wizard to Deploy the Access Point Appliance

You can deploy the Access Point appliance 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.

It is also possible to use the command-line VMware OVF Tool to deploy the appliance, see "Using OVF Command Line Tool to Deploy the Access Point Appliance," on page 16. With this tool, you can set advanced properties that are not available in the deployment wizard.

Important For production environments, VMware recommends that you use the sample "Using PowerShell to Deploy Access Point Appliance," on page 11. Using the PowerShell script to deploy Access Point overcomes the main difficulties of using OVF Tool directly on the command line. The script calls the OVF Tool command but validates the settings and automatically constructs the correct command line syntax. This method allows advanced settings such as configuration of the TLS/SSL server certificate to be applied at deployment time.

Prerequisites

- Familiarize yourself with the deployment options available in the wizard. See "Access Point Deployment Properties," on page 20. 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 server instance or load balancer that this Access Point appliance will point to.
- Determine the number of network interfaces and static IP addresses to configure for the Access Point appliance. See "Networking Requirements," on page 10.

  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 2.5GB. 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 9.
- 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-`*`Y.Y`*`.0.0-`*`xxxxxxx`*`_OVF10.ova`), where *Y.Y* is the version number and *xxxxxxx* is the build number.
- 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.

For an IPv4 network, use the native vSphere Client or the vSphere Web Client. For an IPv6 network, use the vSphere Web Client.

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	For an IPv4 network, you can use one, two, or three network interfaces (NICs). For an IPv6 network, use three NICs. Access Point requires a separate static IP address for each NIC. 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 IPv4 or IPv6 from the **IP protocol** drop down list. b Select the first row in the table **Internet** and then click the down arrow to select the destination network. If you select IPv6 as the IP protocol, you must select the network that has IPv6 capabilities. 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. c 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. d 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: ■ **NIC Modes STATICV4/STATICV6**. If you enter STATICV4, you must enter the IPv4 address for the NIC. If you enter STATICV6, you must enter the IPv6 address for the NIC. ■ **IPv4 address**. Enter the IPv4 address for the NIC if you entered STATICV4 for the NIC mode. ■ **IPv6 address**. Enter the IPv6 address for the NIC if you entered STATICV6 for the NIC mode. ■ **Host Network Prefix**. Network prefix length. Provide this value if you entered STATICV6 for the NIC mode. ■ **DNS server addresses**. Enter space-separated IPv4 or IPv6 addresses of the domain name servers for the VM. ■ **Management network IP address** if you specified 2 NICs, and **Backend network IP address** if you specified 3 NICs ■ **Password options**. Enter the password for the root user of this VM and the password for the administrator user who enables REST API access. ■ **Server URL** . Enter the Server URL for IPv4. ■ **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. For a description of all deployment properties, see "Access Point Deployment Properties," on page 20.

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, you will see the Web page provided by the server that Access Point is pointing to. For example, 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.

The Access Point appliance is deployed and starts automatically.

What to do next

IMPORTANT Configure the clock (UTC) on the Access Point appliance so that the appliance has the correct time. For example, open a console window on the Access Point virtual machine and use arrow buttons to select the correct time zone. Also 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 OVF Command Line 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.

IMPORTANT For production environments, VMware recommends that you use the sample "Using PowerShell to Deploy Access Point Appliance," on page 11. Using the PowerShell script to deploy Access Point overcomes the main difficulties of using OVF Tool directly on the command line. The script calls the OVF Tool command but validates the settings and automatically constructs the correct command line syntax. This method allows advanced settings such as configuration of the TLS/SSL server certificate to be applied at deployment time. The interactive deployment wizard does not include these advanced settings.

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 20.

Prerequisites for Access Point Deployment

- Familiarize yourself with the deployment options available. See "Access Point Deployment Properties," on page 20. 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 Horizon server 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 10.

  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 9.

- 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-Y.Y.0.0-xxxxxxx_OVF10.ova`), where *Y.Y* is the version number and *xxxxxxx* is the build number.

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://[fc00:10:112:54::220]^
--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-Y.Y.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://[fc00:10:112:54::220]\
--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-Y.Y.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 View Connection Server or a Horizon Air Node. In addition to specifying the Horizon server URL and the Horizon 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. This example shows IPv6 addresses. To use IPv4 addresses, replace the IPv6 addresses with IPv4 addresses.

```
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://[fc00:10:112:54::220]", ^
\"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\": \"[fc00:10:112:54::242]", ^
\"blastEnabled\": true, ^
\"blastExternalUrl\": \"https://[fc00:10:112:54::242]", ^
\"tunnelEnabled\": true, ^
\"tunnelExternalUrl\": \"https://[fc00:10:112:54::242]", ^
\"proxyPattern\":\"/\" } ] }^
}" ^
euc-access-point-Y.Y.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 View Connection Server or a Horizon Air Node. In addition to specifying the Horizon server URL and the Horizon server thumbprint, the `settingsJSON` property sets the external URLs for the secure gateways. This example shows IPv6 addresses. To use IPv4 addresses, replace the IPv6 addresses with IPv4 addresses.

