Deploying and Configuring Access Point

Unified Access Gateway 2.8

vmware®

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

https://docs.vmware.com/

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 VMware Access Point

Deploying and Configuring Access Point provides information about designing VMware Horizon®, VMware Identity Manager™, and VMware AirWatch® deployment that uses VMware Access Point™ for secure external access to your organization's applications. These applications can be 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.

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 data center operations.

Preparing to Deploy 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.

This section includes the following topics:

Access Point as a Secure Gateway

Access Point is a layer 7 security appliance that is normally installed in a demilitarized zone (DMZ). Access Point is used to ensure that the only traffic entering the corporate data center is traffic on behalf of a strongly authenticated remote user.

Access Point directs authentication requests to the appropriate server and discards any unauthenticated request. 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, to accurately control access.

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 extra layer of security by shielding virtual desktops, application hosts, and servers from the public-facing Internet.

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

Using Access Point Instead of a Virtual Private Network

Access Point and generic VPN solutions are similar as they both ensure that traffic is forwarded to an internal network only on behalf of strongly authenticated users.

Access Point advantages over generic VPN include the following.

- Access Control Manager. Access Point applies access rules automatically. Access Point recognizes the entitlements of the users and 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 to maintain the required rules.
- User Interface. Access Point does not alter the straightforward Horizon Client user interface. With Access Point, when the Horizon Client is launched, authenticated users are in their View environment and have controlled access to their desktops and applications. A VPN requires that you must set up the VPN software first and authenticate separately before launching the Horizon Client.
- Performance. Access Point is designed to maximize security and performance. With Access Point, PCoIP, HTML access, and WebSocket protocols are secured without requiring additional encapsulation. VPNs are implemented as SSL VPNs. This implementation meets security requirements and with Transport Layer Security (TLS) enabled, are considered secure, but the underlying protocol with SSL/TLS is just TCP-based. With modern video remoting protocols exploiting connectionless UDPbased 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 System and Network Requirements

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

VMware Product Versions Supported

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.

Access Point 2.8 can be used as a secure gateway with the following VMware offerings.

- Vmware AirWatch 8.4 and later
- VMware Identity Manager 2.7 and later

- VMware Horizon 6.2 and later
- VMware Horizon Air Hybrid Mode 1.0 and later
- VMware Horizon Air 15.3 and later

Hardware Requirements for ESXi Server

The Access Point appliance 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.

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. If you do not install this plug-in before you start the deployment wizard, the wizard prompts you to install the plug-in. This requires that you close the browser and exist the wizard.

Note 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 time is synchronized with the 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 ESX ihost.

Virtual Appliance 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.

Ensure that the datastore you use for the appliance has enough free disk space and meets other system requirements.

- Virtual appliance download size is 2.5 GB
- Thin-provisioned disk minimum requirement is 2.5 GB
- Thick-provisioned disk minimum requirement is 20 GB

The following information is required to deploy the virtual appliance

- Static IP address
- IP address of the DNS server
- Password for the root user
- URL of the server instance of the load balancer that the Access Point appliance points to

Networking Configuration 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 are rotated by default. You must use syslog to preserve these log entries. See Collecting Logs from the Access Point Appliance.

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.

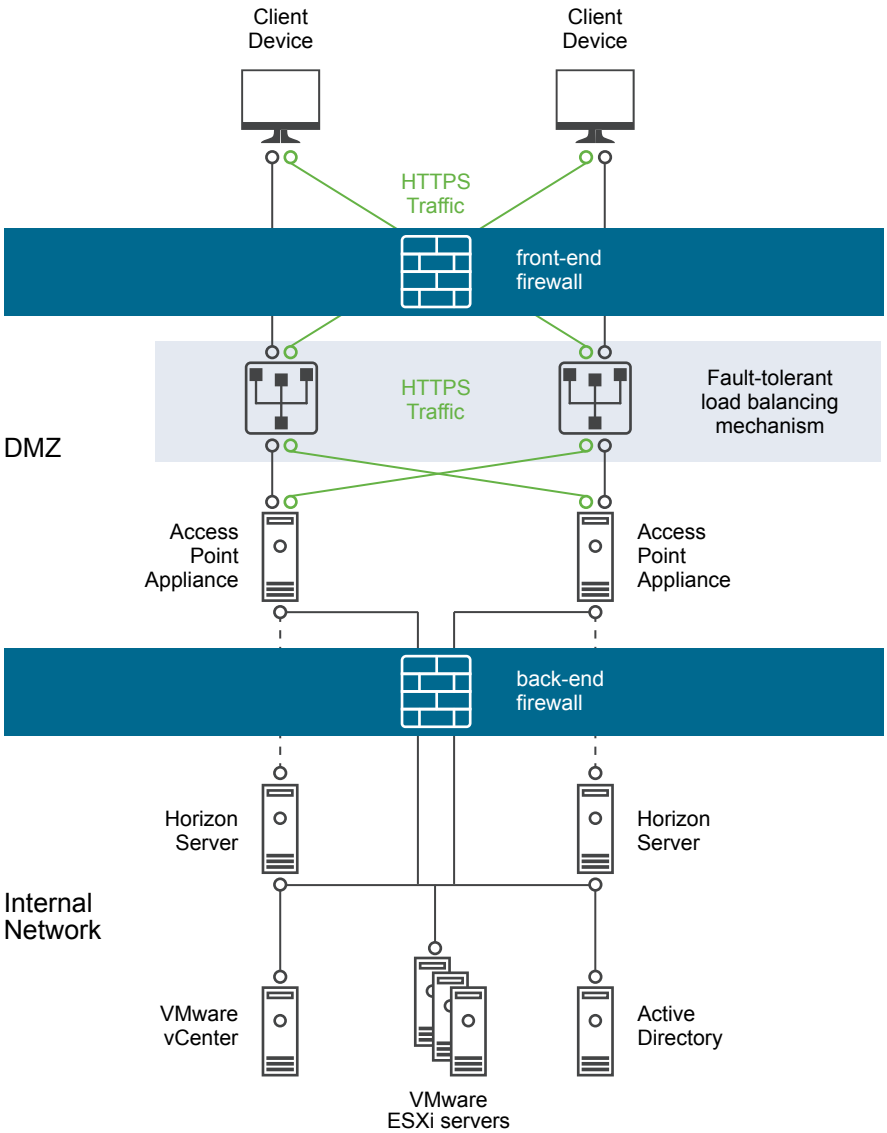
- An external network-facing, front-end firewall is required to protect both the DMZ and the internal network. You configure this firewall to allow external network traffic to reach the DMZ.
- A back-end firewall, between the DMZ and the internal network, is required to provide a second tier of security. 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 1-1. Dual Firewall Topology



Access Point Load Balancing Topologies

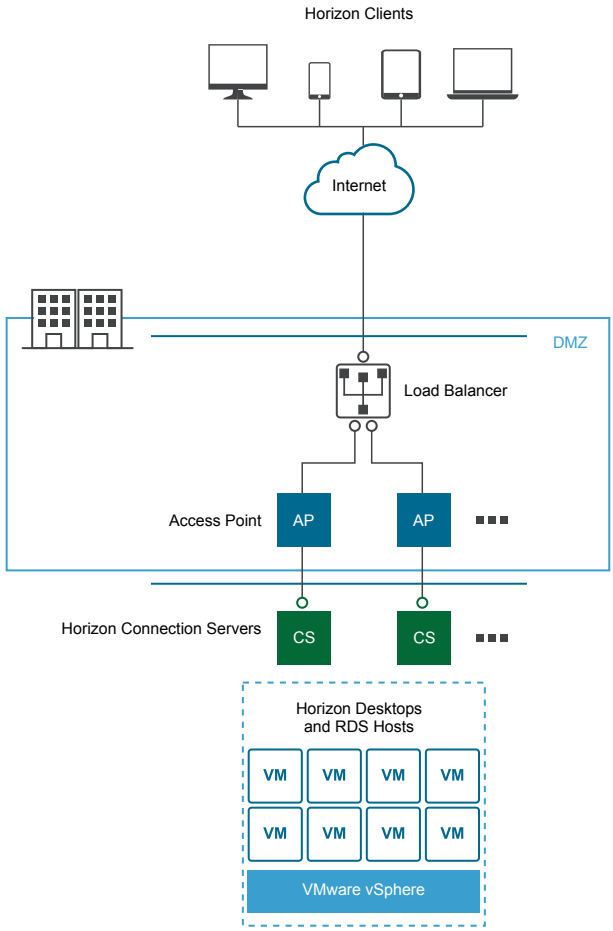
You can implement any of several different topologies.

