Deploying and Configuring VMware Unified Access Gateway

Unified Access Gateway 3.1

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 Unified Access Gateway

Deploying and Configuring Unified Access Gateway provides information about designing VMware Horizon®, VMware Identity Manager™, and VMware AirWatch® deployment that uses VMware Unified Access Gateway™ 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 Unified Access Gateway virtual appliances and changing the configuration settings after deployment.

Intended Audience

This information is intended for anyone who wants to deploy and use Unified Access Gateway 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 VMware Unified Access Gateway

1

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

Note VMware Unified Access Gateway® was formerly named VMware Access Point.

This chapter includes the following topics:

Unified Access Gateway as a Secure Gateway

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

Unified Access Gateway directs authentication requests to the appropriate server and discards any unauthenticated request. Users can access only the resources that they are authorized to access.

Unified Access Gateway 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.

Unified Access Gateway acts 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.

Unified Access Gateway is designed specifically for the 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 Unified Access Gateway Instead of a Virtual Private Network

Unified Access Gateway 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.

Unified Access Gateway advantages over generic VPN include the following.

- Access Control Manager. Unified Access Gateway applies access rules automatically. Unified Access Gateway recognizes the entitlements of the users and the addressing required to connect internally. 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. Unified Access Gateway does not alter the straightforward Horizon Client user interface. With Unified Access Gateway, 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. Unified Access Gateway is designed to maximize security and performance. With Unified Access Gateway, 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, is considered secure, but the underlying protocol with SSL/TLS is just TCP-based. With modern video remoting protocols exploiting connectionless UDP-based transports, the performance benefits can be significantly eroded when forced over a TCP-based transport. This does not apply to all VPN technologies, as those that can also operate with DTLS or IPsec instead of SSL/TLS can work well with View desktop protocols.

Unified Access Gateway System and Network Requirements

To deploy the Unified Access Gateway 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 Unified Access Gateway. 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.

Hardware Requirements for ESXi Server

The Unified Access Gateway appliance must be deployed on a version of vSphere that is the same as a version supported for the VMware 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 exit the wizard.

Note Configure the clock (UTC) on the Unified Access Gateway appliance so that the appliance has the correct time. For example, open a console window on the Unified Access Gateway 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 ESXi host.

Virtual Appliance Requirements

The OVF package for the Unified Access Gateway appliance automatically selects the virtual machine configuration that the Unified Access Gateway 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.

- CPU minimum requirement is 2000 MHz
- Minimum memory of 4GB

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

- Virtual appliance download size is 1.4 GB
- Thin-provisioned disk minimum requirement is 2.6 GB
- Thick-provisioned disk minimum requirement is 20 GB

The following information is required to deploy the virtual appliance.

- Static IP address (recommended)
- IP address of the DNS server
- Password for the root user
- Password for the admin user

- URL of the server instance of the load balancer that the Unified Access Gateway appliance points to

Browser Versions Supported

Supported browsers for launching the Admin UI are Chrome, Firefox, and Internet Explorer. Please use the most current version of the browser.

Hardware Requirements When Using Windows Hyper-V Server

When you use Unified Access Gateway for an AirWatch Per-App Tunnel deployment, you can install the Unified Access Gateway appliance on a Microsoft Hyper-V server.

Supported Microsoft servers are Windows Server 2012 R2 and Windows Server 2016.

Networking Configuration Requirements

You can use one, two, or three network interfaces and Unified Access Gateway requires a separate static IP address for each. Many DMZ implementations use separated networks to secure the different traffic types. Configure Unified Access Gateway 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 is 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 Unified Access Gateway 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.

If Unified Access Gateway is deployed without IP Pools (vCenter Server), the deployment is successful, but when you try to access Unified Access Gateway using the Admin UI from the browser, the Admin UI service does not launch.

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

Firewall Rules for DMZ-Based Unified Access Gateway Appliances

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

A DMZ-based Unified Access Gateway 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 service, which greatly reduces the risk of compromising your internal network.

To allow external client devices to connect to a Unified Access Gateway 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 a Unified Access Gateway appliance within the DMZ on TCP port 443. If you use the Blast protocol, port 8443 must be open on the firewall, but you can configure Blast for port 443 as well.

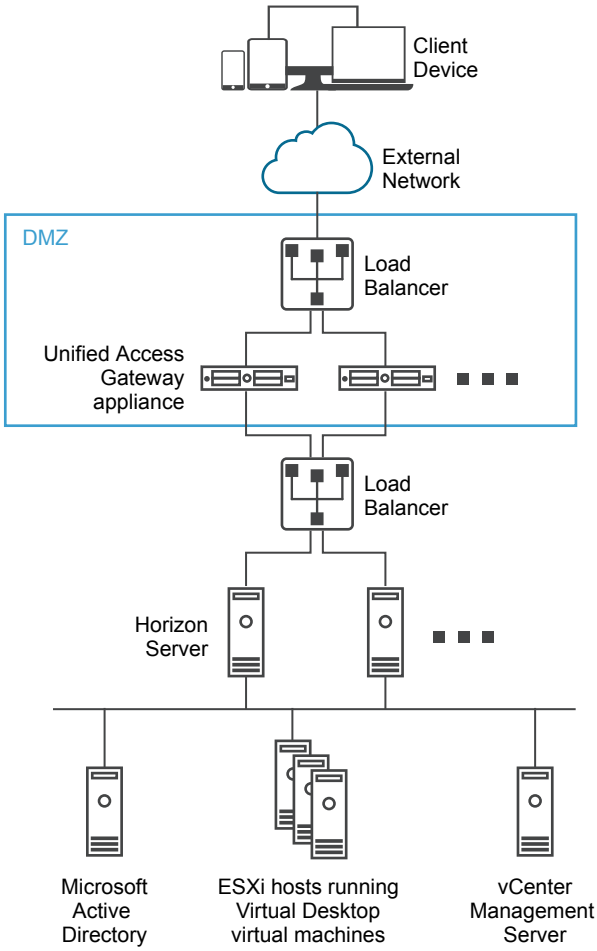
Table 1-1. Port Requirements

Port	Portal	Source	Target	Description
443	TCP	Internet	Unified Access Gateway	For Web traffic, Horizon Client XML - API, Horizon Tunnel, and Blast Extreme
443	UDP	Internet	Unified Access Gateway	UDP (optional)
8443	UDP	Internet	Unified Access Gateway	Blast Extreme (optional)
8443	TCP	Internet	Unified Access Gateway	Blast Extreme (optional)
4172	TCP and UDP	Internet	Unified Access Gateway	PCoIP (optional)
443	TCP	Unified Access Gateway	Horizon Broker	Horizon Client XML-API
22443	TCP and UDP	Unified Access Gateway	Desktops and RDS Hosts	Blast Extreme
4172	TCP and UDP	Unified Access Gateway	Desktops and RDS Hosts	PCoIP (optional)
32111	TCP	Unified Access Gateway	Desktops and RDS Hosts	Framework channel for USB Redirection
9427	TCP	Unified Access Gateway	Desktops and RDS Hosts	MMR and CDR
9443	TCP	Admin UI	Unified Access Gateway	Management interface

Note All UDP ports require forward datagrams and reply datagams to be allowed.

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

Figure 1-1. Unified Access Gateway In DMZ Topology



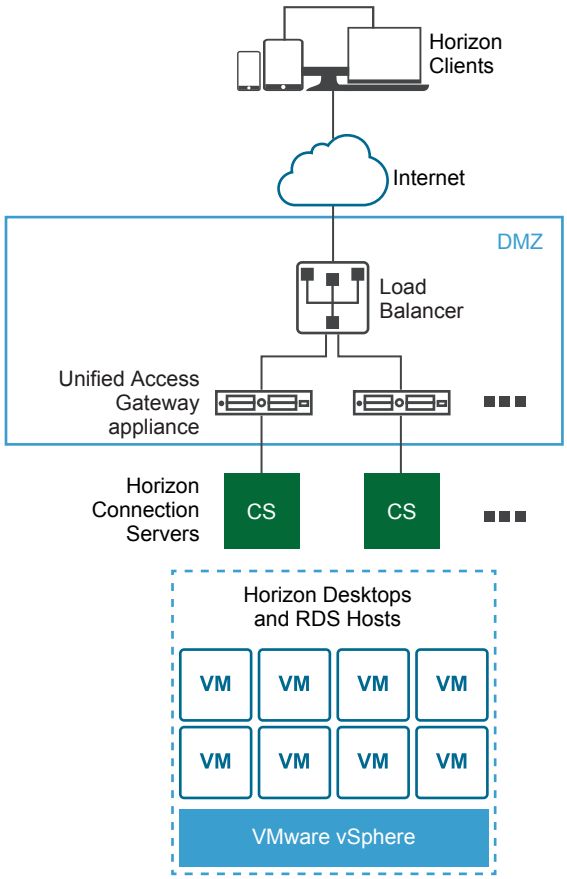
Unified Access Gateway Load Balancing Topologies

A Unified Access Gateway appliance in the DMZ can be configured to point to a server or a load balancer that fronts a group of servers. Unified Access Gateway appliances work with standard third-party load balancing solutions that are configured for HTTPS.