```
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://[fc00:10:112:54::220]", \
"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": "[fc00:10:112:54::242]", \
"blastEnabled": true, \
"blastExternalUrl": "https://[fc00:10:112:54::242]", \
"tunnelEnabled": true, \
"tunnelExternalUrl": "https://[fc00:10:112:54::242]", \
"proxyPattern":"/"  } ] } \
}' \
euc-access-point-Y.Y.0.0-xxxxxxx_OVF10.ova  \
vi://root:password@vc.example.com/ExampleDC/host/ap
```

For a list of the REST API properties for configuring Access Point, see "Configuration Settings for System Settings and Server Certificates," on page 59.

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 "Using the OVF Template Wizard to Deploy the Access Point Appliance," on page 13. To specify the properties by using the OVF Tool command-line interface, see "Using OVF Command Line Tool to Deploy the Access Point Appliance," on page 16.

IMPORTANT For production environments, VMware recommends that you use the sample "Using PowerShell to Deploy Access Point Appliance," on page 11. Using the PowerShell script to deploy Access Point overcomes the main difficulties of using OVF Tool directly on the command line. The script calls the OVF Tool command but validates the settings and automatically constructs the correct command line syntax. This method allows advanced settings such as configuration of the TLS/SSL server certificate to be applied at deployment time. The interactive deployment wizard does not include these advanced settings.

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 the public IPv4 or IPv6 address used for accessing this virtual machine on the Internet. **NOTE** The computer name is set through a DNS query of this Internet IPv4 or IPv6 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.

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

Deployment Property	OVF Tool Option	Description
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.
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.

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

Deployment Property	OVF Tool Option	Description
Destination server URL	`--prop:proxyDestinationURL=`*URL*	(Required) Specifies the destination URL of the load balancer or server. The Access Point appliance directs traffic to the server at this destination. The destination URL must contain the protocol, host name or IP address, and port number (example: https://load-balancer.example.com:443) Default: none.
Destination server thumbrpints	`--prop:proxyDestinationURLThumbprints=`*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 Horizon server URL, 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 18.

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.

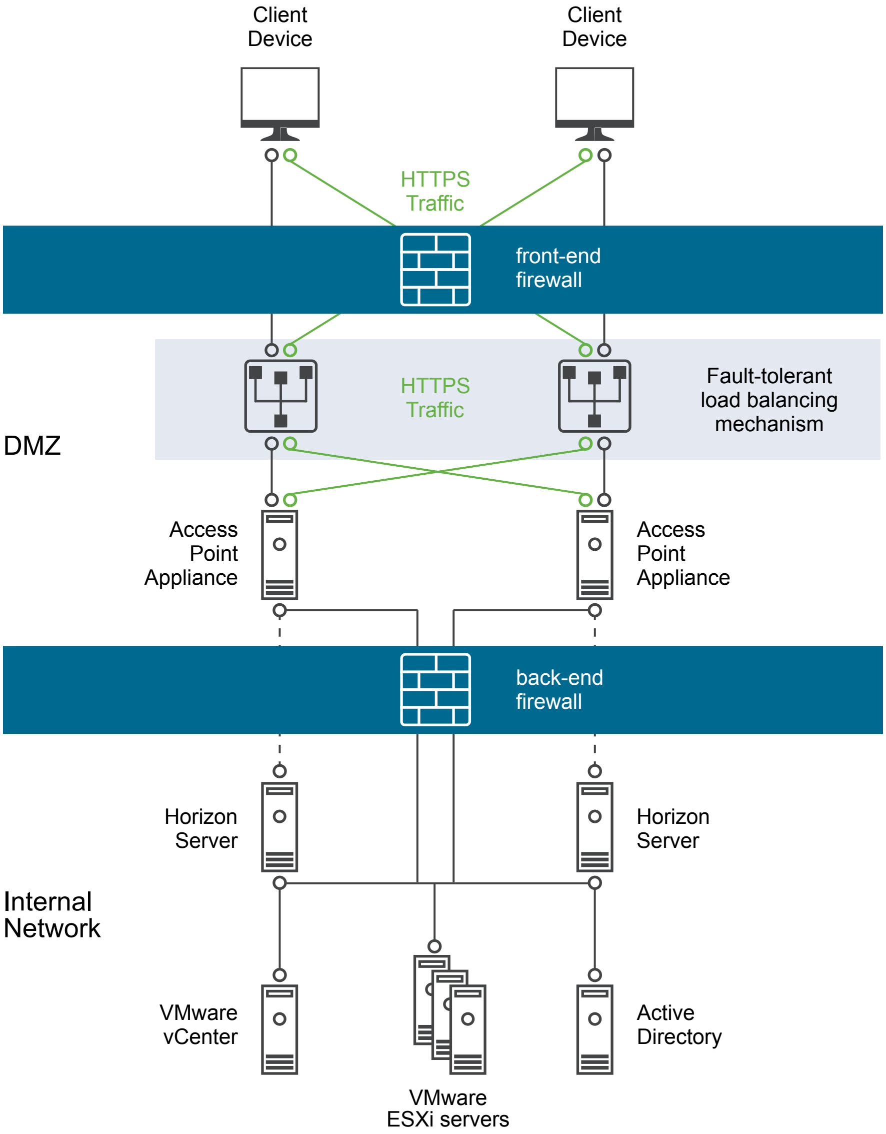
- An external network-facing, front-end firewall is required to protect both the DMZ and the internal network. You configure this firewall to allow external network traffic to reach the DMZ.
- A back-end firewall, between the DMZ and the internal network, is required to provide a second tier of security.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

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

To allow external client devices to connect to an Access Point appliance within the DMZ, the front-end firewall must allow traffic on certain ports. By default the external client devices and external Web clients (HTML Access) connect to an Access Point appliance within the DMZ on TCP port 443. If you use the Blast protocol, port 443 must be open on the firewall. If you use the PCOIP protocol, port 4172 must be open on the firewall.

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

Figure 2-2. Dual Firewall Topology



Access Point Topologies

You can implement any of several different topologies.

An Access Point appliance in the DMZ can be configured to point to a server or a load balancer that fronts a group of servers. 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 servers, the selection of the 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 server instance. The 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.

You can alternatively have one or more Access Point appliances point to an individual server instance. In both approaches, use a load balancer in front of two or more Access Point appliances in the DMZ.

Use Cases for Access Point Deployment 3

You can use Access Point use cases or deployment scenarios to identify, clarify, and organize the deployment in your environment. Use the configuration service settings required for deployment of Access Point appliance.

You can deploy Access Point with Horizon View, Horizon Air Hybrid-Mode, VMware Identity Manager, and VMware AirWatch.

This chapter includes the following topics:

Access Point Deployment with Horizon View and Horizon Air Hybrid-Mode

You can deploy Access Point with Horizon View and Horizon Air Hybrid-Mode. For the View component of VMware Horizon, Access Point appliances fulfill the same role that was previously played by View security servers.

Deployment Scenario

Access Point provides secure remote access to on-premises virtual desktops and applications in a customer data center. This operates with an on-premises deployment of Horizon View or Horizon Air Hybrid-Mode for unified management.

Access Point provides the enterprise with strong assurance of the identity of the user, and precisely controls access to their entitled desktops and applications.

Access Point virtual appliances are typically deployed in a network demilitarized zone (DMZ), and they ensure that all traffic entering the data center to desktop and application resources is traffic on behalf of a strongly authenticated user. Access Point virtual appliances also ensure that the traffic for an authenticated user can be directed only to desktop and application resources to which the user is actually entitled. This level of protection involves specific inspection of desktop protocols and coordination of potentially rapid changing policies and network addresses, and so on, to be able to accurately control access.

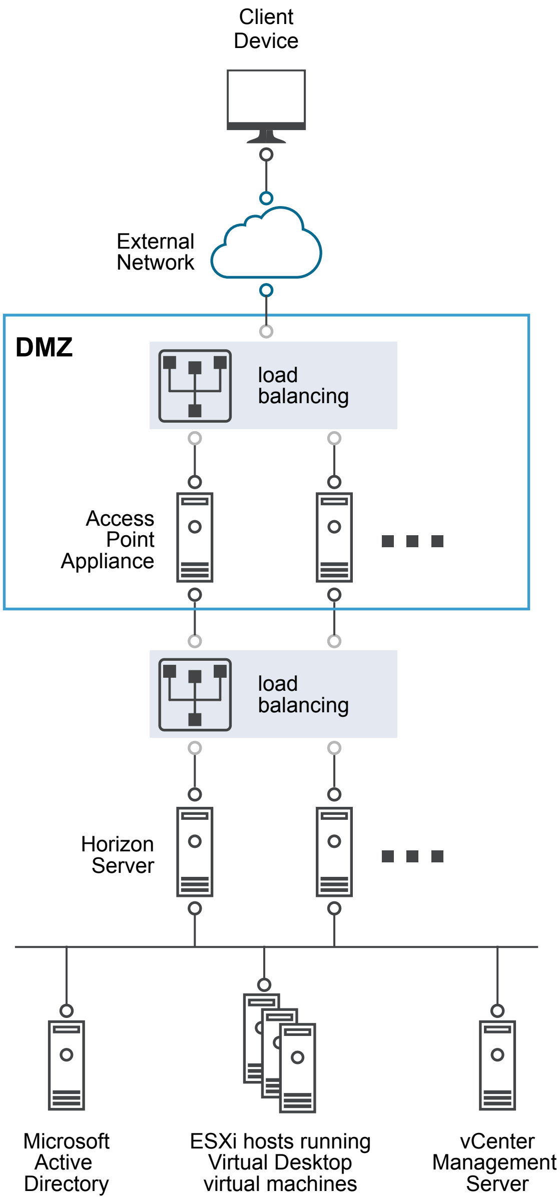