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 have a load balancer 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.

Figure 1-2. Multiple Access Point Appliances Behind a Load Balancer



Horizon Protocols

When a Horizon Client user connects to a Horizon environment, several different protocols are used. The first connection is always the primary XML-API protocol over HTTPS. Following successful authentication, one or more secondary protocols are also made.

- Primary Horizon Protocol

  The user enters a hostname at the Horizon Client and this starts the primary Horizon protocol. This is a control protocol for authentication authorization, and session management. It uses XML structured messages over HTTPS (HTTP over SSL). This protocol is sometimes known as the Horizon XML-API control protocol. In a load balanced environment as shown above in the Multiple Access Point Appliances Behind a Load Balancer figure, the load balancer routes this connection to one of the Access Point appliances. The load balancer usually selects the appliance based first on availability, and then out of the available appliances routes traffic based on the least number of current sessions. This configuration evenly distributes the traffic from different clients across the available set of Access Point appliances

- Secondary Horizon Protocols

  After the Horizon Client establishes secure communication to one of the Access Point appliances, the user authenticates. If this authentication attempt is successful, then one or more secondary connections are made from the Horizon client. These secondary connections can include the following

  - HTTPS Tunnel used for encapsulating TCP protocols such as RDP, MMR/CDR and the client framework channel. (TCP 443).
  - Blast Extreme display protocol (TCP 443 and UDP 443).
  - PCoIP display protocol (TCP 4172 and UDP 4172).

These secondary Horizon protocols must be routed to the same Access Point appliance to which the primary Horizon protocol was routed. Access Point can then authorize the secondary protocols based on the authenticated user session. An important security capability of Access Point is that Access Point only forwards traffic into the corporate data center if the traffic is on behalf of an authenticated user. If the secondary protocols is routed incorrectly to a different Access Point appliance than the primary protocol appliance, they are not authorized and are dropped in the DMZ. The connection fails. Incorrectly routing the secondary protocols is a common problem, if the load balancer is not configured correctly.

DMZ Design for Access Point with Multiple Network Interface Cards

Access Point is a layer 7 security appliance that is normally installed in a Demilitarized Zone (DMZ). Access Point is used to ensure that the only traffic entering the corporate data center is traffic on behalf of a strongly authenticated remote user.

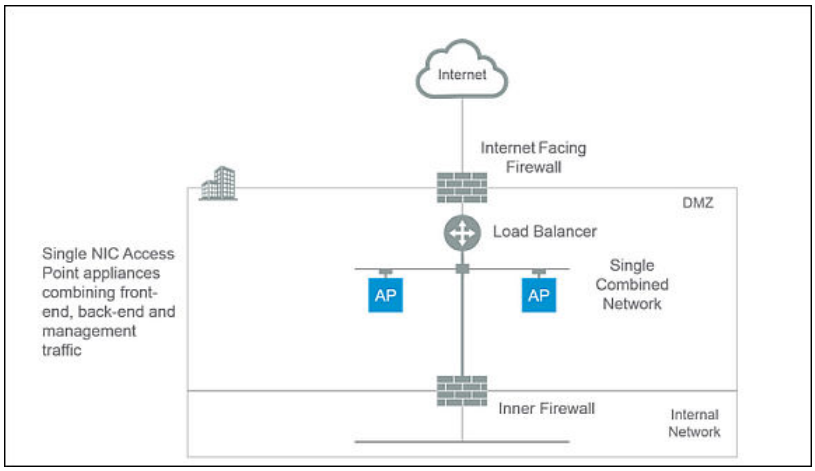
One of the configuration settings for Access Point is the number of virtual Network Interface Cards (NICs) to use. When you deploy Access Point, you select a deployment configuration for your network. You can specify one, two, or three NICS settings which is specified as onenic, twonic or threenic.

Reducing the number of open ports on each virtual LAN and separating out the different types of network traffic can significantly improve security. The benefits are mainly in terms of separating and isolating the different types of network traffic as part of a defense-in-depth DMZ security design strategy. This can be achieved either by implementing separate physical switches within the DMZ, with multiple virtual LANs within the DMZ, or as part of a full VMware NSX managed DMZ.

Typical Single NIC DMZ Deployment

The simplest deployment of Access Point is with a single NIC where all network traffic is combined onto a single network. Traffic from the Internet-facing firewall is directed to one of the available Access Point appliances. Access Point then forwards the authorized traffic through the inner firewall to resources on the internal network. Access Point discards unauthorized traffic.

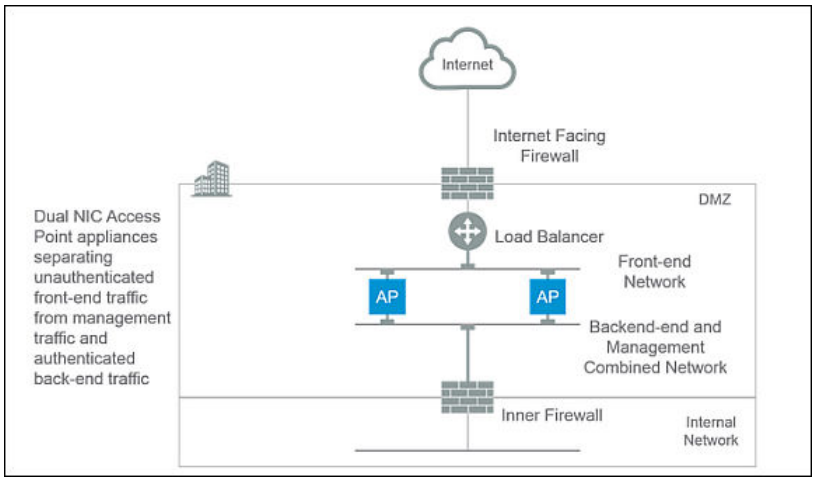
Figure 1-3. Access Point Single NIC Option



Separating Unauthenticated User Traffic from Back-End and Management Traffic

An improvement over the single NIC deployment is to specify two NICs. The first is still used for Internet facing unauthenticated access, but the back-end authenticated traffic and management traffic are separated onto a different network.

Figure 1-4. Access Point Two NIC Option



In a two NIC deployment, traffic going to the internal network through the inner firewall must be authorized by Access Point. Unauthorized traffic is not on this back-end network. Management traffic such as the REST API for Access Point is only on this second network

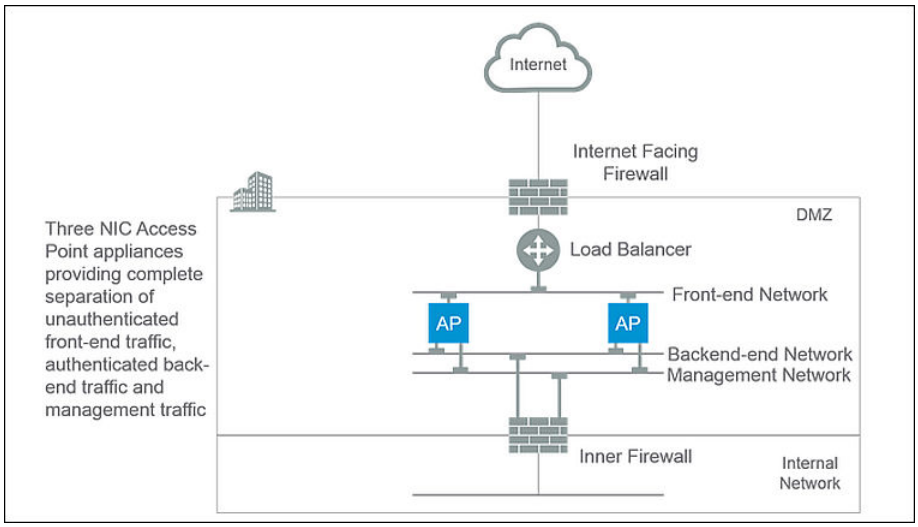
If a device on the unauthenticated front-end network was compromised, such as the load balancer, then reconfiguring that device to bypass Access Point is not possible in this two NIC deployment. It combines layer 4 firewall rules with layer 7 Access Point security. Similarly, if the Internet facing firewall was misconfigured to allow TCP port 9443 through, this would still not expose the Access Point Management REST API to Internet users. A defense-in-depth principle uses multiple levels of protection, such as knowing that a single configuration mistake or system attack does not necessarily create an overall vulnerability

In a two NIC deployment, it is common to put additional infrastructure systems such as DNS servers, RSA SecurID Authentication Manager servers on the back-end network within the DMZ so that these servers cannot be visible on the Internet facing network. Putting infrastructure systems within the DMZ guards against layer 2 attacks from the Internet facing LAN from a compromised front-end system and effectively reduces the overall attack surface.