If the Unified Access Gateway 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 Unified Access Gateway, you can point the Unified Access Gateway appliance to this same load balancer that is often already being used.

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

Figure 1-2. Multiple Unified Access Gateway 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. The protocol uses XML structured messages over HTTPS. This protocol is sometimes known as the Horizon XML-API control protocol. In a load balanced environment as shown in the Multiple Unified Access Gateway Appliances Behind a Load Balancer figure, the load balancer routes this connection to one of the Unified Access Gateway 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 Unified Access Gateway appliances

- Secondary Horizon Protocols

After the Horizon Client establishes secure communication to one of the Unified Access Gateway 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, TCP 8443, UDP 443 and UDP 8443)
- PCoIP display protocol (TCP 443, UDP 443)

These secondary Horizon protocols must be routed to the same Unified Access Gateway appliance to which the primary Horizon protocol was routed. Unified Access Gateway can then authorize the secondary protocols based on the authenticated user session. An important security capability of Unified Access Gateway is that Unified Access Gateway only forwards traffic into the corporate data center if the traffic is on behalf of an authenticated user. If the secondary protocol is routed incorrectly to a different Unified Access Gateway appliance than the primary protocol appliance, users 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 Unified Access Gateway with Multiple Network Interface Cards

One of the configuration settings for Unified Access Gateway is the number of virtual Network Interface Cards (NICs) to use. When you deploy Unified Access Gateway, you select a deployment configuration for your network.

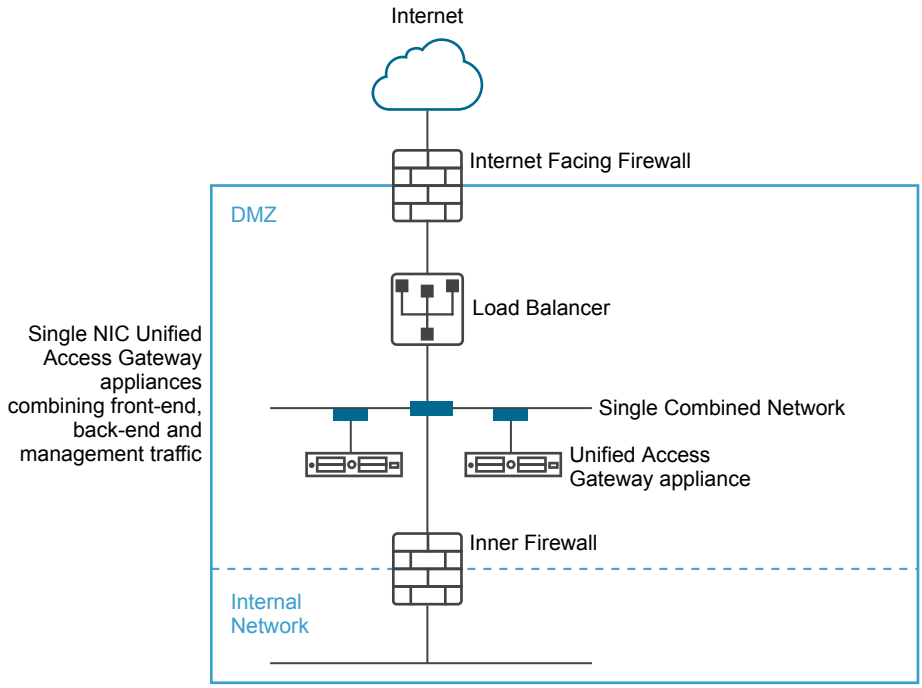
You can specify one, two, or three NICS settings which are specified as onenic, twonic or threenic.

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 Unified Access Gateway 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 Unified Access Gateway appliances. Unified Access Gateway then forwards the authorized traffic through the inner firewall to resources on the internal network. Unified Access Gateway discards unauthorized traffic.

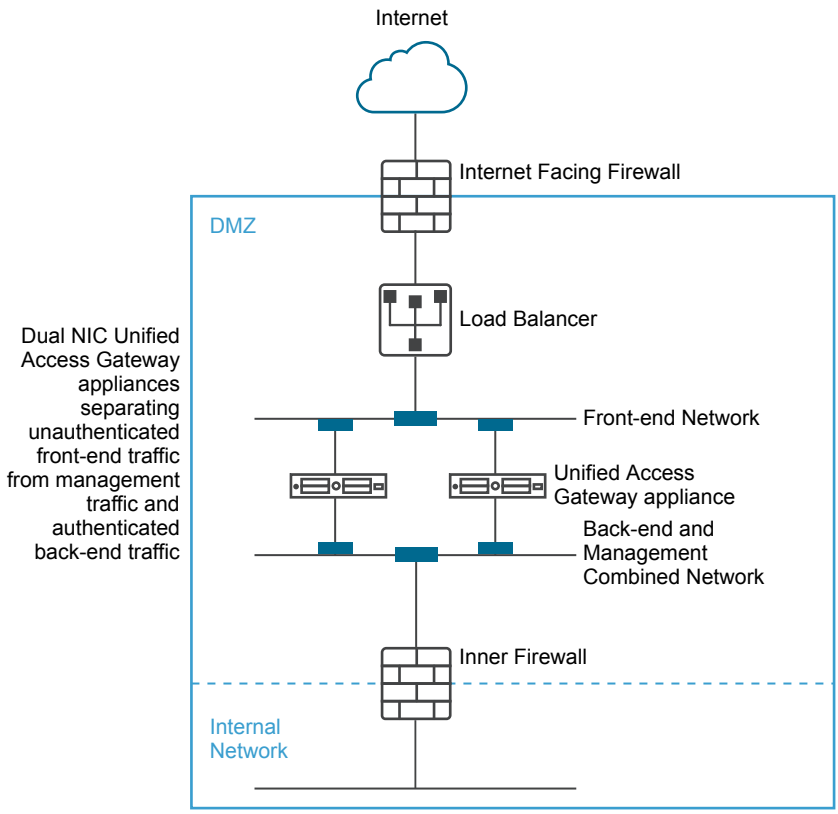
Figure 1-3. Unified Access Gateway Single NIC Option



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. Unified Access Gateway Two NIC Option



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

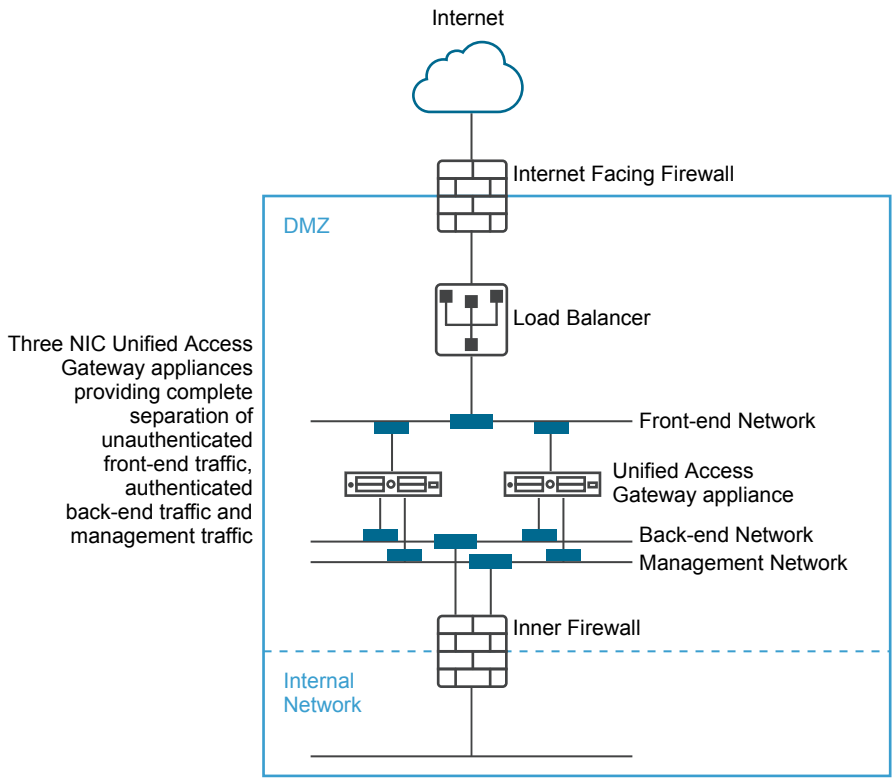
If a device on the unauthenticated front-end network, such as the load balancer, was compromised then reconfiguring that device to bypass Unified Access Gateway is not possible in this two NIC deployment. It combines layer 4 firewall rules with layer 7 Unified Access Gateway security. Similarly, if the Internet facing firewall was misconfigured to allow TCP port 9443 through, this would still not expose the Unified Access Gateway 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, you can 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 Unified Access Gateway 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.

Unified Access Gateway 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. Unified Access Gateway Three NIC Option



Upgrade with Zero Downtime

Zero downtime upgrades let you upgrade Unified Access Gateway with no downtime for the users. Before you upgrade a Unified Access Gateway appliance, the quiesce mode in the Unified Access Gateway system configuration pages is changed from NO to YES.