You must verify the requirements for seamless Access Point deployment with Horizon.

- Access Point appliance points to a load balancer in front of the Horizon servers, the selection of the server instance is dynamic.
- Access Point replaces the Horizon security server.
- Port 443 must be available for Blast TCP/UDP.

- The Blast Secure Gateway and PCoIP Secure Gateway must be enabled when Access Point is deployed with Horizon. This ensures that the display protocols can serve as proxies automatically through Access Point.The BlastExternalURL and pcoipExternalURL settings specify connection addresses used by the Horizon clients to route these display protocol connections through the appropriate gateways on Access Point. This provides improved security as these gateways ensure that the display protocol traffic is controlled on behalf of an authenticated user. Unauthorized display protocol traffic is disregarded by Access Point.

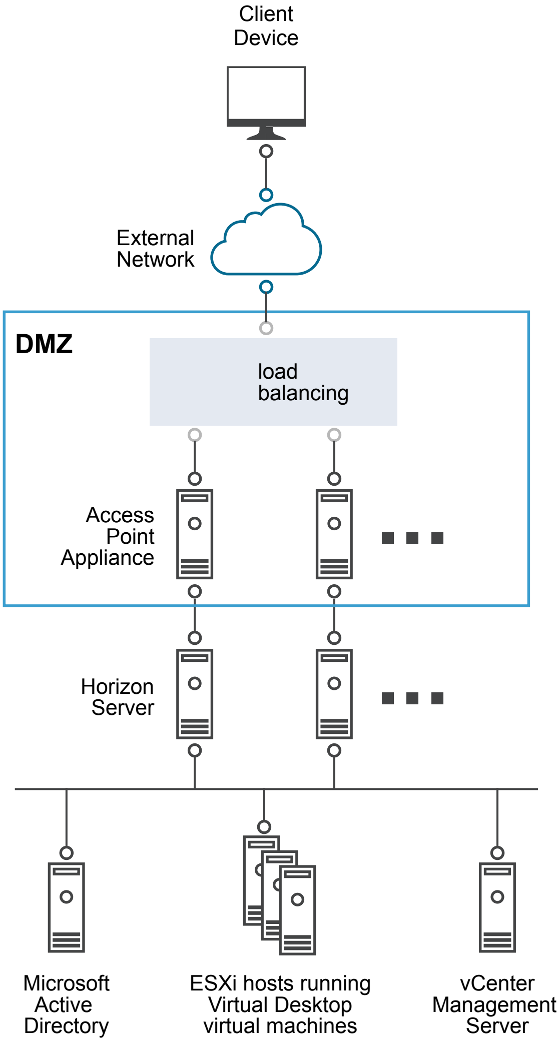
The main difference from View security server is that Access Point is implemented as a hardened, locked-down, preconfigured Linux-based virtual machine, as opposed to software running on a general-purpose Windows operating system. Access Point also scales differently; the restriction to pair it with a single View Connection Server has been removed. You can connect Access Point to an individual View Connection Server, or you can connect it through a load balancer in front of multiple View Connection Servers, giving improved high availability. It acts as a layer between Horizon Clients and backend View Connection Servers, and as deployment is so fast, it can rapidly scale up or down to meet the demands of fast-changing enterprises.

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


Client Device
External Network
DMZ
load balancing
Access Point Appliance
load balancing
Horizon Server
Microsoft Active Directory
ESXi hosts running Virtual Desktop virtual machines
vCenter Management Server

Alternatively you can have one or more Access Point appliance point to an individual server instance. In both approaches, use a load balancer in front of two or more Access Point appliances in the DMZ.

Figure 3-2. Access Point Appliance Pointing to a Horizon Server Instance



Authentication

User authentication is very similar to View security server. Supported user authentication methods in Access Point include:

- Active Directory domain password
- Kiosk mode
- RSA SecurID two-factor
- RADIUS via a number of third party, two-factor security-vendor solutions
- Smart card, CAC, or PIV X.509 user certificates
- SAML

These authentication methods are supported in combination with View Connection Server. Access Point does not require to communicate directly with Active Directory. This communication serves as a proxy via the View Connection Server, which can directly access Active Directory. After the user session has been authenticated according to the authentication policy, Access Point is then able to forward requests for entitlement information, and desktop and application launch requests, to View Connection Server. Access Point is also manages its desktop and application protocol handlers to allow them to forward only authorized protocol traffic.

Access Point handles smart card authentication itself. This includes options for Access Point to communicate with Online Certificate Status Protocol (OCSP) servers to check for X.509 certificate revocation, and so on.

Edge Service Settings for View

These settings are included in the EdgeServiceSettings resource. Use this edge service to configure Access Point to point to a server that uses the View XML protocol, such as View Connection Server, Horizon Air, or Horizon Air Hybrid-mode. The REST API 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 3-1. Edge Service Settings Resource for View

REST API Property	Description and Example	Default Value
`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` is 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.)
`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*:443 (*appliance* is the fully qualified domain name of the Access Point appliance.)

Table 3-1. Edge Service Settings Resource for View (Continued)

REST API Property	Description and Example	Default Value
`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.	**`(/|/view-client(.*)|/portal(.*))`**
`samlSP`	Set this property for setting up smart card authentication. See "Configure Smart Card Authentication on the Access Point Appliance," on page 45.	None
`matchWindowsUserName`	Set this property to enable securID-auth to true and then match SecureID and Windows user name.	FALSE
`gatewayLocation`	Identifies the location from where the connection request originates. The security server and Access Point sets the gateway-location. The location can be external or internal.	External **NOTE** The admin can override this location by providing the correct configuration.
`windowsSSOEnabled`	Set this property to enable radius-auth to true. The Windows login now uses the credentials that were used in the first successful RADIUS access request.	FALSE

Access Point Deployment as Reverse Proxy for VMware Identity Manager

You can configure Web Reverse Proxy service to use Access Point 2.6 and 2.7 with VMware Identity Manager

Deployment Scenario

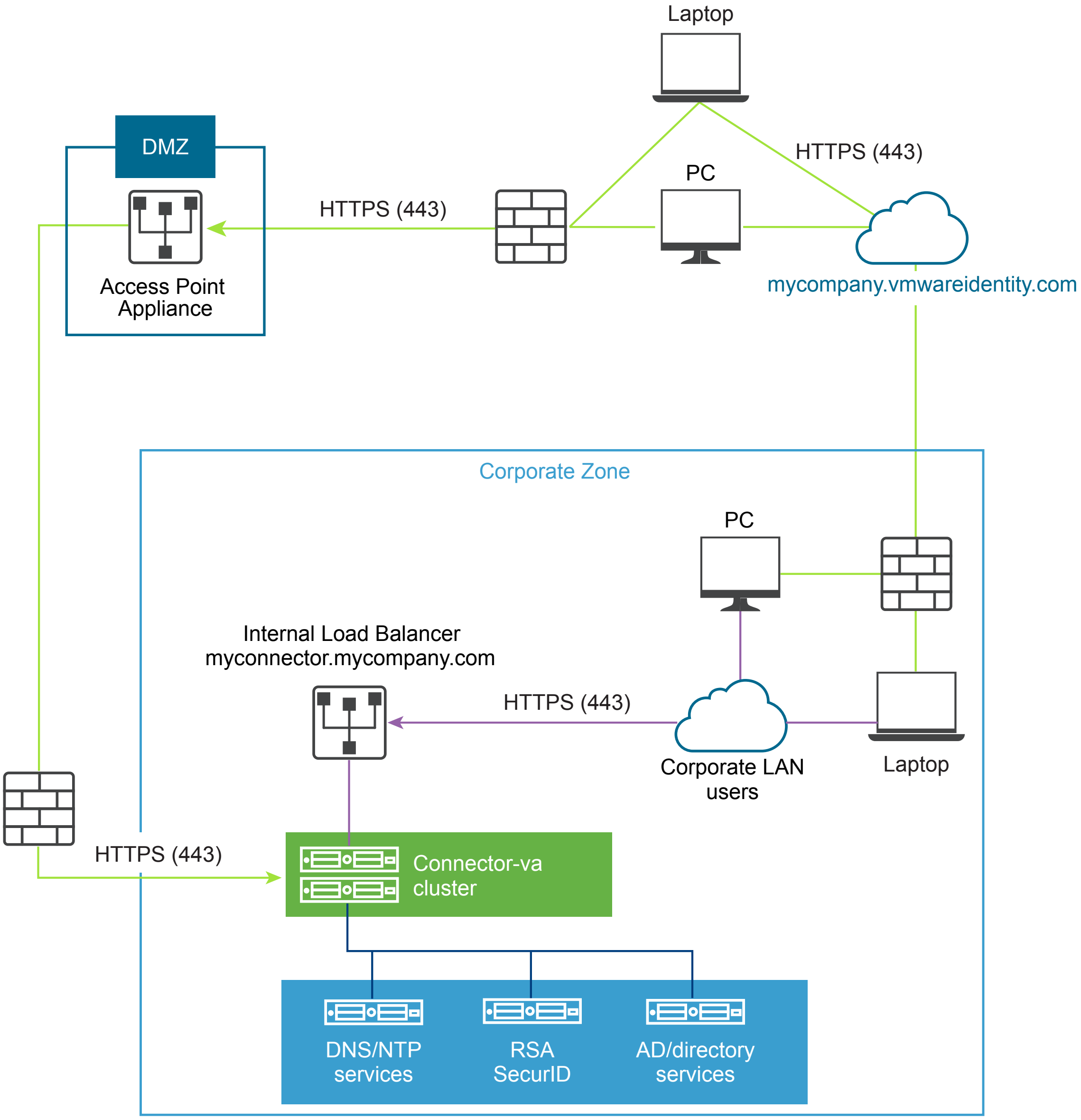
Access Point provides secure remote access to an on-premises deployment of VMware Identity Manager. Access Point virtual appliances are typically deployed in a network demilitarized zone (DMZ). With VMware Identity Manager they operate as a web reverse proxy between the user's browser and the Identity Manager service in the data centre. It also enables remote access to VMware Identity Manager catalogue to launch Horizon applications.

Requirements for Access Point deployment with VMware Identity Manager

- Split DNS
- VMware Identity Manager appliance must have fully qualified domain name (FQDN) as hostname.

- Access Point must use internal DNS. This means that the proxyDestinationURL must use FQDN.

Figure 3-3. Access Point Appliance Pointing the Connector



Sample PowerShell Script