Most Access Point network traffic is the display protocols for Blast and PCoIP. With a single NIC, display protocol traffic to and from the Internet is combined with traffic to and from the back-end systems. When two or more NICs are used, the traffic is spread across front-end and back-end NICs and networks. This reduces the potential bottleneck of a single NIC and results in performance benefits.

Access Point supports a further separation by also allowing separation of the management traffic onto a specific management LAN. HTTPS management traffic to port 9443 is then only possible from the management LAN.

Figure 1-5. Access Point Three NIC Option



Deploying Access Point Appliance

2

Access Point is packaged as an OVF and is deployed onto a vSphere ESX or ESXi host as a pre-configured virtual appliance.

Two primary methods can be used to install the Access Point appliance.

- The vSphere Client or vSphere Web Client can be used to deploy the Access Point OVF template. You are prompted for basic settings, including the NIC deployment configuration, IP address, and management interface passwords. After the OVF is deployed, log in to the Access Point admin user interface to configure Access Point system settings, set up secure edge services in multiple use cases, and configure authentication in the DMZ. See Deploy Access Point Using the OVF Template Wizard.
- PowerShell scripts can be used to deploy Access Point and set up secure edge services in multiple use cases. You download the zip file, configure the PowerShell script for your environment, and run the script to deploy Access Point. See Using PowerShell to Deploy the Access Point Appliance.

This section includes the following topics:

Using the OVF Template Wizard to Deploy Access Point

To deploy Access Point, you deploy the OVF template using the vSphere Client or vSphere Web Client, power on the appliance, and configure settings.

After the Access Point is deployed, you go to the administration user interface (UI) to set up the Access Point environment and configure the desktop and application resources and the authentication methods to use in the DMZ.

Access Point Deployment Properties

When you deploy the OVF, you configure how many network interfaces (NIC) are required, the IP address and set the administrator password. The other deployment properties can be set from the Access Point administration pages.

Table 2-1. Deployment Options Access Point

Deployment Property	Description
Deployment configuration	Specifies how many network interfaces are available in the Access Point virtual machine. By default, this property is not set, which means that one network interface controller (NIC) is used.
External (Internet-facing) 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	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	Specifies the IP address of the interface that is connected to the back-end network. If not configured, network traffic sent to the back-end systems is routed through the other network interfaces. Default: none.
DNS server addresses	(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	(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	(Required) If you do not set this password, you will not be able to access the administration console and REST API on the Access Point appliance. Passwords must be at least 8 characters long, contain at least one uppercase and one lowercase letter, one digit, and one special character, which includes ! @ # $ % * ( ). Default: none.

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

Deployment Property	Description
Locale to use for localized messages	(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	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.

Deploy Access Point Using the OVF Template Wizard

You can deploy the Access Point appliance by logging in to vCenter Server and using the Deploy OVF Template wizard.

Note If you use the vSphere Web Client to deploy the OVF, 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 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.

Prerequisites

- Familiarize yourself with the deployment options available in the wizard. See Access Point System and Network Requirements.
- Determine the number of network interfaces and static IP addresses to configure for the Access Point appliance. See Networking Configuration Requirements.
- 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.

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 data center, 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. Review the product details, version, and size requirements.

4 Follow the wizard prompts, and take the following guidelines into consideration as you complete 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 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 access the administration console and 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,

Option	Description
	All other settings are either optional or already have a default setting entered. Note the password requirements listed on the wizard page. For a description of all deployment properties, see Access Point Deployment Properties.

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 can 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 see the Web page provided by the server that Access Point is pointing to. 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

Log in to the Access Point admin user interface (UI) and configure the desktop and application resources to allow remote access from the Internet through Access Point and the authentication methods to use in the DMZ. The administration console URL is in the format `https://<mycoAccessPointappliance.com:9443/admin/index.html`.

Configuring Access Point From the Admin Configuration Pages

After you deploy the OVF and the Access Point appliance is powered on, log in to the Access Point admin User Interface to configure the following settings.

- Access Point system configuration and SSL server certificate.
- Edge service settings for Horizon, Reverse Proxy, Per App Tunnel and Proxy Settings for AirWatch.
- Authentication settings for RSA SecurID, RADIUS, X.509 Certificate, and RSA Adaptive Authentication.
- SAML identity provider and service provider settings.

The following options can be accessed from the configuration pages.

- Download Access Point log zip files.

- Export Access Point settings to retrieve the configuration settings.
- Import Access Point settings to create and update an entire Access Point configuration.

Configure Access Point System Settings

You can configure the security protocols and cryptographic algorithms that are used to encrypt communications between clients and the Access Point appliance from the admin configuration pages.

Prerequisites

- Review the Access Point Deployment Properties. The following settings information is required
  - Static IP address for the Access Point appliance
  - IP Address of the DNS server
  - Password for the administration console
  - URL of the server instance or load balancer that the Access Point appliance points to
  - Syslog server URL to save the event log files

Procedure

1. In the admin UI Configure Manual section, click **Select**.
2. In the Advanced Settings section, click the **System Configuration** gearbox icon.
3. Edit the following Access Point appliance configuration values.

Option	Default Value and Description
Locale	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
Admin Password	This password was set when you deployed the appliance. You can reset it. 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 ! @ # $ % * ( ).
Cipher Suites	Most cases, the default settings do not need to be changed. This is the cryptographic algorithms that are used to encrypt communications between clients and the Access Point appliance. Cipher settings are used for enabling various security protocols.
Honor Cipher Order	Default is NO. Select **YES** to enable TLS cipher list order control.
SSL 3.0 Enabled	Default is NO. Select **YES** to enable SSL 3.0 security protocol.
TLS 1.0 Enabled	Default is NO. Select **YES** to enable TLS 1.0 security protocol.
TLS 1.1 Enabled	Default is YES. The TLS 1.1 security protocol is enabled.

Option	Default Value and Description
TLS 1.2 Enabled	Default is YES. The TLS 1.2 security protocol is enabled.
Syslog URL	Enter the Syslog server URL that is used for logging Access Point events. This value can be a URL or a host name or IP address. If you do not set the syslog server URL, no events are logged. Enter as `syslog://server.example.com:514`.
Health Check URL	Enter a URL that the load balancer connects to and checks the health of Access Point.
Cookies to be Cached	The set of cookies that Access Point caches. The default is none.
IP Mode	Select the static IP mode, either STATICV4 OR STATICV6.
Session Timeout	Default value is **36000000** milliseconds.
Quiesce Mode	Enable **YES** to pause the Access Point appliance to achieve a consistent state to perform maintenance tasks
Monitor Interval	Default value is **60**.

4 Click **Save**.

What to do next

Configure the edge service settings for the components that Access Point is deployed with. After the edge settings are configured, configure the authentication settings.

Update SSL Server Signed Certificates

You can replace your signed certificates when they expire.

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.

Prerequisites

- New signed certificate and private key saved to a computer that you can access
- Convert the certificate to PEM-format files and convert the .pem to one-line format. See Convert Certificate Files to One-Line PEM Format.