When the quiesce mode value is YES, the Unified Access Gateway appliance is shown as not available when the load balancer checks the health of the appliance. Requests that come to the load balancer are sent to the next Unified Access Gateway appliance that is behind the load balancer.

Prerequisites

- Two or more Unified Access Gateway appliances configured behind the load balancer
- The Health Check URL setting configured with a URL that the load balancer connects to check the health of Unified Access Gateway appliance
- Check the health of the appliance in the load balancer. Type the REST API command `GET https://mycoUnifiedAccessGateway.com:443/favicon.ico`.

The response is `HTTP/1.1 200 OK`, if the Quiesce Mode is set to No, or `HTTP/1.1 503`, if the Quiesce Mode is set to Yes.

Note Do not use any other URL other than `GET https://mycoUnifiedAccessGateway.com:443/favicon.ico`. Doing so will lead to incorrect status response and resource leaks.

Procedure

1. In the admin UI Configure Manual section, click **Select**.
2. In the Advanced Settings section, click the **System Configuration** gearbox icon.
3. In the **Quiesce Mode** row, enable **YES** to pause the Unified Access Gateway appliance.

   When the appliance is stopped, existing sessions that the appliance is serving are honored for 10 hours, after which the sessions are closed.
4. Click **Save**.

New requests that come to the load balancer are sent to next Unified Access Gateway appliance.

What to do next

Export the settings from the paused Unified Access Gateway appliance. Deploy a new version of Unified Access Gateway and import the settings. The new version of Unified Access Gateway appliance can be added to the load balancer.

Join or Leave the Customer Experience Improvement Program

The VMware Customer Experience Improvement Program (CEIP) provides information that VMware uses to improve its products and services, to fix problems, and to advise you on how best to deploy and use VMware products.

This product participates in VMware's Customer Experience Improvement Program ("CEIP"). Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html.

You can join or leave the CEIP for this product at any time from the Admin UI.

Procedure

1. From **Advanced Settings > System Configuration** select Yes or No.

   If you select Yes, the Customer Experience Improvement Program dialog appears with the checkbox selected to indicate that you are joining the program.
2. Review the information on the dialog and click **Close**.
3. Click **Save** on the System Configuration page to save your changes.

Deploying Unified Access Gateway Appliance

2

Unified Access Gateway 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 Unified Access Gateway appliance on a vSphere ESX or ESXi host. Microsoft Server 2012 and 2016 Hyper-V roles are supported.

- The vSphere Client or vSphere Web Client can be used to deploy the Unified Access Gateway 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 Unified Access Gateway admin user interface to configure Unified Access Gateway system settings, set up secure edge services in multiple use cases, and configure authentication in the DMZ. See Deploy Unified Access Gateway Using the OVF Template Wizard.
- PowerShell scripts can be used to deploy Unified Access Gateway 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 Unified Access Gateway. See Using PowerShell to Deploy the Unified Access Gateway Appliance.

Note For AirWatch Per-app Tunnel and Proxy use cases, you can deploy Unified Access Gateway on either ESXi or Microsoft Hyper-V environments.

This chapter includes the following topics:

Using the OVF Template Wizard to Deploy Unified Access Gateway

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

When you deploy the OVF, you configure how many network interfaces (NIC) are required, the IP address and set up the administrator and root passwords.

After the Unified Access Gateway is deployed, go to the administration user interface (UI) to set up the Unified Access Gateway environment. In the admin UI, configure the desktop and application resources and the authentication methods to use in the DMZ. To log in to the admin UI pages, go to `https://<mycoUnifiedGatewayAppliance>.com:9443/admin/index.html`.

Deploy Unified Access Gateway Using the OVF Template Wizard

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

Two versions of the Unified Access Gateway OVA are available, standard OVA and a FIPS version of the OVA. The FIPS 140-2 version runs with the FIPS certified set of ciphers and hashes and has restrictive services enabled that support FIPS certified libraries. When Unified Access Gateway is deployed in FIPS mode, the appliance cannot be changed to the standard OVA deployment mode.

Note 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

- Review the deployment options that are available in the wizard. See Unified Access Gateway System and Network Requirements.
- Determine the number of network interfaces and static IP addresses to configure for the Unified Access Gateway appliance. See Networking Configuration Requirements.
- Download the `.ova` installer file for the Unified Access Gateway 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, browse to the `.ova` file that you downloaded or enter a URL and click **Next**.

   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
Name and Location	Enter a name for the Unified Access Gateway virtual appliance. The name must be unique within the inventory folder. Names are case sensitive. Select a location for the virtual appliance.
Deployment Configuration	For an IPv4 network, you can use one, two, or three network interfaces (NICs). For an IPv6 network, use three NICs. Unified Access Gateway requires a separate static IP address for each NIC. Many DMZ implementations use separated networks to secure the different traffic types. Configure Unified Access Gateway according to the network design of the DMZ in which it is deployed.
Host / Cluster	Select the host or cluster in which to run the virtual appliance.
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.
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. Map the networks used in the OVF template to networks in your inventory. 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, 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.

Option	Description
Customize Network Properties	The text boxes on the Properties page are specific to Unified Access Gateway 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. ■ **IPMode: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. ■ **Comma separated list of forward rules in the form {tcp|udp}/listening-port-number/destination-ip-address:destination-port-nu** ■ **NIC 1 (ETH0) IPv4 address**. Enter the IPv4 address for the NIC if you entered STATICV4 for the NIC mode. ■ **Comma separated list of IPv4 custom routes for NIC 1 (eth0) in the form ipv4-network-address/bits.ipv4-gateway-address** ■ **NIC 1 (eth0) IPv6 address**. Enter the IPv6 address for the NIC if you entered STATICV6 for the NIC mode. ■ **NIC 1 (eth0) IPv4 Overriding Netmask**. Enter the IPv4 netmask for the NIC that would override the eth0 default netmask from the Network Protocol Profile (NPP). ■ **NIC 1 (eth0) IPv6 Overriding Prefix**. Enter the IPv6 prefix for the NIC that would override the eth0 default prefix from the Network Protocol Profile (NPP). ■ **DNS server addresses**. Enter space-separated IPv4 or IPv6 addresses of the domain name servers for the Unified Access Gateway appliance. Example of IPv4 entry is 192.0.2.1 192.0.2.2. Example of IPv6 entry is fc00:10:112:54::1 ■ **Default Gateway**. Enter a default value set by the vSphere network protocol profiles (Note: Enter a default gateway value only if IP mode is STATICV4/STATICV6). ■ **NIC 2 (eth1) IPv4 address**. Enter the IPv4 address for the NIC if you entered STATICV4 for the NIC mode. ■ **Comma separated list of IPv4 custom routes for NIC 2 (eth1) in the form ipv4-network-address/bits.ipv4-gateway-address** ■ **NIC 2 (eth1) IPv6 address**. Enter the IPv6 address for the NIC if you entered STATICV6 for the NIC mode. ■ **NIC 2 (eth1) IPv4 Overriding Netmask**. Enter the IPv4 netmask for the NIC that would override the eth1 default netmask from the Network Protocol Profile (NPP). ■ **NIC 2 (eth1) IPv6 Overriding Prefix**. Enter the IPv6 prefix for the NIC that would override the eth1 default prefix from the Network Protocol Profile (NPP). ■ **NIC 3 (eth2) IPv4 address**. Enter the IPv4 address for the NIC if you entered STATICV4 for the NIC mode. ■ **Comma separated list of IPv4 custom routes for NIC 3 (eth2) in the form ipv4-network-address/bits.ipv4-gateway-address** ■ **NIC 3 (eth2) IPv6 address**. Enter the IPv6 address for the NIC if you entered STATICV6 for the NIC mode. ■ **NIC 3 (eth2) IPv4 Overriding Netmask**. Enter the IPv4 netmask for the NIC that would override the eth2 default netmask from the Network Protocol Profile (NPP).

Option	Description
	■ **NIC 3 (eth2) IPv6 Overriding Prefix**. Enter the IPv6 prefix for the NIC that would override the eth2 default prefix from the Network Protocol Profile (NPP). ■ **Password options**. Enter the password for the root user of this VM and the password for the administrator user who accesses the administration console and enables REST API access. ■ **Password options**. Enter the password for the admin user who logs in to the Admin UI to configure Unified Access Gateway and who can enable the REST API access. ■ **TLS Port 443 Sharing**. Select this box to enable port443 sharing with HA Proxy. If selected here, this value cannot be modified from within the Admin UI. You can view the TLS SNI rules from within the Admin UI from either VMware Tunnel or Content Gateway settings. Other settings are either optional or already have a default setting entered.
Join CEIP	Select **Join the VMware Customer Experience Improvement Program** to join CEIP or deselect the option to leave CEIP.