```
name=AP2

source=E:\Access Point 2.6\euc-access-point-2.6.0.0-3643916_OVF10.ova

target=vi://administrator@vsphere.local:PASSWORD@191.168.1.3/Datacenter/host/191.168.1.3

ds=SSD1

netInternet=External
netManagementNetwork=Internal
netBackendNetwork=Internal
```

```
deploymentOption=twonic
ip0=192.168.1.2
ip1=10.11.11.4

dns=10.11.11.1

[SSLCert]

pemCerts=full chain.pem

pemPrivKey=privateKey.pem

[WebReverseProxy]

proxyDestinationURL=https://workspace.myhorizondemo.com

proxyPattern=(/|/SAAS(.*)|/hc(.*)|/web(.*)|/catalog-portal(.*))

unSecurePattern=(/catalog-
portal(.*)|/|/SAAS/|/SAAS|/SAAS/API/1.0/GET/image(.*)|/SAAS/horizon/css(.*)|/SAAS/horizon/angula
r(.*)|/SAAS/horizon/js(.*)|/SAAS/horizon/js-
lib(.*)|/SAAS/auth/login(.*)|/SAAS/jersey/manager/api/branding|/SAAS/horizon/images/(.*)|/SAAS/je
rsey/manager/api/images/(.*)|/hc/(.*)/authenticate/(.*)|/hc/static/(.*)|/SAAS/auth/saml/response
|/SAAS/auth/authenticatedUserDispatcher|/web(.*)|/SAAS/apps/|/SAAS/horizon/portal/(.*)|/SAAS/hori
zon/fonts(.*)|/SAAS/API/1.0/POST/sso(.*)|/SAAS/API/1.0/REST/system/info(.*)|/SAAS/API/1.0/REST/au
th/cert(.*)|/SAAS/API/1.0/REST/oauth2/activate(.*)|/SAAS/API/1.0/GET/user/devices/register(.*)|/S
AAS/API/1.0/oauth2/token(.*)|/SAAS/API/1.0/REST/oauth2/session(.*)|/SAAS/API/1.0/REST/user/resour
ces(.*)|/hc/t/(.*)/(.*)/authenticate(.*)|/SAAS/API/1.0/REST/auth/logout(.*)|/SAAS/auth/saml/respo
nse(.*)|/SAAS/(.*)/(.*)auth/login(.*)|/SAAS/API/1.0/GET/apps/launch(.*)|/SAAS/API/1.0/REST/user/a
pplications(.*)|/SAAS/auth/federation/sso(.*)|/SAAS/auth/oauth2/authorize(.*)|/hc/prepareSaml/fai
lure(.*)|/SAAS/auth/oauthtoken(.*)|/SAAS/API/1.0/GET/metadata/idp.xml|/SAAS/auth/saml/artifact/re
solve(.*)|/hc/(.*)/authAdapter(.*)|/hc/authenticate/(.*)|/SAAS/auth/logout|/SAAS/common.js|/SAA
S/auth/launchInput(.*)|/SAAS/launchUsersApplication.do(.*)|/hc/API/1.0/REST/thinapp/download(.*)
|/hc/t/(.*)/(.*)/logout(.*))
loginRedirectURL=/SAAS/auth/login?dest=%s
authCookie=HZN
```

Tech Preview of Authn Reverse Proxy

Access Point as a solution provides access to catalog for remote users for SSO and access to resources. You must enable Authn reverse proxy on ES Manager. Currently, RSA SecureID and RADIUS authentication methods are supported.

Note You must generate IDP metadata before enabling authentication on web reverse proxy.

Access Point provides remote access to VMware Identity Manager and WIKI with or without authentication from browser-based client and then launch Horizon desktop.

- Browser Desktop to use Access Point as an authenticating reverse proxy so that you must successfully RADIUS authenticate in the DMZ with Access Point using HTML rendered login screens, and only after authentication to be connected to Identity Manager in the corporate network.

Reverse proxy support is limited with Access Point 2.7 release to VMware Identity Manager and internal web resources such as confluence and WIKI. In future, the list of resources will be extended.

Note The `authCookie` and `unSecurePattern` properties are not valid for Authn reverse proxy. You must use `authMethods` property to define the authentication method.

Edge Service Settings for VMware Identity Manager Web Reverse Proxy

These settings are included in the EdgeServiceSettings resource. Use this edge service to configure a reverse Web proxy for VMware Identity Manager. To use this edge service you must have Access Point 2.6 or 2.7.

The REST API URL is https://*access-point-appliance.example.com*:9443/rest/v1/config/edgeservice/webreverseproxy. In this URL, *access-point-appliance.example.com* is the fully qualified domain name of the Access Point appliance.

Example for REST API properties.