Procedure

1 In the administration console, click **Select**.

2 In the Advanced Settings section, click the SSL Server Certificate Settings gearbox icon.

3 In the Private Key row, click **Select** and browse to the private key file.

4 Click **Open** to upload the file.

5 In the Certificate Chain row, click Select and browse to the certificate chain file.

6 Click **Open** to upload the file.

7 Click **Save**.

What to do next

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

Using PowerShell to Deploy Access Point

3

A PowerShell script can be used to deploy Access Point. The PowerShell script is delivered as a sample script that you can adapt to your environment specific needs.

When you use the PowerShell script, to deployAccess Point, the script calls the OVF Tool command and validates the settings to automatically construct the correct command-line syntax. This method also allows advanced settings such as configuration of the TLS/SSL server certificate to be applied at deployment time.

This section includes the following topics:

System Requirements to Deploy Access Point Using PowerShell

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

- vSphere ESX host with a vCenter Server.
- 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.
- 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/.

You must select the vSphere datastore and the network to use.

A vSphere Network Protocol Profile must be associated with every referenced network name. This 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.

Using PowerShell to Deploy the Access Point Appliance

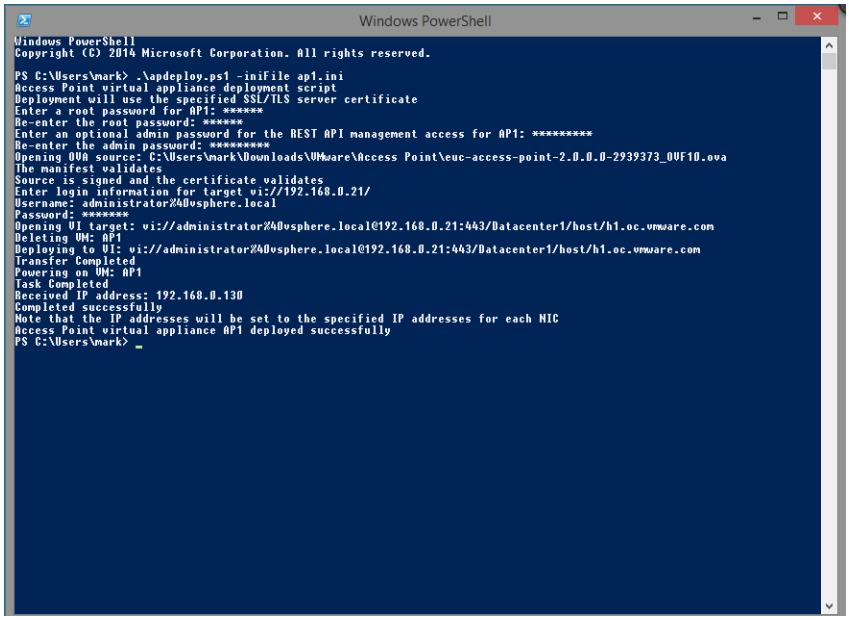
PowerShell scripts prepare you environment with all the configuration settings. When you run the PowerShell script to deploy Access Point, the solution is ready for production on first system boot.

Prerequisites

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

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

  Figure 3-1. Sample PowerShell Script



Procedure

1. Download the Access Point OVA from My VMware to your Windows machine.
2. Download the ap-deploy-XXX.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 can use the sample .INI files in the apdeploy .ZIP file to create the .INI file and modify the settings appropriately.

   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.

Example of the .INI File to modify.

```
name=AP1
source=C:\APs\euc-access-point-2.8.0.0-000000000_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]
```