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-UAG-appliance
```

In this URL, *FQDN-of-UAG-appliance* is the DNS-resolvable, fully qualified domain name of the Unified Access Gateway appliance.

If deployment was successful, you see the Web page provided by the server that Unified Access Gateway 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 Unified Access Gateway appliance is deployed and starts automatically.

What to do next

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

Note If you are not able to access the admin UI log in screen, check to see if the virtual machine has the IP address displayed during the installation of the OVA. If the IP address is not configured, use the vami command mentioned in the UI to reconfigure the NICs. Run the command as " `cd /opt/vmware/share/vami`" then the command "`./vami_config_net`".

Configuring Unified Access Gateway From the Admin Configuration Pages

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

Note The first time you launch the Unified Access Gateway Admin console, you will be prompted to change the password you set when you deployed the appliance.

The General Settings and Advanced Settings pages include the following.

- Unified Access Gateway system configuration and TLS server certificate
- Edge service settings for Horizon, Reverse Proxy, and VMware Tunnel, and Content Gateway (also referred to as CG)
- Authentication settings for RSA SecurID, RADIUS, X.509 Certificate, and RSA Adaptive Authentication
- SAML identity provider and service provider settings
- Network settings
- Endpoint Compliance Check Provider settings
- Identity Bridging setting configuration

The following options can be accessed from the Support Settings pages.

- Download Unified Access Gateway log zip files
- Export Unified Access Gateway settings to retrieve the configuration settings
- Set the log level settings
- Import Unified Access Gateway settings to create and update an entire Unified Access Gateway configuration

Configure Unified Access Gateway System Settings

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

Prerequisites

- Review the Unified Access Gateway Deployment Properties. The following settings information is required
  - Static IP address for the Unified Access Gateway appliance
  - IP Address of the DNS server
  - Password for the administration console
  - URL of the server instance or load balancer that the Unified Access Gateway 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 Unified Access Gateway appliance configuration values.

Option	Default Value and Description
UAG Name	Unique UAG appliance name.
Locale	Specifies the locale to use when generating error messages. ■ **en_US** for American English. This is the default. ■ **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 ■ **es** for Spanish ■ **pt_BR** for Brazilian Portuguese ■ **en_BR** for British English
Admin Password	You can reset the Admin password here. Whenever you change the password, you must log in to the Admin UI again before resuming your work. 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 Unified Access Gateway appliance. Cipher settings are used for enabling various security protocols.

Option	Default Value and Description
Honor Cipher Order	Default is NO. Select **YES** to enable TLS cipher list order control.
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.
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 Unified Access Gateway 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 Unified Access Gateway.
Cookies to be Cached	The set of cookies that Unified Access Gateway 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 Unified Access Gateway appliance to achieve a consistent state to perform maintenance tasks
Monitor Interval	Default value is **60**.
Password Age	Number of days current administrator password is valid. The default is 90 days. Specify zero (0) if password will never expire.
Request Timeout	Specify the request timeout in seconds. The default is 3000.
Body Receive Timeout	Specify the body receive timeout in seconds. The default is 5000.
Authentication Timeout	Specify the authentication timeout in seconds. The default is 300000.
Join CEIP	If enabled, sends Customer Experience Improvement Program ("CEIP") information to VMware. See Join or Leave the Customer Experience Improvement Program for details.

4 Click **Save**.

What to do next

Configure the edge service settings for the components that Unified Access Gateway 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 Unified Access Gateway 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. Select a Certificate Type of **PEM** or **PFX**.
4. If the Certificate Type is **PEM**:
   a. In the Private Key row, click **Select** and browse to the private key file.
   b. Click **Open** to upload the file.
   c. In the Certificate Chain row, click **Select** and browse to the certificate chain file.
   d. Click **Open** to upload the file.
5. If the Certificate Type is **PFX**:
   a. In the Upload PFX row, click **Select** and browse to the pfx file.
   b. Click **Open** to upload the file.
   c. Enter the password of the PFX certificate.
   d. Enter the alias of the PFX certificate. This is used when multiple certificates are present in the certificate store.
6. 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 Unified Access Gateway

3

A PowerShell script can be used to deploy Unified Access Gateway. 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 deploy Unified Access Gateway, 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 chapter includes the following topics:

System Requirements to Deploy Unified Access Gateway Using PowerShell

To deploy Unified Access Gateway 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 data store 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 Unified Access Gateway uses these values so make sure the values are correct.

Using PowerShell to Deploy the Unified Access Gateway Appliance

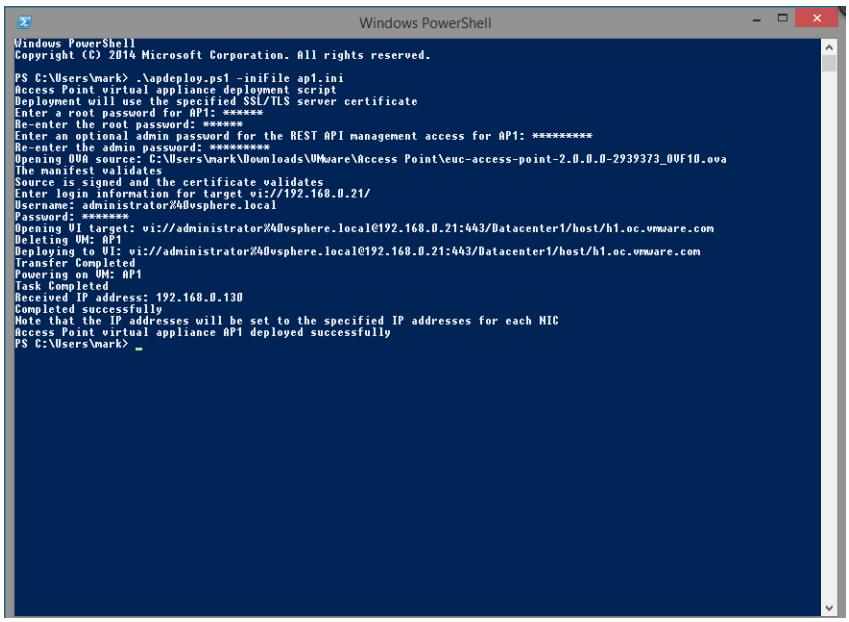
PowerShell scripts prepare you environment with all the configuration settings. When you run the PowerShell script to deploy Unified Access Gateway, the solution is ready for production on first system boot.

Prerequisites

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

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

  Figure 3-1. Sample PowerShell Script



Procedure

1. Download the Unified Access Gateway 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 an .INI configuration file for the Unified Access Gateway virtual appliance.

For example: Deploy a new Unified Access Gateway 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 Unified Access Gateway 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**.

Unified Access Gateway appliance is deployed and available for production.

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

Deployment Use Cases for Unified Access Gateway

4

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

You can deploy Unified Access Gateway with Horizon, Horizon Cloud with On-Premises Infrastructure, VMware Identity Manager, and VMware AirWatch.

This chapter includes the following topics:

Deployment with Horizon and Horizon Cloud with On-Premises Infrastructure

You can deploy Unified Access Gateway with Horizon Cloud with On-Premises Infrastructure and Horizon Air cloud infrastructure. For the Horizon deployment, the Unified Access Gateway appliance replaces Horizon security server.