```
{
  "locale": "en_US",
  "adminPassword": "*****",
  "cipherSuites":
"TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CB
C_SHA",
  "ssl30Enabled": false,
  "tls10Enabled": false,
  "tls11Enabled": true,
  "tls12Enabled": true,
  "healthCheckUrl": "/favicon.ico",
  "cookiesToBeCached": "none",
  "ipMode": "STATICV4",
  "sessionTimeout": 36000000,
  "quiesceMode": false,
  "monitorInterval": 60
}
```

Table 3-2. REST API Properties for the EdgeServiceSettings Resource for Web Reverse Proxy for vIDM

REST API Property	Description and Example	Values
`enabled`	Specifies whether the service is Enabled in Access Point.	False
`identifier`	Specifies the type of edge service.	None
`proxyDestinationUrl`	Specifies the URL of the proxy requests that the users request to Access Point to access a service. For example, https://vidm-server.example.com.	None
`healthCheckUrl`	Specifies the URL that the load balancer connects to and checks the health of Access Point.	`/favicon.ico` - a graphic inbuilt in Access Point.
`proxyPattern`	Specifies the matching URI paths that are forwarded to the destination URL.	**`(/|/SAAS(.*)|/hc(.*)|/web(.*)|/catalog-portal(.*))`**

Table 3-2. REST API Properties for the EdgeServiceSettings Resource for Web Reverse Proxy for vIDM (Continued)

<table>
<tr><th>REST API Property</th><th>Description and Example</th><th>Values</th></tr>
<tr><td>unSecurePattern</td><td>Specifies an unsecured URL pattern for a login page. This is static content.</td><td><b>(/catalog-portal(.*)|/|/SAAS/|/SAAS|/SAAS/API/1.0/GET/image(.*)|/SAAS/horizon/css(.*)|/SAAS/horizon/angular(.*)|/SAAS/horizon/js(.*)|/SAAS/horizon/js-lib(.*)|/SAAS/auth/login(.*)|/SAAS/jersey/manager/api/branding|/SAAS/horizon/images/(.*)|/SAAS/jersey/manager/api/images/(.*)|/hc/(.*)/authenticate/(.*)|/hc/static/(.*)|/SAAS/auth/saml/response|/SAAS/auth/authenticatedUserDispatcher|/web(.*)|/SAAS/apps/|/SAAS/horizon/portal/(.*)|/SAAS/horizon/fonts(.*)|/SAAS/API/1.0/POST/sso(.*)|/SAAS/API/1.0/REST/system/info(.*)|/SAAS/API/1.0/REST/auth/cert(.*)|/SAAS/API/1.0/REST/oauth2/activate(.*)|/SAAS/API/1.0/GET/user/devices/register(.*)|/SAAS/API/1.0/oauth2/token(.)|/SAAS/API/1.0/REST/oauth2/session(.*)|/SAAS/API/1.0/REST/user/resources(.*)|/hc/t/(.*)/(.*)/authenticate(.*)|/SAAS/API/1.0/REST/auth/logout(.*)|/SAAS/auth/saml/response(.*)|/SAAS/(.*)/(.*)auth/login(.*)|/SAAS/API/1.0/GET/apps/launch(.*)|/SAAS/API/1.0/REST/user/applications(.*)|/SAAS/auth/federation/sso(.*)|/SAAS/auth/oauth2/authorize(.*)|/hc/prepareSaml/failure(.*)|/SAAS/auth/oauthtoken(.*)|/SAAS/API/1.0/GET/metadata/idp.xml|/SAAS/auth/saml/artifact/resolve(.*)|/hc/(.*)/authAdapter(.*)|/hc/authenticate/(.*)|/SAAS/auth/logout|/SAAS/common.js|/SAAS/auth/launchInput(.*)|/SAAS/launchUsersApplication.do(.*)|/hc/API/1.0/REST/thinapp/download(.*)|/hc/t/(.*)/(.*)/logout(.*))</b></td></tr>
<tr><td>authCookie</td><td>Specifies an authentication cookie name.</td><td><b>HZN</b></td></tr>
<tr><td>authMethods</td><td>Specifies the authentication method for Authn reverse proxy.
<b>Note</b> This is applicable as a tech preview for Access Point 2.7 release.</td><td>radius-auth</td></tr>
</table>

Table 3-2. REST API Properties for the EdgeServiceSettings Resource for Web Reverse Proxy for vIDM (Continued)

REST API Property	Description and Example	Values
`cookiesToBeCached`	Specifies the cookies that require to be cached.	None
`loginRedirectURL`	If the user connects to a protected URL, he is redirected.	**`/SAAS/auth/login?dest=%s`**

Access Point Deployment with AirWatch

The Access Point appliance is deployed on the DMZ. Deployment involves installing the Access Point components and the AirWatch components such as Agent, Tunnel Gateway, and Tunnel Proxy services

Deploying the AirWatch Tunnel for your AirWatch environment involves setting up the initial hardware, configuring the server information, and app settings in the AirWatch Admin Console, downloading an installer file, and running the installer on your AirWatch Tunnel server.

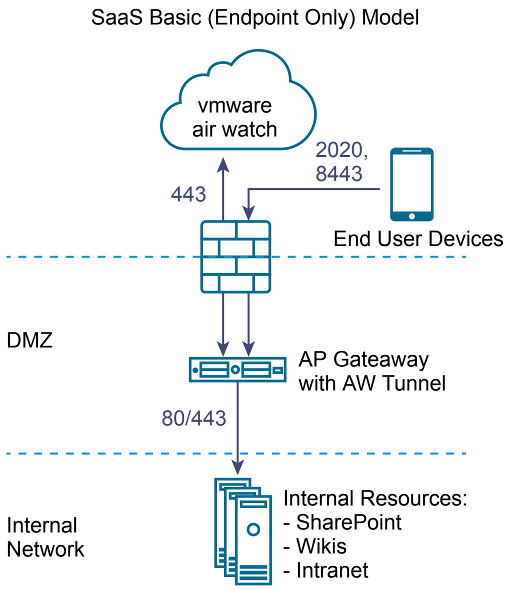
You can manually configure each of the edge services after the OVF installation is completed and the values are changed.

For more information on deploying Access Point with AirWatch, see https://resources.air-watch.com/view/vb7zp7wwhpw756m2pfxy .

Deployment Scenario 1: Tunnel Proxy Deployment

The tunnel proxy deployment secures the network traffic between an end user device and a website through the AirWatch Browser mobile application. The mobile application creates a secure HTTPS connection with the Tunnel Proxy server and protects the sensitive data. To use an internal application with AirWatch Tunnel Proxy, ensure that the AirWatch SDK is embedded in your application which gives you tunneling capabilities with this component.

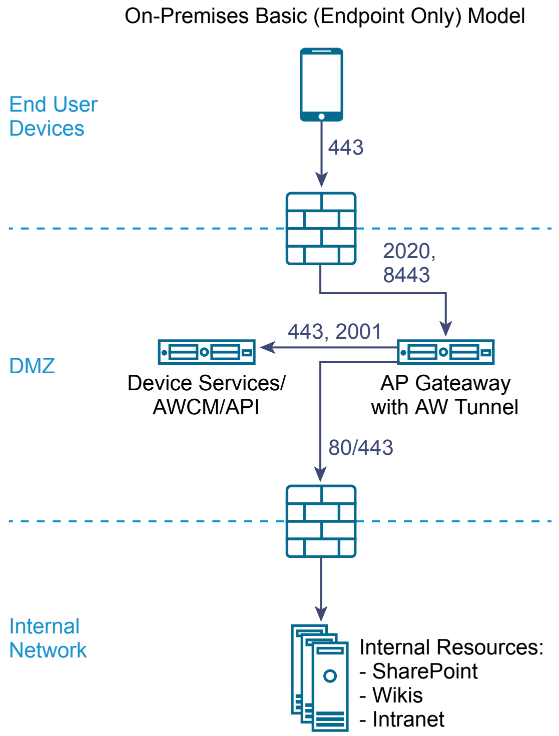
Figure 3-4. Proxy Deployment



Deployment Scenario 2: Tunnel Gateway or Per-App VPN Deployment

The Tunnel Gateway or Per-App VPN Tunnel Deployment allows both internal and public applications to securely access corporate resources that reside in your secure internal network. It uses the Per-App VPN capabilities offered by the operating systems such as iOS 7+ or Android 5.0+. These operating systems allow specific applications approved by the mobility administrators to access internal resources on an app-by-app basis. The advantage of using this solution is that no code change is required to the mobile applications. The support from operating system provides a seamless user experience and added security than any other custom solution.

Figure 3-5. Per-App VPN Deployment



Edge Service Settings for AirWatch

The REST API URL is https://access-point-appliance.example.com:9443/rest/v1/config/edgeservice/. In this URL, access-point-appliance.example.com is the fully qualified domain name of theAccess Point appliance.

REST API Property	Description and Example	Values
apiServerUrl	Specifies the AirWatch API server URL.	**`[http[s]://]hostname[:port]`** The destination URL must contain the protocol, host name or IP address, and port number (example: https://load-balancer.example.com:443) Default: none.
apiServerUsername	Specifies the username to login into API server.	Default: none.
apiServerPassword	Specifies the password to login into the API server.	Default: none.
organizationGroupCode	Specifies the organization of the user.	Default: none.

REST API Property	Description and Example	Values
airwatchServerHostname	Specifies the AirWatch server hostname.	Default: none.
reinitializeGatewayProcess	Specifies if the Tunnel Gateway or Tunnel Proxy service is initialized. If the value is True, reinitialize the Tunnel Gateway or Tunnel Proxy by force.	False
outboundProxyHost	Specifies the host where the Outbound Proxy is installed. This is different from Tunnel Proxy.	Default: none.
outboundProxyPort	Specifies the port of the Outbound Proxy.	8080
ntlmAuthentication	Specifies if the NTLM authentication is configured for Outbound Proxy.	False
outboundProxyUsername	Specifies the username to login into the Outbound Proxy.	Default: none.
outboundProxyPassword	Specifies the password to login into Outbound Proxy.	None
airwatchOutboundProxy	Specifies if the Outbound Proxy is configured. It the value is True, the outbound proxy is configured.	False
airwatchComponentsInstalled	Specifies the list of AirWatch components that are installed.	Tunnel Proxy

Configuring Access Point Using TLS/SSL Certificates

4

You must configure the TLS/SSL Certificates for Access Point appliances.

Note Configuring the TLS/SSL certificates for Access Pointappliance applies to Horizon View, Horizon Air Hybrid-Mode, and Web Reverse Proxy only.

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, or to use the PowerShell scripts, 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 `mycaservercert.pfx`, use the following commands to convert the certificate:

   ```
   openssl pkcs12 -in mycaservercert.pfx -nokeys -out mycaservercert.pem
   openssl pkcs12 -in mycaservercert.pfx -nodes -nocerts -out mycaservercert.pem
   openssl rsa -in mycaservercertkey.pem -check -out mycaservercertkeyrsa.pem
   ```

3. Edit `mycaservercert.pem` and remove any unnecessary certificate entries. It should contain the one SSL server certificate followed by any necessary intermediate CA certificates and root CA certificate.

4. 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. If you have an intermediate certificate, that certificate must also be in one-line format and add to the first certificate so that both certificates are on the same line.

You can now configure certificates for Access Point by using these `.pem` files with the PowerShell scripts attached to the blog post "Using PowerShell to Deploy VMware Access Point," available at https://communities.vmware.com/docs/DOC-30835. Alternatively, you can 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 41. For smart card certificates, see "Configure Smart Card Authentication on the Access Point Appliance," on page 45.

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 PowerShell scripts or 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.

This procedure describes how to use the REST API to replace the certificate. An easier alternative might be to use the PowerShell scripts attached to the blog post "Using PowerShell to Deploy VMware Access Point," available at https://communities.vmware.com/docs/DOC-30835. If you have already deployed the named Access Point appliance, then running the script again will power off the appliance, delete it, and redeploy it with the current settings you specify.

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 40.

- 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 or 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 v1.1 and TLS v1.2 are enabled. TLS v1.0 is disabled and SSL v3.0 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 "Configuration Settings for System Settings and Server Certificates," on page 59.

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": "false",
  "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.

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