5 To make sure that the script execution is successful, type the PowerShell set-executionpolicy command.

```
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.

Deployment Use Cases

4

The deployment scenarios described in this chapter can help you identify and organize the Access Point deployment in your environment.

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

This section 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). Deploying in the DMZ 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 entitled. This level of protection involves specific inspection of desktop protocols and coordination of potentially rapid changing policies and network addresses, to accurately control access.

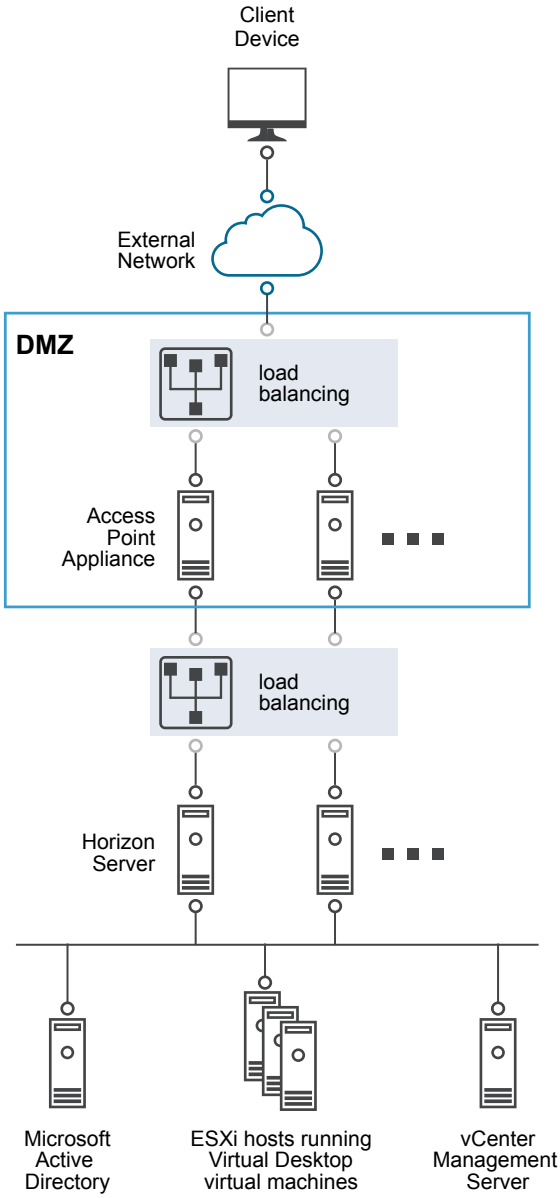
You must verify the requirements for seamless Access Point deployment with Horizon.

- 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.
- Disable the secure gateways on View Connection Server instances and enable these gateways on the Access Point appliances.

The main difference from View security server is that Access Point is as follows.

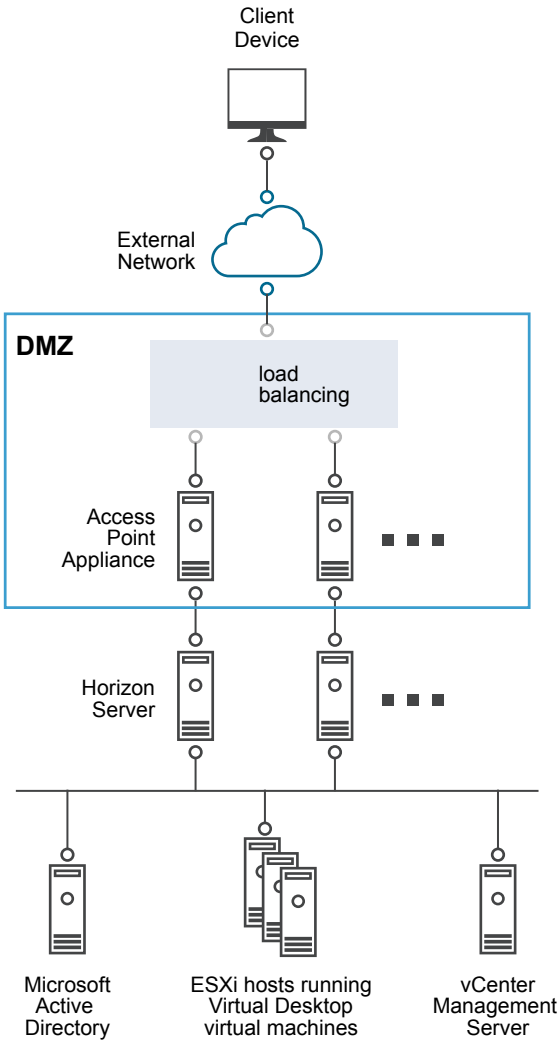
- Secure deployment. Access Point is implemented as a hardened, locked-down, preconfigured Linux-based virtual machine
- Scalable. You can connect Access Point to an individual View Connection Server, or you can connect it through a load balancer in front of multiple View Connection Servers, giving improved high availability. It acts as a layer between Horizon Clients and back end View Connection Servers. As the deployment is fast, it can rapidly scale up or down to meet the demands of fast-changing enterprises.

Figure 4-1. Access Point Appliance Pointing to a Load Balancer



Alternatively you can have one or more Access Point appliances pointing 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 4-2. 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 the following.

- Active Directory user name and password
- Kiosk mode. For details about Kiosk mode, see the Horizon documentation.
- RSA SecurID two-factor authentication, formally certified by RSA for SecurID
- 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 is not required to communicate directly with Active Directory. This communication serves as a proxy through the View Connection Server, which can directly access Active Directory. After the user session is authenticated according to the authentication policy, Access Point can forward requests for entitlement information, and desktop and application launch requests, to the View Connection Server. Access Point 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.

Configure Horizon Settings

You can deploy Access Point from Horizon View and Horizon Air Hybrid-Mode. For the View component of VMware Horizon, the Access Point appliance fulfills the same role that was previously played by the View security server.

Procedure

1. In the admin UI Configure Manually section, click **Select**.
2. In the General Settings > Edge Service Settings line, click **Show**.
3. Click the **Horizon Settings** gearbox icon.
4. In the Horizon Settings page, change NO to **YES** to enable Horizon
5. Configure the following edge service settings resources for Horizon

Option	Description
Identifier	Set by default to View. Access Point can communicate with servers that use the View XML protocol, such as View Connection Server, Horizon Air, and Horizon Air Hybrid-mode.
Connection Server URL	Enter the address of the Horizon server or load balancer. Enter as https://00.00.00.00
Proxy Destination URL Thumb Prints	Enter the list of Horizon server thumbprints. If you do not provide a comma-separated list of thumbprints, the server certificates must be issued by a trusted CA. Enter the hexadecimal thumpbrint digits. For example, type C3:89:A2:19:DC:7A:48:2B:85:1C:81:EC:5E:8F:6A:3C:33:F2:95:C3

6 To configure the authentication method rule, and other advanced settings, click **More**.

Option	Description
Auth Methods	Select the authentication methods to use. The default is to use pass-through authentication of the user name and password. The authentication methods you configured in Access Point are listed in the drop-down menus. To configure authentication that includes applying a second authentication method if the first authentication attempt fails. a Select one authentication method from the first drop-down menu. b Click the **+** and select either AND or OR. c Select the second authentication method from the third drop-down menu. To require users to authenticate through two authentication methods, change OR to AND in the drop-down.
Health Check URL	If a load balancer is configured, enter the URL that the load balancer uses to connect and check the health of the Access Point appliance.
SAML SP	Enter the name of the SAML service provider for the View XMLAPI broker. This name must either match the name of a configured service provider metadata or be the special value DEMO.
PCOIP Enabled	Change NO to **YES** to specifies whether the PCoIP Secure Gateway is enabled.
Proxy External URL	Enter the external URL of the Access Point appliance. Clients use this URL for secure connections through the PCoIP Secure Gateway. This connection is used for PCoIP traffic. The default is the Access Point IP address and port 4172.
Smart Card Hint Prompt	Change NO to **YES** to enable Access Point appliance to support the smart card user name hints feature. With the smart card hint feature, a user's smart card certificate can map to multiple Active directory domain user accounts.
Blast Enabled	To use the Blast Secure Gateway, change NO to **YES**.
Blast External URL	Enter the FQDN URL of the Access Point appliance that end users use to make a secure connection from the Web browsers through the Blast Secure Gateway. Enter as https://exampleappliance:443
Tunnel Enabled	If the View secure tunnel is used, change NO to **YES**. The Client uses the external URL for tunnel connections through the View Secure Gateway. The tunnel is used for RDP, USB, and multimedia redirection (MMR) traffic.
Tunnel External URL	Enter the external URL of the Access Point appliance. The default Access Point default value is used if not set.
Match Windows User Name	Change NO to **YES** to match RSA SecurID and Windows user name. When set to YES, securID-auth is set to true and the securID and Windows user name matching is enforced.
Gateway Location	Change NO to **YES** to enable the location from where the requests originate. The security server and Access Point set the gateway location. The location can be external or internal.
Windows SSO Enabled	Change NO to **YES** to enable RADIUS authentication. The Windows log in uses the credentials that are used the first successful RADIUS access request.

7 Click **Save**.

Access Point Deployment as Reverse Proxy

Access Point can be used as a Web reverse proxy and can act as either a plain reverse proxy or an authenticating reverse proxy in the DMZ.

Deployment Scenario

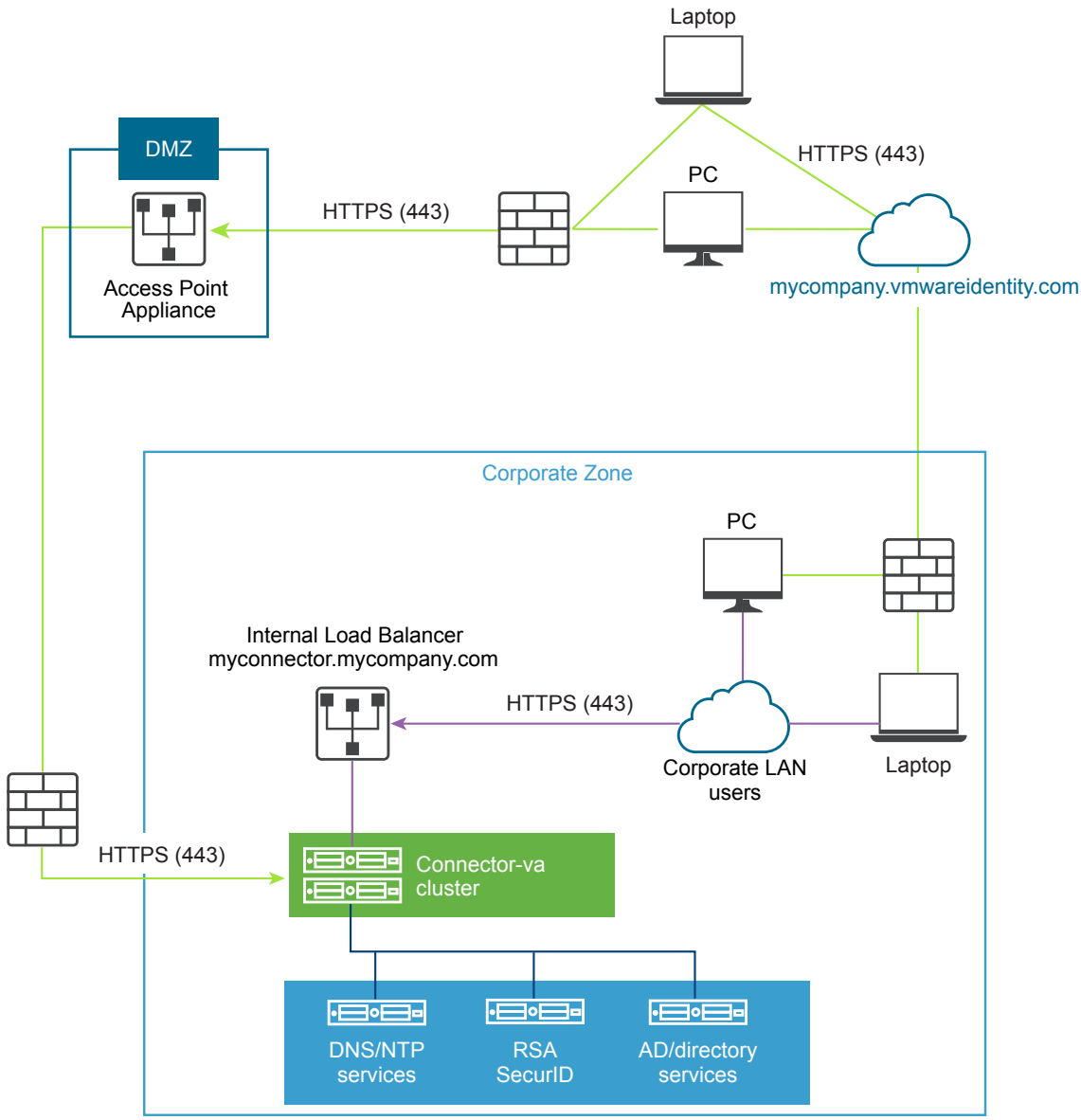
Access Point provides secure remote access to an on-premises deployment of VMware Identity Manager. Access Point appliances are typically deployed in a network demilitarized zone (DMZ). With VMware Identity Manager, the Access Point appliance operates as a Web reverse proxy between a user's browser and the VMware Identity Manager service in the data center. Access Point also enables remote access to the VMware Identity Manager catalog to launch Horizon applications.

Requirements for Access Point deployment with VMware Identity Manager

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

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

Figure 4-3. Access Point Appliance Pointing the Connector



Understanding Reverse Proxy

Access Point as a solution provides access to the app portal for remote users to single-sign-on and access their resources. You enable Authn reverse proxy on an edge service Manager. Currently, RSA SecurID and RADIUS authentication methods are supported.

Note You must generate the identity provider metadata before enabling authentication on Web reverse proxy.

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

- Browers-based clients are supported using RADIUS and RSA SecurID as the authentication methods.

Reverse proxy support is limited with Access Point 2.8 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.

Configure Reverse Proxy for VMware Identity Manager

You can configure Web Reverse Proxy service to use Access Point with VMware Identity Manager.

Prerequisites

Requirements for Access Point deployment with VMware Identity manager.