Deployment Scenario

Unified Access Gateway 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 or Horizon Air for unified management.

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

Unified Access Gateway 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. Unified Access Gateway 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.

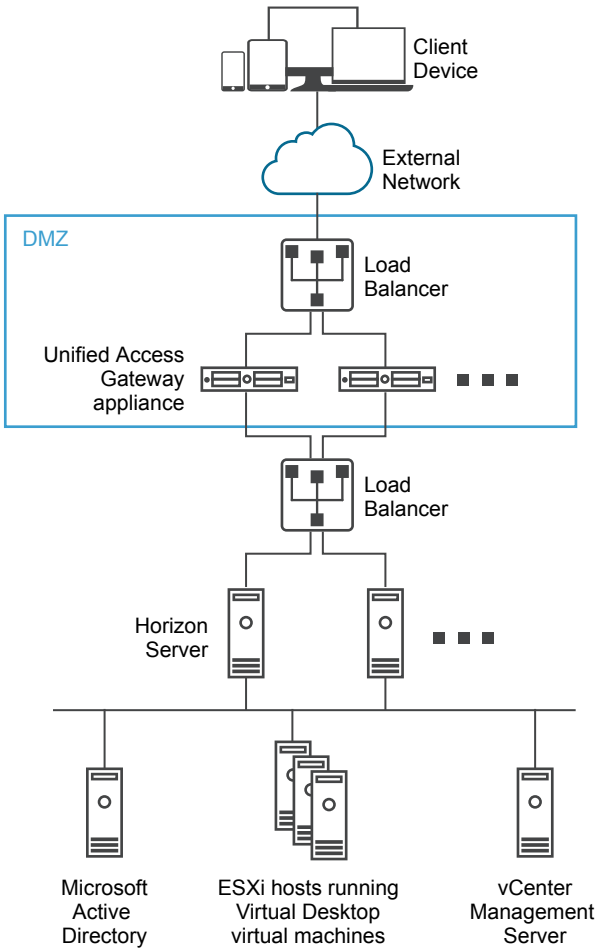
You must verify the requirements for seamless Unified Access Gateway deployment with Horizon.

- Unified Access Gateway appliance points to a load balancer in front of the Horizon servers, the selection of the server instance is dynamic.
- Unified Access Gateway replaces the Horizon security server.
- By default, port 8443 must be available for Blast TCP/UDP. However, port 443 can also be configured for Blast TCP/UDP.
- The Blast Secure Gateway and PCoIP Secure Gateway must be enabled when Unified Access Gateway is deployed with Horizon. This ensures that the display protocols can serve as proxies automatically through Unified Access Gateway. The BlastExternalURL and pcoipExternalURL settings specify connection addresses used by the Horizon Clients to route these display protocol connections through the appropriate gateways on Unified Access Gateway. 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 Unified Access Gateway.
- Disable the secure gateways (Blast Secure Gateway and PCoIP Secure Gateway) on Horizon Connection Server instances and enable these gateways on the Unified Access Gateway appliances.

The differences between Horizon security server and Unified Access Gateway appliance is as follows.

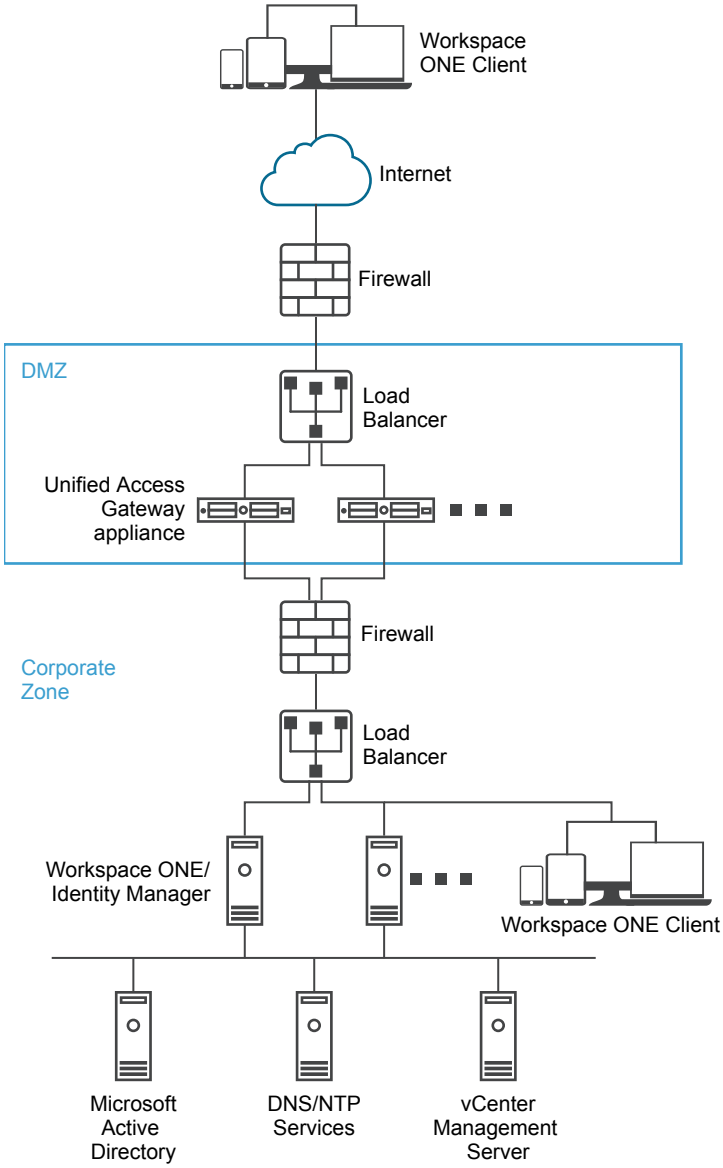
- Secure deployment. Unified Access Gateway is implemented as a hardened, locked-down, preconfigured Linux-based virtual machine
- Scalable. You can connect Unified Access Gateway to an individual Horizon Connection Server, or you can connect it through a load balancer in front of multiple Horizon Connection Servers, giving improved high availability. It acts as a layer between Horizon Clients and back end Horizon 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. Unified Access Gateway Appliance Pointing to a Load Balancer



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

Figure 4-2. Unified Access Gateway Appliance Pointing to a Horizon Server Instance



Authentication

User authentication is similar to View security server. Supported user authentication methods in Unified Access Gateway 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 various third party, two-factor security-vendor solutions
- Smart card, CAC, or PIV X.509 user certificates
- SAML

These authentication methods are supported with View Connection Server. Unified Access Gateway 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, Unified Access Gateway can forward requests for entitlement information, and desktop and application launch requests, to the View Connection Server. Unified Access Gateway also manages its desktop and application protocol handlers to allow them to forward only authorized protocol traffic.

Unified Access Gateway handles smart card authentication itself. This includes options for Unified Access Gateway 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 Unified Access Gateway with Horizon Cloud with On-Premises Infrastructure and Horizon Air cloud infrastructure. For the Horizon deployment, the Unified Access Gateway appliance replaces Horizon security server.

Procedure

1. In the admin UI **Configure Manually** section, click **Select**.
2. In the **General Settings > Edge Service Settings**, 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 Horizon. Unified Access Gateway can communicate with servers that use the Horizon XML protocol, such as Horizon Connection Server, Horizon Air, and Horizon Cloud with On-Premises Infrastructure.
Connection Server URL	Enter the address of the Horizon server or load balancer. Enter as https://00.00.00.00.
Connection Server URL Thumbprint	Enter the list of Horizon server thumbprints. If you do not provide a list of thumbprints, the server certificates must be issued by a trusted CA. Enter the hexadecimal thumbprint digits. For example, sha1= 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 Unified Access Gateway 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 URI Path	The URI path for the connection server that Unified Access Gateway connects to, for health status monitoring.
Enable PCOIP	Change NO to **YES** to specify whether the PCoIP Secure Gateway is enabled.
PCOIP External URL	Enter the external URL of the Unified Access Gateway appliance. Clients use this URL for secure connections through the PCoIP Secure Gateway. This connection is used for PCoIP traffic. The default is the Unified Access Gateway IP address and port 4172.
Enable Blast	To use the Blast Secure Gateway, change NO to **YES**.
Blast External URL	Enter the FQDN URL of the Unified Access Gateway appliance that end users use to make a secure connection from the Web browsers through the Blast Secure Gateway. Enter as `https://exampleappliance:443`.
Enable Tunnel	If the Horizon secure tunnel is used, change NO to **YES**. The Client uses the external URL for tunnel connections through the Horizon Secure Gateway. The tunnel is used for RDP, USB, and multimedia redirection (MMR) traffic.
Tunnel External URL	Enter the external URL of the Unified Access Gateway appliance. The default value is used if not set.
Endpoint Compliance Check Provider	Select the endpoint compliance check provider. Default is OPSWAT.
Proxy Pattern	Enter the regular expression that matches the URIs that are related to the Horizon Server URL (*proxyDestinationUrl*). For the Horizon Connection server, a forward slash (/) is a typical value to redirect to the HTML Access Web client when using the Unified Access Gateway appliance.
SAML SP	Enter the name of the SAML service provider for the Horizon XMLAPI broker. This name must either match the name of a configured service provider metadata or be the special value DEMO.
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	The location from where the connection request originates. The security server and Unified Access Gateway set the gateway location. The location can be external or internal.

Option	Description
Host Entries	Enter a comma separated list of host entries to be added in `/etc/hosts` file. Each entry includes an IP, a hostname, and an optional hostname alias in that order, separated by a space. For example, **`10.192.168.1 example1.com, 10.192.168.2 example2.com example-alias`**.
Disable HTML Access	If set to YES, disables web access to Horizon. See Endpoint Compliance Checks for Horizon for details.

7 Click **Save**.

Blast TCP and UDP External URL Configuration Options

The Blast Secure Gateway includes Blast Extreme Adaptive Transport (BEAT) networking, which dynamically adjusts to network conditions such as varying speeds and packet loss. In Unified Access Gateway, you can configure the ports used by the BEAT protocol.

Blast uses the standard ports TCP 8443 and UDP 8443. UDP 443 can also be used to access a desktop through the UDP tunnel server. The port configuration is set through the Blast External URL property.

Table 4-1. BEAT Port Options