```
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
```

ciphers.json is the JSON request you created in the previous step.

The cipher suites and protocols that you specified are used.

Configuring Authentication in DMZ 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 configure Access Point appliance to perform Smart Card authentication, RSA SecurID authentication, and RADIUS authentication.

Note The Smart Card, RSA SecurID, and RADIUS authentication methods are not applicable to AirWatch deployment.

This chapter includes the following topics:

Configure Smart Card Authentication on the Access Point Appliance

You can configure 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.

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 the Horizon server by using a SAML assertion.

You can also set up authentication so that Access Point requires smart card authentication but then authentication is also passed through to the server, which might require Active Directory authentication. To configure this type of chained authentication, see the `authMethods` property, described in "Common Configuration Settings for Edge Services," on page 61.

Note For VMware Identity Manager, authentication is always only passed through Access Point to VMware Identity Manager. You can configure smart card authentication to be performed on the Access Point appliance only if Access Point is being used with Horizon 7.

Generate Access Point SAML Metadata

You must generate SAML metadata on the Access Point appliance and exchange metadata with the 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 scenario, Access Point is the identity provider and the server is the service provider.

In this procedure, you generate Access Point SAML metadata by using the Access Point REST API. Related topics will describe how to copy this generated SAML metadata to the applicable server.

Prerequisites

- Configure the clock (UTC) on the Access Point appliance so that the appliance has the correct time. For example, open a console window on the Access Point virtual machine and use arrow buttons to select the correct time zone. Also 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 server host, smart card authentication might not work.

- 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 the 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 40.

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
```

The contents of this file begin with the following text:

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

Creating a SAML Authenticator Used by Other Service Providers

After you generate SAML metadata on the Access Point appliance, you can copy that data to the back-end service provider. Copying this data to the service provider is part of the process of creating a SAML authenticator so that Access Point can be used as an identity provider.

For a Horizon Air Hybrid-mode server, see the product documentation for specific instructions.

Copy Service Provider SAML Metadata to Access Point

After you create and enable a SAML authenticator so that Access Point can be used as an identity provider, you can generate SAML metadata on that back-end system and use the metadata to create a service provider on the Access Point appliance. This exchange of data establishes trust between the identity provider (Access Point) and the back-end service provider, such as View Connection Server.

Prerequisites

Verify that you have created a SAML authenticator for Access Point on the back-end service provider server.

Procedure

1 Retrieve the service provider SAML metadata, which is generally in the form of an XML file.

For instructions, refer to the documentation for the service provider.

Different service providers have different procedures. For example, you must open a browser and enter a URL such as: https://*connection-server.example.com*/SAML/metadata/sp.xml

You can then use a **Save As** command to save the Web page to an XML file. The contents of this file begin with the following text:

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

2 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.

```
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
```

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 for a service provider, and *connection-server-metadata.xml* is the metadata file you created in the previous step.

Access Point and the service provider 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.

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 48.

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 is used in Step 4 of this procedure.

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.

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 48. 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 40. 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 the service provider and copied the service provider SAML metadata to Access Point appliance.
- Familiarize yourself with the smart card certificate properties and determine which settings to use. See "Smart Card Certificate Properties for Advanced Options," on page 50.
- If you use a load balancer between Access Point and the service provider instances, verify that TLS/SSL termination is not done on the load balancer. The load balancer must be configured to pass authentication through to the back-end service provider, such as 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 the edge service you are using.

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

   This example uses the VIEW edge service because for this release smart card authentication is supported only if you use the VIEW edge service.

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

   For readability, this example shows only the required properties for configuring smart card authentication, and not the long list of properties included in edge service configuration. When you create the JSON request, copy and paste all of the edge service settings you are using and be sure to add or configure these smart card properties.

   connection-server-sp is an example of a service provider name. You specified a service provider name when you copied the service provider metadata to the Access Point appliance.

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

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

Property Name	Description	Valid Values
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.
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

Configure RSA SecurID Authentication on the Access Point Appliance

On the Access Point appliance, you must enable RSA SecurID authentication, copy in the contents of the configuration file for the RSA SecureID server, and change the authentication type to RSA SecurID authentication.

Prerequisites

- Verify that the server to be used as the authentication manager server has the RSA SecurID software installed and configured.
- Export the `sdconf.rec` file from the RSA Secure Authentication Manager server. See the RSA Authentication Manager documentation.

Procedure

1 After downloading the `sdconf.rec` file from the RSA Secure Authentication Manager server, run the following commands to change the file format into Base64 and convert that format to a one-line format that can be passed in a JSON string to the Access Point REST API.

   a Run a command, Linux `base64` command to produce the Base64 encoding format for the `sdconf.rec` file.

   ```
   base64 sdconf.rec > sdconfBase64.txt
   ```

   b Run a `cat` command to convert the Base64 file to single-line JSON format.

   ```
   cat sdconfBase64.txt | tr '\n' '\\' | sed -e 's/\\/\\n/g'
   ```

2 Use a REST client, such as `curl` or `postman`, to invoke the Access Point REST API and get the default RSA SecurID authentication settings.

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

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

3 Paste the output of the `cat` command into the `serverConfig` field of a JSON request for enabling RSA SecurID authentication.

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

   ```
   {
   "enabled": "true",
   "name": "securid-auth",
   "numIterations": "5",
   "externalHostName": "10.20.30.40",
   "internalHostName": "10.20.30.40",
   "nameIdSuffix": ""
   "serverConfig": ""OwYFI7owv5UrAdlfnOsW2 ... nVesmbkLRjNOYxqm"
   }
   ```

   In this example, the ellipses indicate the middle content of the base64 `sdconfBase64.txt` file. The format of this file must be one-line format that can be passed in a JSON string to the Access Point REST API.

   Use `externalHostName` to specify the external address of the Access Point appliance that is specified in the SecurID server's agent, and use `internalHostName` to specify the internal, static IP address of the Access Point appliance.

   Use `numIterations` to specify the number of attempts that are allowed for logging in. In this example, a user is allowed 5 attempts to supply the correct SecurID code.

4 Use a REST client to get the default edge service settings for the Horizon server.

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

   This example specifies the VIEW edge service because for this release two-factor authentication is supported only if you use the View edge service.

5 Paste the following information into a JSON request for enabling RSA SecurID authentication for the Horizon server and add the `authMethods` property.

```
{
  "identifier": "VIEW",
  "enabled": true,
  "proxyDestinationUrl": "https://horizon-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",
  "authMethods": "securid-auth"
}
```

This example shows only some of the properties that are common to all edge services. In this example, *horizon-server.example.com* is the fully qualified domain name of the Horizon server. You specified this name when you deployed 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 RSA SecurID authentication.

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

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

End users can now use RSA SecurID tokens when logging in to Access Point.

Configure RADIUS Authentication on the Access Point Appliance

On the Access Point appliance, you must enable RADIUS authentication, specify some configuration settings from the RADIUS server, and change the authentication type to RADIUS authentication.

Prerequisites

- Verify that the server to be used as the authentication manager server has the RADIUS software installed and configured. Follow the vendor's configuration documentation.
- Make a note of the RADIUS server's host name or IP address, the port number on which it is listening for RADIUS authentication (usually 1812), the authentication type (PAP, CHAP, MSCHAPv1, or MSCHAPv2), and the shared secret.

  You can enter values for a primary and a secondary RADIUS authenticator.