- Split DNS
- VMware Identity Manager service must have fully qualified domain name (FQDN) as hostname.
- Access Point must use internal DNS. This means that the proxyDestination URL must use FQDN.

Procedure

1. In the admin UI Configure Manually section, click **Select**.
2. In the General Settings > Edge Service Settings line, click **Show**.
3. Click the **Reverse Proxy Settings** gearbox icon.
4. In the Reverse Proxy Settings page, change NO to **YES** to enable reverse proxy.
5. Configure the following edge service settings resources for Horizon.

Option	Description
Identifier	The edge service identifier is set to WEB_REVERSE_PROXY.
Proxy Destination URL	Enter the address of the VMware Identity Manager server. For example, enter as **`https://vmwareidentitymgr.example.com`**.
Proxy Destination URL Thumbprints	Enter a comma-separated list of acceptable SSL server certificate thumbprints for the proxyDestination Url. If you include the wildcard *, any certificate is allowed. This is a colon-separated list of thumbprints. A thumbprint is in the format [alg=]xx:xx, where alg can be sha1, the default or md5. The 'xx' are hexicdecimal digits. For example, sha=C3:89:A2:19:DC:7A:48:2B:85:1C:81:EC:5E:8F:6A:3C:33:F2:95:C3 If you do not configure the thumbprints, the server certificates must be issued by a trusted CA.
Proxy Pattern	Enter the matching URI paths that forward to the destination URL. For example, enter as **`(/|/SAAS(.*)|/hc(.*)|/web(.*)|/catalog-portal(.*))`**.

6 To configure other advanced settings, click **More**.

Option	Description
Auth Methods	The default is to use pass-through authentication of the user name and password. The authentication methods you configured in Access Point are listed in the drop-down menus. The authentication methods you configured in Access Point are listed in the drop-down menu.
Health Check URL	If a load balancer is configured, enter the URL that the load balancer uses to connect and check the health of the Access Point appliance.
SAML SP	`Enter the name of the SAML service provider for the WRONG WRONG WRONG tip`
Activation Code	Enter the code generated by VMware Identity Manager service and imported into Access Point to set up trust between VMware Identity Manager and Access Point.
External URL	

7 Click **Save**.

Access Point Deployment with AirWatch Tunnel

The Access Point appliance is deployed on the DMZ. Deployment involves installing the Access Point components and the AirWatch components such as Agent 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.

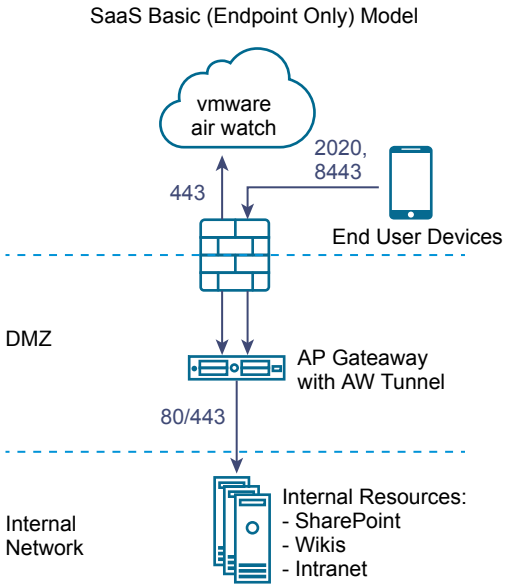
For more information on deploying Access Point with AirWatch, see https://resources.air-watch.com/view/vb7zp7wwhpw756m2pfxy .

Tunnel Proxy Deployment for AirWatch

The tunnel proxy deployment secures the network traffic between an end user device and a website through the VMware Browser mobile application from AirWatch.

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 4-4. Tunnel Proxy Deployment

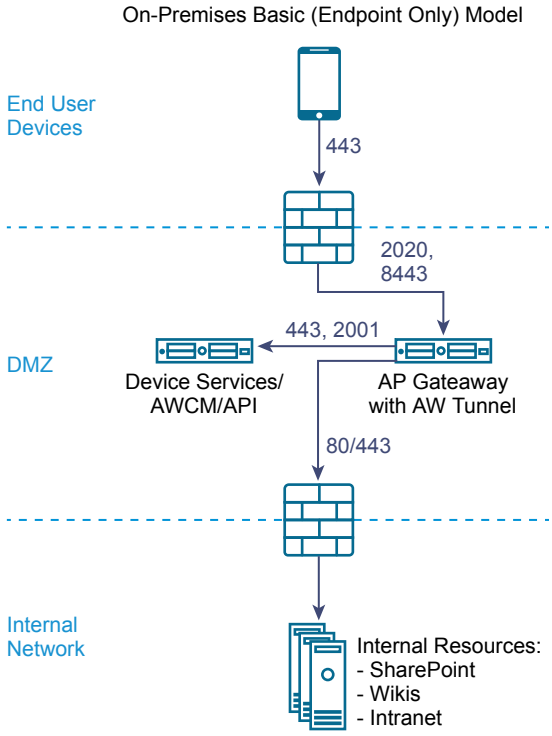


Per-App Tunnel Deployment with AirWatch

The Per-App 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 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 4-5. Per-App Tunnel Deployment



Configure Per-App Tunnel and Proxy Settings for AirWatch

Tunnel proxy deployment secures the network traffic between an end user device and a Website through the VMware Browser mobile application.

Procedure

1. In the admin UI Configure Manually section, click **Select**.
2. In the General Settings > Edge Service Settings line, click **Show**.
3. Click **Per App Tunnel and Proxy Settings** gearbox icon.
4. Change NO to **YES** to enable tunnel proxy.
5. Configure the following edge service settings resources.

Option	Description
Identifier	Set by default to View. Access Point can communicate with servers that use the View XML protocol, such as View Connection Server, Horizon Air, and Horizon Air Hybrid-mode.
API Server URL	Enter the AirWatch API server URL. For example, enter as https://example.com:<port>.
API Server User Name	Enter the user name to log in to the API server.
API Server Password	Enter the password to log in to the API server.

Option	Description
Organization Group Code	Enter the organization of the user.
AirWatch Server Hostname	Enter the AirWatch server host name.

6 To configure other advanced settings, click **More**.

Option	Description
AirWatch Outbound Proxy	Change NO to **YES** to initialize the Tunnel Proxy service.
Outbound Proxy HOST	Enter the host name where the outbound proxy is installed. **Note** This is not the Tunnel Proxy.
Outbound Proxy PORT	Enter the port number of the outbound proxy.
Outbound Proxy User Name	Enter the user name to log in to the outbound proxy.
Outbound Proxy Password	Enter the password to log in to the outbound proxy.
NTLM Authentication	Change NO to **YES** to specify that the outbound proxy request requires NTLM authentication.
Use for AirWatch Tunnel Proxy	Change NO to **YES** to use this proxy as an outbound proxy for AirWatch Tunnel. If not enabled, Access Point uses this proxy for the initial API call to get the configuration from the AirWatch admin console.

7 Click **Save**.

Configuring Access Point Using TLS/SSL Certificates

5

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

Note Configuring the TLS/SSL certificates for theAccess Point appliance 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 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. For smart card certificates, see Configuring Certificate or Smart Card Authentication on the Access Point Appliance.

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.
- 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`.

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

6

When you initially deploy VMware Access Point, Active Directory password authentication is set up as the default. Users enter their Active Directory user name and password and these credentials are sent through to a back-end system for authentication.

You can configure the Access Point service to perform Certificate/Smart Card authentication, RSA SecurID authentication, RADIUS authentication, and RSA Adaptive Authentication.

Note Password authentication with Active Directory is the only authentication method that can be used with an AirWatch deployment.

This section includes the following topics:

Configuring Certificate or Smart Card Authentication on the Access Point Appliance

You can configure x509 certificate authentication in Access Point to allow clients to authenticate with certificates on their desktop or mobile devices or to use a smart card adapter for authentication.

Certificate-based authentication is based on what the user has (the private key or smart card), and what the person knows (the password to the private key or the smart card 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 to access 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 the Access Point service. Access Point uses a SAML assertion to communicate information about the end user's X.509 certificate and the smart card PIN to the Horizon server.

You can configure certificate revocation checking to prevent users who have their user certificates revoked from authenticating. Certificates are often revoked when a user leaves an organization, loses a smart card, or moves from one department to another. Certificate revocation checking with certificate revocation lists (CRLs) and with the Online Certificate Status Protocol (OCSP) is supported. 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 a certificate.

You can configure both CRL and OCSP in the same certificate authentication adapter configuration. When you configure both types of certificate revocation checking and the Use CRL in case of OCSP failure check box is enabled, OCSP is checked first and if OCSP fails, revocation checking falls back to CRL. Revocation checking does not fall back to OCSP if CRL fails.

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.

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

Configure Certificate Authentication on Access Point

You enable and configure certificate authentication from the Access Point administration console.

Prerequisites

- Obtain the root certificate and intermediate certificates from the CA that signed the certificates presented by your users. See Obtain the Certificate Authority Certificates
- Verify that the Access Point SAML metadata is added on the service provider and the service provider SAML metadata is copied the Access Point appliance.
- (Optional) List of Object Identifier (OID) of valid certificate policies for certificate authentication.