Blast External URL	TCP Port Used by Client	UDP Port Used by Client	Description
https://ap1.myco.com	8443	8443	This form is the default and requires that TCP 8443, and optionally UDP 8443, to be opened at the firewall to allow the connections from the Internet to Unified Access Gateway
https://ap1.myco.com:443	443	8443	Use this form when TCP 443 or UDP 8443 are required to be opened.
https://ap1.myco.com:xxxx	xxxx	8443	
https://ap1.myco.com:xxxx/?UDPPort=yyyy	xxxx	yyyy	

To configure ports other than the default, an internal IP forwarding rule must be added for the respective protocol when deployed. The forwarding rules might be specified on the deployment in the OVF template or through the INI files that are input through the PowerShell commands.

Endpoint Compliance Checks for Horizon

The Endpoint Compliance Checks feature on Unified Access Gateway provides an extra layer of security for accessing Horizon desktops in addition to the other user authentication services that are available on Unified Access Gateway.

You can use the Endpoint Compliance Checks feature to ensure compliance to various policies such as an antivirus policy or encryption policy on endpoints, for example.

Endpoint compliance policy is defined on a service running in cloud or on-premises.

If Endpoint Compliance Checks is enabled, Unified Access Gateway allows only compliant VDI desktops to be launched and blocks launching of all non-compliant endpoints.

Prerequisites

1 Sign up for an OPSWAT account and register your applications on the OPSWAT site. See https://go.opswat.com/communityRegistration.

2 Note down the client key and client secret key. You need the keys to configure OPSWAT in Unified Access Gateway.

3 Log in to the OPSWAT site and configure the compliance policies for your endpoints. See the relevant OPSWAT documentation.

4 On the OPSWAT homepage, click **Connect Metadefender Endpoint Management** and download and install the agent software on the client device.

Procedure

1 Log in to Admin UI and go to **Advance Settings > Endpoint Compliance Check Provider Settings**.

2 Click **Add** to add the **Client Key** and **Client Secret** key details.

The **Endpoint Compliance Check Provider** and **Hostname** fields are already filled. Do not change these values.

3 From the Admin UI, navigate to Horizon settings, locate **Endpoint compliance check provider** field, and select OPSWAT from the drop-down menu.

4 Click **Save**.

5 Connect to the remote desktop using the Endpoint compliance check provider client.

The configured Horizon View desktops are listed and when you launch a desktop, the client device is validated for compliance.

Deployment as Reverse Proxy

Unified Access Gateway 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

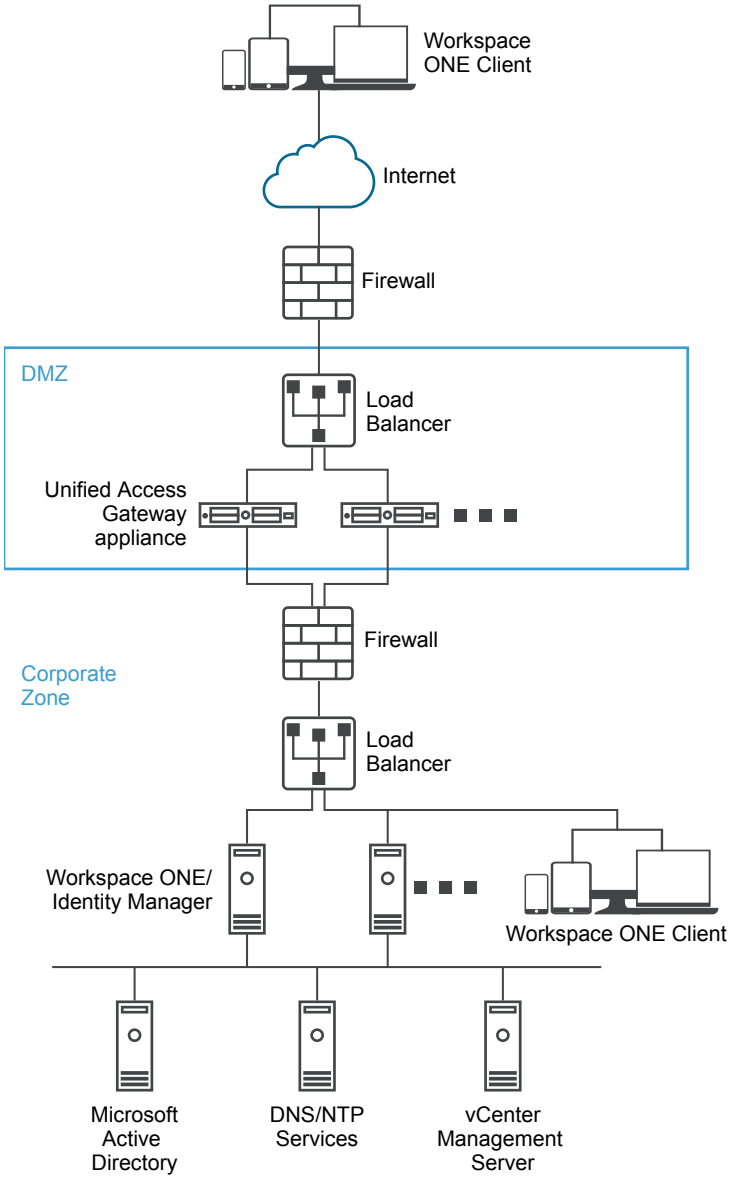
Unified Access Gateway provides secure remote access to an on-premises deployment of VMware Identity Manager. Unified Access Gateway appliances are typically deployed in a network demilitarized zone (DMZ). With VMware Identity Manager, the Unified Access Gateway appliance operates as a Web reverse proxy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

Requirements for Unified Access Gateway deployment with VMware Identity Manager.

- Split DNS

- VMware Identity Manager appliance must have a fully qualified domain name (FQDN) as hostname.
- Unified Access Gateway must use internal DNS. This means that the proxyDestinationURL must use FQDN.

Figure 4-3. Unified Access Gateway Appliance Pointing VMware Identity Manager



Understanding Reverse Proxy

Unified Access Gateway, 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.

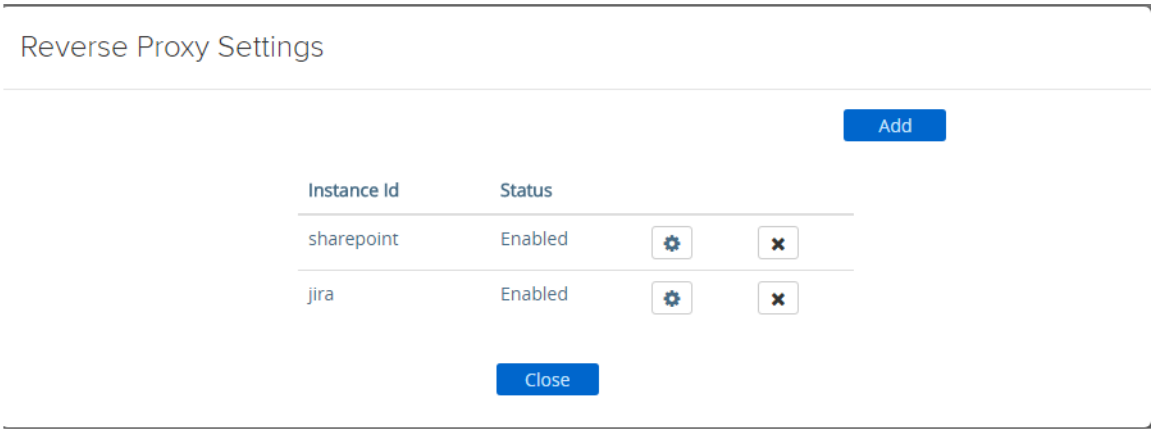
Note You must generate the identity provider metadata before enabling authentication on Web reverse proxy.

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

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

You can configure multiple instances of the reverse proxy and each configured instance can be deleted.

Figure 4-4. Multiple Reverse Proxies Configured



Configure Reverse Proxy

You can configure the Web reverse proxy service to use Unified Access Gateway with VMware Identity Manager.

Prerequisites

Requirements for deployment with VMware Identity Manager.

- Split DNS. The split DNS can be used to resolve the name to different IP addresses depending on whether the IP is internal or external.
- VMware Identity Manager service must have fully qualified domain name (FQDN) as hostname.
- Unified Access Gateway must use internal DNS. This means that the proxy Destination 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 Setting page, click **Add**.
5. In the Enable Reverse Proxy Settings section, change NO to **YES** to enable reverse proxy.

6 Configure the following edge service settings.

Option	Description
Identifier	The edge service identifier is set to Web reverse proxy.
Instance Id	The unique name to identify and differentiate a Web reverse proxy instance from all other Web reverse proxy instances.
Proxy Destination URL	Enter the address of the Web application.
Proxy Destination URL Thumbprints	Enter a list of acceptable SSL server certificate thumbprints for the proxyDestination URL. If you include the wildcard *, any certificate is allowed. A thumbprint is in the format [alg=]xx:xx, where alg can be sha1, the default, or md5. The 'xx' are hexadecimal digits. The ':' separator can also be a space or missing. The case in a thumbprint is ignored. For example: sha1=B6 77 DC 9C 19 94 2E F1 78 F0 AD 4B EC 85 D1 7A F8 8B DC 34, sha256=ad:5c:f1:48:47:94:7e:80:82:73:13:6c:83:52:be:78:ed:ff: 50:23:56:a8:42:8a:d9:30:fc:3a:33:d6:c6:db 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(.*))`. **Note** When you are configuring multiple reverse proxies, provide the hostname in the proxy host pattern.

7 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 Unified Access Gateway are listed in the drop-down menus.
Health Check URI Path	Unified Access Gateway connects to this URI path to check the health of your web application.
SAML SP	This field is required when configuring UAG as authenticated reverse proxy for VMware Identity Manager. Enter the name of the SAML service provider for the View XML API broker. This name must either match the name of a service provider you configured with Unified Access Gateway or be the special value `DEMO`. If there are multiple service providers configured withUnified Access Gateway, their names must be unique.
Activation Code	Enter the code generated by VMware Identity Manager service and imported into Unified Access Gateway to set up trust between VMware Identity Manager and Unified Access Gateway. Note that the Activation Code is not required for on-premise deployments. See *VMware Identity Manager Cloud Deployment* for details on how to generate an Activation Code.
External URL	The default value is the Unified Access Gateway host URL, port 443. You can enter another external URL. Enter as `https://<host:port>`.

Option	Description