Procedure

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

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/radius-auth
```

2 To enable RADIUS authentication, create a JSON request by using the settings returned from the `curl` or `postman` command.

Access Point 2.6 supports three new properties for RADIUS authentication.

Table 5-2. Properties for Radius Authentication

Option	Description
`directAuthChainedUsername`	Enables direct authentication to RADIUS server during auth chaining. Default value is NULL.
`enabledAux`	Enables the secondary RADIUS server when set to TRUE. Default value is FALSE.
`nameIdSuffix`	Specifies the nameId which enables View to provide TrueSSO experience. It is empty by default.

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

```
{
"enabled": "true",
"name": "radius-auth",
"hostName": "10.10.10.10",
"hostName_2": "20.20.20.20",
"serverTimeout": "3",
"serverTimeout_2": "3",
"radiusDisplayHint": "",
"numIterations": "5",
"numAttempts": "5",
"numAttempts_2": "5",
"realmPrefix": "",
"realmPrefix_2": "",
"realmSuffix": "",
"realmSuffix_2": "",
"authPort": "1812",
"authPort_2": "1812",
"accountingPort": "0",
"accountingPort_2": "0",
"sharedSecret": "_PASSWORD_PLACEHOLDER_J94SP2QO45E6R8X2M_",
"sharedSecret_2": "_PASSWORD_PLACEHOLDER_J94SP2QO45E6R8X2M_",
"authType": "MSCHAP2",
"authType_2": "PAP"
}
```

Property	Description
hostName	The IP address of the RADIUS server. Use `hostName_2` to specify a secondary server.
serverTimeout	The number of seconds taken for the server timeout interval. Use `serverTimeout_2` to configure the secondary server. For all of the following properties, the property names with "_2" are for configuring the secondary server, if you use one.
numAttempts	The number of login attempts that are allowed. In this example, a user is allowed 5 attempts to supply the correct RADIUS code.
realmPrefix	The string that is placed at the beginning of the user name when it is sent to the RADIUS server. For example, if the user name entered is **`jdoe`** and the realm prefix is **`DOMAIN-A\`**, the user name **`DOMAIN-A\jdoe`** is sent to the RADIUS server.
realmSuffix	If you specify a realm suffix or postfix string, the string that is placed at the end of the user name when it is sent to the RADIUS server. For example, if the user name entered is **`jdoe`** and the realm suffix is **`@mycorp.com`**, the user name **`jdoe@mycorp.com`** is sent to the RADIUS server.
authPort	The authentication port number of the RADIUS server. The default is 1812.

Property	Description
accountingPort	Set this port to 0 unless you want to enable RADIUS accounting. Set this port to a non-zero number only if your RADIUS server supports collecting accounting data. If the RADIUS server does not support accounting messages and you set this port to a non-zero number, the messages are sent, ignored, and retried a number of times, resulting in a delay in authentication. Accounting data is used to bill users based on usage time and data. Accounting data can also be used for statistical purposes and for general network monitoring.
sharedSecret	The shared secret.
authType	The authentication type: PAP, CHAP, MS-CHAPv1, or MS-CHAPv2.

3 Use a REST client to get the default edge service settings for the Horizon server.

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

This example specifies the VIEW edge service because for this release two-factor authentication is supported only if you use the VIEW edge service.

4 Paste this information into a JSON request for enabling RADIUS authentication for the Horizon server and add the `authMethods` property.

```
{
  "identifier": "VIEW",
  "enabled": true,
  "proxyDestinationUrl": "https://horizon-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",
  "authMethods": "radius-auth"
}
```

This example shows only some of the properties that are common to all edge services. In this example, *horizon-server.example.com* is the fully qualified domain name of the Horizon server. You specified this name when you deployed the Access Point appliance. The text for `proxyDestinationUrlThumbprints` is an example only. Replace this text with the thumbprint of your destination server.

5 Use a REST client to send the JSON request to the Access Point API and configure the edge service to use RADIUS authentication.

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

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

End users can now use a RADIUS code when logging in to Access Point.

Using the Access Point REST API 6

To change or add configuration settings after you deploy the Access Point appliance, you can either use the Access Point REST API or you can deploy the appliance again, using different settings.

Note 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, open a console window on the Access Point virtual machine and use arrow buttons to select the correct time zone. Also 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.

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:Password' https://access-point-appliance.example.com:
9443/rest/v1/config/settings
```

In this example, *Password* is the password for the administrator 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. You could use the PUT method for this request:

```
{
  "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",
  "healthCheckUrl": "/favicon.ico",
  "pcoipEnabled": true,
  "pcoipExternalUrl": "10.20.30.40:4172",
  "blastEnabled": true,
  "blastExternalUrl": "https://ap1.example.com:443",
  "tunnelEnabled": true,
  "tunnelExternalUrl": "https://ap1.example.com:443"
  "proxyPattern": "/",
  "matchWindowsUserName": false,
  "gatewayLocation": "External",
  "windowsSSOEnabled": false
}
```

This example shows the following settings:

Configuration	Options
identifier	`enabled` **Note** Setting `identifier` to `VIEW` means that Access Point can communicate with servers that use the View XML protocol, such as View Connection Server, Horizon Air, and Horizon Air Hybrid-mode. Setting `identifier` to `webreverseproxy` means that you can use the Web Reverse Proxy edge service, a feature that is available with Access Point 2.6. For example, you would use the Web Reverse Proxy edge service with VMware Identity Manager.
Address of the Horizon server or load balancer	`proxyDestinationUrl`
Horizon server's security certificate thumbprint	`proxyDestinationUrlThumbprints`

This example also shows the following settings that are specific to the View edge service:

- 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.

This chapter includes the following topics:

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).

Configuration Settings for System Settings and Server Certificates

Use the Access Point REST API properties to configure the security certificates, protocols, and cipher suites are used, set up smart card authentication, and more.

You can use the properties listed below to make configuration changes after the Access Point appliance is deployed, or you can alternatively use the OVF Tool property --X:enableHiddenProperties=settingsJSON in the list of 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 20.

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 6-1. 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 with the settings for enabling various security protocols.	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA
ssl30Enabled	Specifies whether the SSLv3.0 security protocol is enabled.	FALSE
tls10Enabled	Specifies whether the TLSv1.0 security protocol is enabled.	FALSE
tls11Enabled	Specifies whether the TLSv1.1 security protocol is enabled.	TRUE
tls12Enabled	Specifies whether the TLSv1.2 security protocol is enabled.	TRUE

Table 6-1. REST API Properties for the SystemSettings Resource (Continued)

REST API Property	Description and Example	Default Value
`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.
`healthCheckUrl`	Specifies the URL that the load balancer connects and checks the health of Access Point.	`/favicon.ico` which is a graphic inbuilt in Access Point.
`quiesceMode`	Pause or alter a device or application to achieve a consistent state.	FALSE
`monitorInterval`	Monitors the interval that the backend systems take to respond to Access Point.	60 seconds

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 6-2. 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

Common Configuration Settings for Edge Services

In addition to specifying system settings, you must configure the edge service for the type of role you want Access Point to engage. For example, you configure the View edge service to use Access Point with VMware Horizon 7 or VMware Horizon Air Hybrid-Mode. You configure the Web Reverse Proxy service to use Access Point with VMware Identity Manager.

Edge Service Settings That Are Common to All Types of Edge Services

The properties listed in the following table must be configured regardless of which type of edge service you configure. These settings are included in the EdgeServiceSettings resource. The REST API URL is https://*access-point-appliance.example.com*:9443/rest/v1/config/edgeservice/*edge-service-type*. In this URL, *access-point-appliance.example.com* is the fully qualified domain name of the Access Point appliance.

NOTE The REST API properties for the resource are generic to View and VMware Identity Manager. However, the specific supported properties are listed in the topics for View and Web Reverse Proxy services exclusively.