- For revocation checking, the file location of the CRL and the URL of the OCSP server.
- (Optional) OCSP Response Signing certificate file location.
- Consent form content, if a consent form displays before authentication.

Procedure

1. In the admin UI Configure Manually section, click **Select**.
2. In the General Settings Authentication Settings section, click **Show**.
3. Click the gearbox in the X.509 Certificate line.

4 Configure the X.509 Certificate form.

An asterisk indicates a required text box. All other text boxes are optional.

Option	Description
Enable X.509 Certificate	Change NO to **YES** to enable certificate authentication.
***Name**	Name this authentication method.
***Root and Intermediate CA Certificates**	Click **Select** to select the certificate files to upload. You can select multiple root CA and intermediate CA certificates that are encoded as DER or PEM.
CRL Cache Size	Enter the certificate revocation list cache size. The default is 100
Enable Cert Revocation	Change NO to **YES** to enable certificate revocation checking. Revocation checking prevents users who have revoked user certificates from authenticating.
Use CRL from Certificates	Select the check box to use the certificate revocation list (CRL) published by the CA that issued the certificates to validate the status of a certificate, revoked or not revoked.
CRL Location	Enter the server file path or the local file path from which to retrieve the CRL.
Enable OCSP Revocation	Select the check box to use the Online Certificate Status Protocol (OCSP) certificate validation protocol to get the revocation status of a certificate.
Use CRL in case of OCSP Failure	If you configure both CRL and OCSP, you can select this box to fall back to using CRL if OCSP checking is not available.
Send OCSP Nonce	Select this check box if you want the unique identifier of the OCSP request to be sent in the response.
OCSP URL	If you enabled OCSP revocation, enter the OCSP server address for revocation checking.
OCSP Responder's Signing Certificate	Enter the path to the OCSP certificate for the responder, */path/to/file.cer*.
Enable Consent Form before Authentication	Select this check box to include a consent form page to appear before users log in to their Workspace ONE portal using certificate authentication.
Consent Form Content	Type the text here that displays in the consent form.

5 Click **Save**.

What to do next

When X.509 Certificate authentication is configured and Access Point appliance is set up behind a load balancer, make sure that Access Point is configured with SSL pass-through at the load balancer and not configured to terminate SSL at the load balancer. This configuration ensures that the SSL handshake is between the Access Point and the client in order to pass the certificate to Access Point.

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.

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 RSA SecurID Authentication in Access Point

After the Access Point appliance is configured as the authentication agent in the RSA SecurID server, you must add the RSA SecurID configuration information to the Access Point appliance.

Prerequisites

- Verify that RSA Authentication Manager (the RSA SecurID server) is installed and properly configured.
- Download the compressed sdconf.rec file from the RSA SEcurID server and extract the server configuration file.

Procedure

1. In the admin UI Configure Manually section, click **Select**.
2. In the General Settings Authentication Settings section, click **Show**.
3. Click the gearbox in the RSA SecurID line.
4. Configure the RSA SecurID page.

   Information used and files generated on the RSA SecurID server are required when you configure the SecurID page.

Option	Action
Enable RSA SecurID	Change NO to **YES** to enable SecurID authentication.
*Name	The name is securid-auth.
*Number of Iterations	Enter the number of authentication attempts that are allowed. This is the maximum number of failed login attempts when using the RSA SecurID token. The default is 5 attempts. **Note** When more than one directory is configured and you implement RSA SecurID authentication with additional directories, configure **Number of authentication attempts allowed** with the same value for each RSA SecurID configuration. If the value is not the same, SecurID authentication fails.
*External HOST Name	Enter the IP address of the Access Point instance. The value you enter must match the value you used when you added the Access Point appliance as an authentication agent to the RSA SecurID server.
*Internal HOST Name	Enter the value assigned to the **IP address** prompt in the RSA SecurID server.
*Server Configuration	Click Change to upload the RSA SecurID server configuration file. First, you must download the compressed file from the RSA SecurID server and extract the server configuration file, which by default is named `sdconf.rec`.
*Name Id Suffix	Enter the nameId that enables View to provide TrueSSO experience.

Configuring RADIUS fo Access Point

You can configure Access Point so that users are required to use RADIUS authentication. You configure the RADIUS server information on the Access Point appliance.

RADIUS support offers a wide range of alternative two-factor token-based authentication options. Because two-factor authentication solutions, such as RADIUS, work with authentication managers installed on separate servers, you must have the RADIUS server configured and accessible to the identity manager service

When users sign in and RADIUS authentication is enabled, a special login dialog box appears in the browser. Users enter their RADIUS authentication user name and passcode in the login dialog box. If the RADIUS server issues an access challenge, Access Point displays a dialog box prompting for a second passcode. Currently support for RADIUS challenges is limited to prompting for text input.

After a user enters credentials in the dialog box, the RADIUS server can send an SMS text message or email, or text using some other out-of-band mechanism to the user's cell phone with a code. The user can enter this text and code into the login dialog box to complete the authentication.

If the RADIUS server provides the ability to import users from Active Directory, end users might first be prompted to supply Active Directory credentials before being prompted for a RADIUS authentication username and passcode.

Configure RADIUS Authentication

On the Access Point appliance, you must enable RADIUS authentication, enter the 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. Set up the RADIUS server and then configure the RADIUS requests from Access Point. Refer to your RADIUS vendor's setup guides for information about setting up the RADIUS server.

The following RADIUS server information is required.

- IP address or DNS name of the RADIUS server.
- Authentication port numbers. Authentication port is usually 1812.
- Authentication type. The authentication types include PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), MSCHAP1, MSCHAP2 (Microsoft Challenge Handshake Authentication Protocol, versions 1 and 2).
- RADIUS shared secret that is used for encryption and decryption in RADIUS protocol messages.
- Specific timeout and retry values needed for RADIUS authentication

Procedure

1. In the admin UI Configure Manually section, click **Select**.

2 In the General Settings Authenticating Settings section, click **Show**.

3 Click the gearbox in the RADIUS line.

Option	Action
Enable RADIUS	Change NO to **YES** to enable RADIUS authentication.
Name*	The name is radius-auth
Authentication type*	Enter the authentication protocol that is supported by the RADIUS server. Either PAP, CHAP, MSCHAP1, OR MSCHAP2.
Shared secret*	Enter the RADIUS shared secret.
Number of Authentication attempts allowed *	Enter the maximum number of failed login attempts when using RADIUS to log in. The default is three attempts.
Number of attempts to RADIUS server*	Enter the total number of retry attempts. If the primary server does not respond, the service waits for the configured time before retrying again.
Server Timeout in Seconds*	Enter the RADIUS server timeout in seconds, after which a retry is sent if the RADIUS server does not respond.
Radius Server Host name *	Enter the host name or the IP address of the RADIUS server.
Authentication Port*	Enter the Radius authentication port number. The port is usually 1812.