UnSecure Pattern	Enter the known VMware Identity Manager redirection pattern. For example: `(/catalog-portal(.*)|/|/SAAS/|/SAAS|/SAAS/API/1.0/GET/image(.*)|/SAAS/horizon/css(.*)|/SAAS/horizon/angular(.*)|/SAAS/horizon/js(.*)|/SAAS/horizon/js-lib(.*)|/SAAS/auth/login(.*)|/SAAS/jersey/manager/api/branding|/SAAS/horizon/images/(.*)|/SAAS/jersey/manager/api/images/(.*)|/hc/(.*)/authenticate/(.*)|/hc/static/(.*)|/SAAS/auth/saml/response|/SAAS/auth/authenticatedUserDispatcher|/web(.*)|/SAAS/apps/|/SAAS/horizon/portal/(.*)|/SAAS/horizon/fonts(.*)|/SAAS/API/1.0/POST/sso(.*)|/SAAS/API/1.0/REST/system/info(.*)|/SAAS/API/1.0/REST/auth/cert(.*)|/SAAS/API/1.0/REST/oauth2/activate(.*)|/SAAS/API/1.0/GET/user/devices/register(.*)|/SAAS/API/1.0/oauth2/token(.*)|/SAAS/API/1.0/REST/oauth2/session(.*)|/SAAS/API/1.0/REST/user/resources(.*)|/hc/t/(.*)/(.*)/authenticate(.*)|/SAAS/API/1.0/REST/auth/logout(.*)|/SAAS/auth/saml/response(.*)|/SAAS/(.*)/(.*)auth/login(.*)|/SAAS/API/1.0/GET/apps/launch(.*)|/SAAS/API/1.0/REST/user/applications(.*)|/SAAS/auth/federation/sso(.*)|/SAAS/auth/oauth2/authorize(.*)|/hc/prepareSaml/failure(.*)|/SAAS/auth/oauthtoken(.*)|/SAAS/API/1.0/GET/metadata/idp.xml|/SAAS/auth/saml/artifact/resolve(.*)|/hc/(.*)/authAdapter(.*)|/hc/authenticate/(.*)|/SAAS/auth/logout|/SAAS/common.js|/SAAS/auth/launchInput(.*)|/SAAS/launchUsersApplication.do(.*)|/hc/API/1.0/REST/thinapp/download(.*)|/hc/t/(.*)/(.*)/logout(.*))`
Auth Cookie	Enter the authentication cookie name. For example: **`HZN`**
Login Redirect URL	If the user logs out of the portal, enter the redirect URL to log back in. For example: **`/SAAS/auth/login?dest=%s`**
Proxy Host Pattern	External hostname used to check the incoming host to see whether it matches the pattern for that particular instance. Host pattern is optional, when configuring Web reverse proxy instances. .
Host Entries	Enter a comma separated list of host entries to be added in /etc/hosts file. Each entry includes an IP, a hostname, and an optional hostname alias in that order, separated by a space. For example, **`10.192.168.1 example1.com, 10.192.168.2 example2.com example-alias`**.

Note UnSecure Pattern, Auth Cookie, and Login Redirect URL options are applicable only with VMware Identity Manager. The values provided here are also applicable to Access Point 2.8 and Unified Access Gateway 2.9.

Note The Auth Cookie and UnSecure Pattern properties are not valid for authn reverse proxy. You must use the Auth Methods property to define the authentication method.

8 Click **Save**.

What to do next

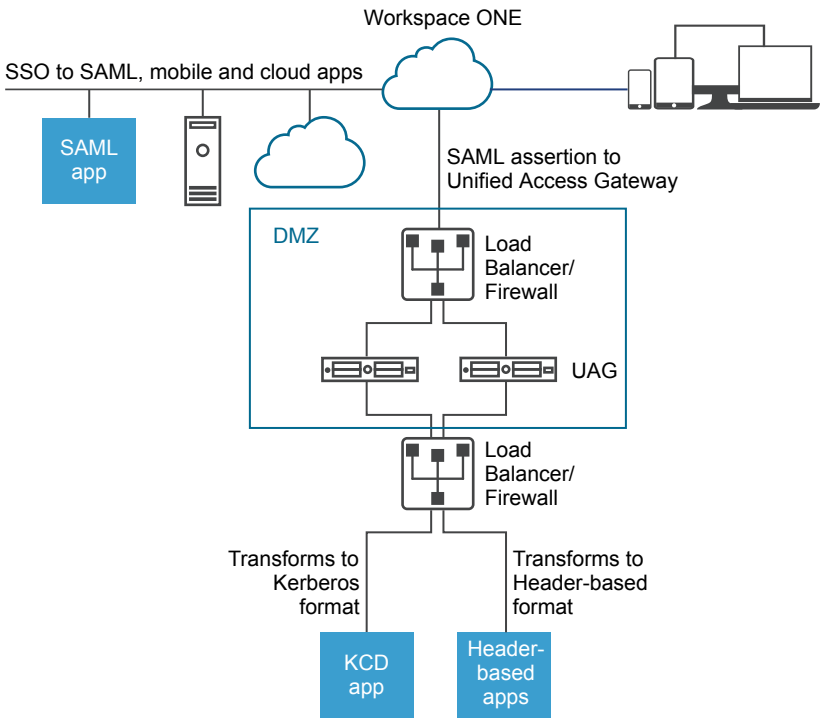
To enable identity bridging, see Configuring Identity Bridging Settings.

Deployment for Single Sign-on Access to On-Premises Legacy Web Apps

The Unified Access Gateway identity bridging feature can be configured to provide single sign-on (SSO) to legacy Web applications that use Kerberos Constrained Delegation (KCD) or header-based authentication.

Unified Access Gateway in identity bridging mode acts as the service provider that passes user authentication to the configured legacy applications. VMware Identity Manager acts as an identity provider and provides SSO into SAML applications. When users access legacy applications that require KCD or header-based authentication, Identity Manager authenticates the user. A SAML assertion with the user's information is sent to the Unified Access Gateway. Unified Access Gateway uses this authentication to allow users to access the application.

Figure 4-5. Unified Access Gateway Identity Bridging Mode



Identity Bridging Deployment Scenarios

Unified Access Gateway identity bridging mode can be configured to work with VMware Workspace® ONE® either in the cloud or in an on-premises environment.

Using Unified Access Gateway Identity Bridging with Workspace ONE Clients in the Cloud

The identity bridging mode can be set up to work with Workspace ONE in the cloud to authenticate users. When a user requests access to a legacy Web application, the identity provider applies applicable authentication and authorization policies.

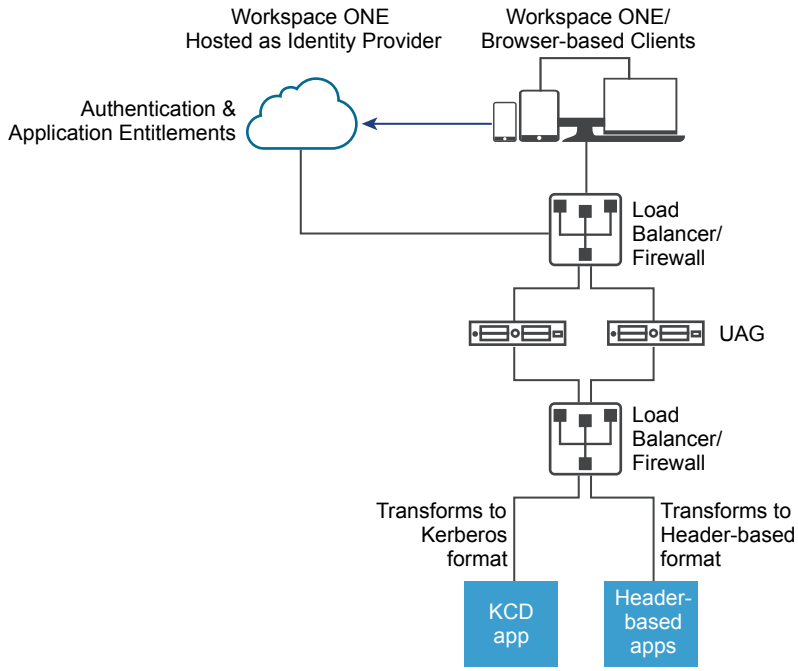
If the user is validated, the identity provider creates a SAML token and sends it to the user. The user passes the SAML token to Unified Access Gateway in the DMZ. Unified Access Gateway validates the SAML token and retrieves the User Principal Name from the token.

If the request is for Kerberos authentication, Kerberos Constrained Delegation is used to negotiate with the Active Directory server. Unified Access Gateway impersonates the user to retrieve the Kerberos token to authenticate with the application.

If the request is for header-based authentication, the user header name is sent to the Web server to request authentication with the application.

The application sends the response back to Unified Access Gateway. The response is returned to the user.

Figure 4-6. Unified Access Gateway Identity Bridging with Workspace ONE in the Cloud



Using Identity Bridging with Workspace ONE Clients On Premises

When the identity bridging mode is set up to authentication users with Workspace ONE in an on premises environment, users enter the URL to access the on-premise legacy Web application through the Unified Access Gateway proxy. Unified Access Gateway redirects the request to the identity provider for authentication. The identity provider applies authentication and authorization policies to the request. If the user is validated, the identity provider creates a SAML token and sends the token to the user.

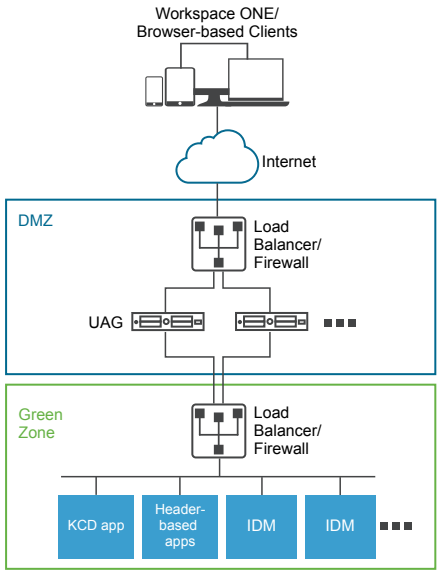
The user passes the SAML token to Unified Access Gateway. Unified Access Gateway validates the SAML token and retrieves the User Principal Name from the token.

If the request is for Kerberos authentication, Kerberos Constrained Delegation is used to negotiate with the Active Directory server. Unified Access Gateway impersonates the user to retrieve the Kerberos token to authenticate with the application.

If the request is for header-based authentication, the user header name is sent to the Web server to request authentication with the application.

The application sends the response back to Unified Access Gateway. The response is returned to the user.

Figure 4-7. Unified Access Gateway Identity Bridging On-Premises



Configuring Identity Bridging Settings

When Kerberos is configured in the back end application, to set up identity bridging in Unified Access Gateway, you upload the identity provider metadata and keytab file and configure the KCD realm settings.

Note This release of identity bridging supports only a single domain setup. This means the user and the SPN should be in the same realm/domain.

When identity bridging is enabled with header-based authentication, keytab settings and KCD realm settings are not required.

Before you configure the identity bridging settings for Kerberos authentication, make sure that the following is available.

- An identity provider is configured and the SAML metadata of the identity provider saved. The SAML metadata file is uploaded to Unified Access Gateway (SAML scenarios only).
- For Kerberos authentication, a server with Kerberos enabled with the realm names for the Key Distribution Centers to use identified.
- For Kerberos authentication, upload the Kerberos keytab file to Unified Access Gateway. The keytab file includes the credentials for the Active Directory service account that is set up to get the Kerberos ticket on behalf of any user in the domain for a given back-end service.

Upload Identity Provider Metadata

To configure the identity bridging feature, you must upload the identity provider's SAML certificate metadata XML file to Unified Access Gateway.

Prerequisites

SAML metadata XML file saved to a computer you can access.