Table 6-3. REST API Properties for the EdgeServiceSettings resource

REST API Property	Description and Example	Default Value
`enabled`	If set to TRUE, specifies that the edge service is enabled.	FALSE
`identifier`	Specifies the type of edge service. The following values are valid for the property: ■ `VIEW` uses the edge service for servers that use the View XML protocol. These servers can include View Connection Server, which is included with VMware Horizon 6 and VMware Horizon 7, and servers used with VMware Horizon Air and VMware Horizon Air Hybrid-mode. ■ `webreverseproxy` uses the Web reverse proxy edge service. This edge service requires Access Point 2.6. Use this edge service for VMware Identity Manager.	None
`proxyDestinationUrl`	Specifies the URL of the VMware Horizon server or load balancer to which the Access Point appliance directs traffic. 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 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, for 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 Horizon server URL. ■ Click the lock icon in the address bar. ■ View the certificate details.	None

Table 6-3. REST API Properties for the EdgeServiceSettings resource (Continued)

REST API Property	Description and Example	Default Value
`healthCheckUrl`	Specifies the URL that the load balancer connects to, and checks the health of Access Point.	`/favicon.ico` - a graphic inbuilt in Access Point.
`unSecurePattern`	Specifies the matching URI paths that are forwarded to the destination URL.	None
`authMethods`	Specifies the type of authentication to use. Set this property to one of the following values unless you want to use pass-through authentication: ■ `sp-auth`, the default, means that authentication is passed through to the service provider (Horizon server). ■ `certificate-auth` means smart card authentication is mandatory. ■ `certificate-auth || sp-auth` means smart card authentication is optional. If a smart card is not used, pass-through authentication is used. ■ `radius-auth && sp-auth` means RADIUS two-factor authentication is used followed by pass-through. ■ `securid-auth && sp-auth` means RSA SecurID authentication is used followed by pass-through. ■ `saml-auth` means SAML authentication is used. ■ `saml-auth || sp-auth` means SAML authentication is optional. If SAML authentication is not used, pass-through authentication is used.	By default, authentication is passed through to the Horizon server, which can be configured for AD password, RSA SecurID, RADIUS, or SAML.
`authCookie`	Specifies an authentication cookie name.	None
`smartCardHintPrompt`	If set to TRUE, enables the Access Point appliance to support the smart card user name hints feature. The smart card user name hints feature is supported only with Access Point 2.7.2 and later. With the smart card user hints feature, a user's smart card certificate can map to multiple Active Directory domain user accounts.	TRUE

Using REST API for Blast Statistics

Use the Access Point REST API to monitor active Blast Secure Gateway sessions.

Before you can get statistics for Blast Secure Gateway sessions, you must set `blastEnabled=true` in the EdgeServiceSettings resource.

The property in the following table is included in the EdgeServiceSettings resource. The REST API URL is https://*access-point-appliance.example.com*:9443/rest/v1/config/edgeservice/*edge-service-type*. In this URL, *access-point-appliance.example.com* is the fully qualified domain name of the Access Point appliance.

Table 6-4. REST API Property for the EdgeServiceSettings Resource

REST API Property	Description and Example	Default Value
`blastEnabled`	If set to TRUE, enables the Blast Secure Gateway session.	FALSE

Use the GET method to get Blast Secure Gateway statistics. The REST API URL is https://*access-point-appliance.example.com*:9443/rest/v1/monitor/stats. In this URL, *access-point-appliance.example.com* is the fully qualified domain name of the Access Point appliance. The statistics are included in the viewEdgeServiceStats resource.

The following example is a sample output:

```
<viewEdgeServiceStats>
<protocol name="blast">
      <status>
        <status>RUNNING</status>
      </status>
      <sessions>1</sessions>
      <maxSessions>1</maxSessions>
    </protocol>
</viewEdgeServiceStats>
```

Using Rest API for AirWatch

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 JSON requests to invoke the Access Point REST API and make configuration changes. The following example shows a configuration JSON for AirWatch edge services.

- Tunnel Gateway Edge Service

  The Tunnel Gateway uses PUT method for API request. The path is located at `/v1/config/edgeservice/tunnelgateway`. The following example is a sample input.

```
 { "identifier": "TUNNEL_GATEWAY",
"enabled": true,
"proxyDestinationUrl": "https://[fc00:10:112:54::220]",
"healthCheckUrl": "/favicon.ico",
"apiServerUrl": "https://dev41.airwatchdev.com",
"apiServerUsername": "orange",
"apiServerPassword": “orange",
"organizationGroupCode": "orange",
"airwatchServerHostname": "10.143.109.23",
"reinitializeGatewayProcess": false,
"airwatchComponentsInstalled": "TUNNEL,PROXY" }
```

- Tunnel Proxy Edge Service

  The Tunnel Proxy uses PUT method for API request. The path is located at `/v1/config/edgeservice/tunnelproxy`. The following example is a sample input.

```
 { "identifier": "TUNNEL_PROXY",
"enabled": true,
"proxyDestinationUrl": "https://[fc00:10:112:54::220]",
"healthCheckUrl": "/favicon.ico",
"apiServerUrl": "https://dev41.airwatchdev.com",
"apiServerUsername": "orange",
"apiServerPassword": “orange",
"organizationGroupCode": "orange",
"airwatchServerHostname": "10.14.10.23",
"reinitializeGatewayProcess": false,
"airwatchComponentsInstalled": "TUNNEL,PROXY" }
```

For more information on REST APIs, see Chapter 6, “Using the Access Point REST API,” on page 57.

Troubleshooting Access Point Deployment

7

You can use a variety of procedures to diagnose and fix problems that you encounter when you deploy Access Point in your environment.

You can use troubleshooting procedures to investigate the causes of such problems and attempt to correct them yourself, or you can obtain assistance from VMware Technical Support.

This chapter includes the following topics:

- "Troubleshooting Deployment Errors," on page 65
- "Collecting Logs from the Access Point Appliance," on page 66
- "Enabling Debug Mode," on page 67

Troubleshooting Deployment Errors

You might experience difficulty when you deploy Access Point in your environment. You can use a variety of procedures for diagnosing and fixing problems with your deployment.

Security warning when running scripts downloaded from internet

Verify that the PowerShell script is the script you intend to run, and then from the PowerShell console, run the following command:

```
unblock-file .\apdeploy.ps1
```

ovftool command not found

Verify that you have installed the OVF Tool software on your Windows machine and that it is installed in the location expected by the script.

Invalid Network in property netmask1

- The message might state netmask0, netmask1 or netmask2. Check that a value has been set in the .INI file for each of the three networks such as netInternet, netManagementNetwork, and netBackendNetwork.
- Verify that a vSphere Network Protocol Profile has been associated with every referenced network name. This specifies network settings such as IPv4 subnet mask, gateway, and so on. Ensure the associated Network Protocol Profile has correct values for each of the settings.

Warning message about the operating system identifier being not supported

The warning message displays that the specified operating system identifier SUSE Linux Enterprise Server 12.0 64-bit (id:85) is not supported on the selected host. It is mapped to the following OS identifier: Other Linux (64-bit).

Ignore this warning message. It is mapped to a supported operating system automatically.

Configure Access Point for RSA SecurID authentication

Add the following lines to the Horizon section of the .INI file.

```
authMethods=securid-auth && sp-auth
matchWindowsUserName=true
```

Add a new section at the bottom of you .INI file.

```
[SecurIDAuth]
serverConfigFile=C:\temp\sdconf.rec
externalHostName=192.168.0.90
internalHostName=192.168.0.90
```

The IP addresses should both be set to the IP address of Access Point. The sdconf.rec file is obtained from RSA Authentication Manager which must be fully configured. Verify that you are using Access Point 2.5 or later version and that the RSA Authentication Manager server is accessible on the network from Access Point. Rerun apdeploy Powershell command to redeploy your Access Point configured for RSA SecurID.

Locator does not refer to an object error

The error notifies that the target= value that is used by vSphere OVF Tool is not correct for your vCenter environment. Use the table listed in https://communities.vmware.com/docs/DOC-30835 for examples of the target format used to refer to a vCenter host or cluster. The top level object is specified as follows:

```
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/
```

The object now lists the possible names to use at the next level.

```
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host/Cluster1/
or
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host/esxhost1
```

The folder names, hostnames, and cluster names used in the target are case sensitive.

Collecting Logs from the Access Point Appliance

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 7-1. 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 7-2. 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.

Access Point Log Files for AirWatch

- `/var/log/airwatch/tunnel/vpnd`

  The tunnel-init.log and tunnel.log are captured from this directory.

- `/var/log.airwatch/proxy`

  The proxy.log is captured from this directory.

- `/var/log/airwatch/appliance-agent`

  The appliance-agent.log is captured from this directory.

Enabling Debug Mode

You can enable the debug mode for an Access Point appliance to view or manipulate the internal state of the appliance. The debug mode lets you test the deployment scenario in your environment.

Prerequisites

- Verify that the Access Point appliance is not in use.

> **Note** It is useful to gather logging information on an Access Point appliance that is not working. The logs can be obtained in the typical way.

Procedure

1 Login to the Access Point machine.

2 Enter the following command in the command line interface.

```
cd /opt/vmare/gateway/conf
```

3 View the log properties file.

```
vi log4j–esmanager.properties
```

4 Locate the following line in the properties file and edit. Replace info by debug.

```
log4j.logger.com.vmware=info,default
```

5 Enter the command to change the logging configuration from any path.

```
supervisorctl restart esmanager
```

Index