Realm Prefix	(Optional) The user account location is called the realm. If you specify a realm prefix string, the string is placed at the beginning of the user name when the name is sent to the RADIUS server. For example, if the user name is entered as jdoe and the realm prefix DOMAIN-A\ is specified, the user name DOMAIN-A\jdoe is sent to the RADIUS server. If you do not configure these fields, only the user name that is entered is sent.
Realm Suffix	(Optional) If you configure a realm suffix, the string is placed at the end of the user name. For example, if the suffix is @myco.com, the user name jdoe@myco.com is sent to the RADIUS server.
Name iD Suffix	Enter the nameId that enables View to provide a True SSO experience.
Login page passphrase hint	Enter the text string to display in the message on the user login page to direct users to enter the correct Radius passcode. For example, if this field is configured with **AD password first and then SMS passcode**, the login page message would read **Enter your AD password first and then SMS passcode.** The default text string is **RADIUS Passcode**.
Enable secondary server	Change NO to **YES** to configure a secondary RADIUS server for high availability. Configure the secondary server information as described in step 3.

4 Click **Save**.

Configuring RSA Adaptive Authentication in Access Point

RSA Adaptive Authentication can be implemented to provide a stronger multi-factor authentication than only user name and password authentication against Active Directory. Adaptive Authentication monitors and authenticates user login attempts based on risk levels and policies.

When Adaptive Authentication is enabled, the risk indicators specified in the risk policies set up in the RSA Policy Management application and the Access Point configuration of adaptive authentication are used to determine whether a user is authenticated with user name and password or whether additional information is needed to authenticate the user.

Supported RSA Adaptive Authentication Methods of Authentication

The RSA Adaptive Authentication strong authentication methods supported in Access Point are out-of-band authentication via phone, email, or SMS text message and challenge questions. You enable on the service the methods of RSA Adaptive Auth that can be provided. RSA Adaptive Auth policies determine which secondary authentication method is used.

Out-of-band authentication is a process that requires sending additional verification along with the user name and password. When users enroll in the RSA Adaptive Authentication server, they provide an email address, a phone number, or both, depending on the server configuration. When additional verification is required, RSA adaptive authentication server sends a one-time passcode through the provided channel. Users enter that passcode along with their user name and password.

Challenge questions require the user to answer a series of questions when they enroll in the RSA Adaptive Authentication server. You can configure how many enrollment questions to ask and the number of challenge questions to present on the login page.

Enrolling Users with RSA Adaptive Authentication Server

Users must be provisioned in the RSA Adaptive Authentication database to use adaptive authentication for authentication. Users are added to the RSA Adaptive Authentication database when they log in the first time with their user name and password. Depending on how you configured RSA Adaptive Authentication in the service, when users log in, they can be asked to provide their email address, phone number, text messaging service number (SMS), or they might be asked to set up responses to challenge questions.

Note RSA Adaptive Authentication does not allow for international characters in user names. If you intend to allow multi-byte characters in the user names, contact RSA support to configure RSA Adaptive Authentication and RSA Authentication Manager.

Configure RSA Adaptive Authentication in Access Point

To configure RSA Adaptive Authentication on the service, you enable RSA Adaptive Authentication; select the adaptive authentication methods to apply, and add the Active Directory connection information and certificate.

Prerequisites

- RSA Adaptive Authentication correctly configured with the authentication methods to use for secondary authentication.
- Details about the SOAP endpoint address and the SOAP user name.
- Active Directory configuration information and the Active Directory SSL certificate available.

Procedure

1. In the admin UI Configure Manually section, click **Select**.
2. In the General Settings Authentication Settings section, click **Show**.
3. Click the gearbox in the RSA Adaptive Authentication line.
4. Select the appropriate settings for your environment.

Note An asterisk indicates a required field. The other fields are optional.

Option	Description
Enable RSA AA Adapter	Change NO to **YES** to enable RSA Adaptive Authentication.
Name*	The name is rsaaa-auth.
SOAP Endpoint*	Enter the SOAP endpoint address for integration between the RSA Adaptive Authentication adapter and the service.
SOAP Username*	Enter the user name and password that is used to sign SOAP messages.
SOAP Password*	Enter the RSA Adaptive Authentication SOAP API password.
RSA Domain	Enter the domain address of the Adaptive Authentication server.
Enable OOB Email	Select YES to enable out-of-band authentication that sends a onetime passcode to the end user by way of an email message.
Enable OOB SMS	Select YES to enable out-of-band authentication that sends a onetime passcode to the end user by way of a SMS text message.
Enable SecurID	Select YES to enable SecurID. Users are asked to enter their RSA token and passcode.
Enable Secret Question	Select YES if you are going to use enrollment and challenge questions for authentication.
Number Enrollment Questions*	Enter the number of questions the user will need to setup when they enroll in the Authentication Adapter server.
Number Challenge Questions*	Enter the number of challenge questions users must answer correctly to login.
Number of authentication attempts allowed*	Enter the number of times to display challenge questions to a user trying to log in before authentication fails.
Type of Directory*	The only directory supported is Active Directory.

Option	Description
Use SSL	Select YES if you use SSL for your directory connection. You add the Active Directory SSL certificate in the Directory Certificate field.
Server Host*	Enter the Active Directory host name.
Server Port	Enter the Active Directory port number.
Use DNS Service Location	Select YES if DNS service location is used for directory connection.
Base DN	Enter the DN from which to start account searches. For example, OU=myUnit,DC=myCorp,DC=com.
Bind DN*	Enter the account that can search for users. For example , CN=binduser,OU=myUnit,DC=myCorp,DC=com
Bind Password	Enter the password for the Bind DN account.
Search Attribute	Enter the account attribute that contains the username.
Directory certificate	To establish secure SSL connections, add the directory server certificate to the text box. In the case of multiple servers, add the root certificate of the certificate authority.
Use STARTTLS	Change NO to **YES** to use STARTTLS.

5 Click **Save**.

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.

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. 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 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.

Procedure

1. In the admin UI Configure Manually section, click **Select**.
2. In the Advanced Settings section, click the **SAML Identity Provider Settings** gearbox icon.
3. Select the **Provide Certificate** check box.
4. To add the Private Key file, click **Select** and browse to the private key file for the certificate.
5. For add the Certificate Chain file, click **Select** and browse to the certificate chain file.
6. Click **Save**.
7. In the Hostname text box, enter the hostname and download the identity provider settings.

Creating a SAML Authenticator Used by Other Service Providers

After you generate the 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. In the Access Point admin UI Configure Manually section, click **Select**.

3 In the Advanced Settings section, click the **SAML Server Provider Settings** gearbox icon.

4 In the Service Provider Name text box, enter the service provider name.

5 In the Metadata XML text box, paste the metadata file you created in step 1.

6 Click **Save**.

Access Point and the service provider can now exchange authentication and authorization information.

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 section includes the following topics:

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
   ```