If using VMware Identity Manager as the identity provider, download and save the SAML metadata file from the VMware Identity Manager admin console, Catalog > Settings SAML Metadata > Identity Provider (IdP) metadata link.

Procedure

1. In the admin UI Configure Manually section, click **Select**.
2. In the **Advanced Settings > Identity Bridging Settings** section, select the **Upload Identity Provider Metadata** gearbox icon.
3. Enter the entity ID for the identity provider in the **Entity ID** text box.

   If you do not enter a value in the Entity ID text box, the identity provider name in the metadata file is parsed and used as the entity ID of the identity provider.
4. In the **IDP Metadata** section, click **Select** and browse to the metadata file you saved. Click **Open**.
5. Click **Save**.

What to do next

For KDC authentication, configure the realm settings and the keytab settings.

For header-based authentication, when you configure the identity bridging feature, complete the User Header Name option with the name of the HTTP header that includes the user ID.

Configure Realm Settings

Configure the domain realm name, the key distribution centers for the realm, and the KDC timeout.

The realm is the name of an administrative entity that maintains authentication data. Selecting a descriptive name for the Kerberos authentication realm is important. Configure the realm, also known as the domain name, and the corresponding KDC service in Unified Access Gateway. When a UPN request comes to a specific realm, Unified Access Gateway internally resolves the KDC to use the Kerberos serviced ticket.

The convention is to make the realm name the same as your domain name, entered in uppercase letters. For example, a realm name is EXAMPLE.NET. The realm name is used by a Kerberos client to generate DNS names.

Starting with UAG 3.0, you can delete previously defined realms.

Prerequisites

A server with Kerberos enabled with the realm names for the Key Distribution Centers to use identified.

Procedure

1. In the admin UI Configure Manually section, click **Select**.
2. In the **Advanced Settings > Identity Bridging Settings** section, select the **Realm Settings** gearbox icon.
3. Click **Add**.
4. Complete the form.

Label	Description
Name of the realm	Enter the realm with the domain name. Enter the realm in uppercase letters. The realm must match the domain name set up in the Active Directory.
Key Distribution Centers	Enter the KDC servers for the realm. Comma separate the list if adding more than one server.
KDC Timeout (in seconds)	Enter the time to wait for the KDC response. The default is 3 seconds.

5. Click **Save**.

What to do next

Configure the keytab settings.

Upload Keytab Settings

A keytab is a file containing pairs of Kerberos principals and encrypted keys. A keytab file is created for applications that require single sign-on. Unified Access Gateway identity bridging uses a keytab file to authenticate to remote systems using Kerberos without entering a password.

When a user is authenticated into Unified Access Gateway from the identity provider,
Unified Access Gateway requests a Kerberos ticket from the Kerberos Domain Controller to authenticate the user.

Unified Access Gateway uses the keytab file to impersonate the user to authenticate to the internal Active Directory domain. Unified Access Gateway must have a domain user service account on the Active Directory domain. Unified Access Gateway is not directly joined to the domain.

Note If the admin regenerates the keytab file for a service account, the keytab file must be uploaded again into Unified Access Gateway.

Prerequisites

Access to the Kerberos keytab file to upload to Unified Access Gateway. The keytab file is a binary file. If possible, use SCP or another secure method to transfer the keytab between computers.

Procedure

1. In the admin UI Configure Manually section, click **Select**.
2. In the **Advanced Settings > Identity Bridging Settings** section, select the **Upload Keytab settings** gearbox icon.
3. (Optional) Enter the Kerberos principal name in the **Principal Name** text box.

   Each principal is always fully qualified with the name of the realm. The realm should be in uppercase.

   Make sure that the principal name entered here is the first principal found in the keytab file. If the same principal name is not in the keytab file that is uploaded, uploading the keytab file fails.
4. In the **Select Keytab file** field, click **Select** and browse to the keytab file you saved. Click **Open**.

   If you did not enter the principal name, the first principal found in the keytab is used. You can merge multiple keytabs into one file.
5. Click **Save**.

What to do next

Configure the Web reverse proxy for Unified Access Gateway identity bridging.

Configure a Web Reverse Proxy for Identity Bridging (SAML)

Enable identity bridging, configure the external host name for the service, and download the Unified Access Gateway service provider metadata file.

This metadata file is uploaded to the Web application configuration page in the VMware Identity Manager service.

Prerequisites

Identity Bridging Settings configured in the Unified Access Gateway admin UI, Advanced Settings section. The following settings must be configured.

- Identity provider metadata uploaded to Unified Access Gateway.
- The Kerberos principal name configured and the keytab file uploaded to Unified Access Gateway.
- The realm name and key distribution center information.

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, click **Add** to create a new proxy setting.

5 Set **Enable Reverse Proxy Settings** to YES, and configure the following edge service settings.

Option	Description
Identifier	The edge service identifier is set to Web reverse proxy.
Instance Id	Unique name for the Web reverse proxy instance.
Proxy Destination URL	Specify the internal URl for the Web application. Unified Access Gateway must be able to resolve and access this URL.
Proxy Destination URL Thumbprints	Enter the URI to match with this proxy setting. A thumbprint is in the format [alg=]xx:xx, where alg can be sha1, the default or md5. The 'xx' are hexadecimal 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	(Optional) Specify a host pattern. The host pattern tells Unified Access Gateway when to forward traffic using this proxy setting if the proxy pattern is not unique. This is decided using the URL used by the client's Web browser. For example, enter as `(/|/SAAS(.*)|/hc(.*)|/web(.*)|/catalog-portal(.*))`.

6 In the Enable Identity Bridging section, change NO to **YES**.

7 Configure the following Identity Bridging settings.

Option	Description
Authentication Types	Select SAML.
Identity Provider	Select the identity provider to use from the drop down menu.
Keytab	In the drop-down menu, select the configured keytab for this reverse proxy.
Target Service Principal Name	Enter the Kerberos service principal name. Each principal is always fully qualified with the name of the realm. For example, `myco_hostname@MYCOMPANY`. Type the realm name in uppercase. If you do not add a name to the text box, the service principal name is derived from the host name of the proxy destination URL.
Service Landing Page	Enter the page that users are redirected to in the identity provider after the assertion is validated. The default setting is `/`.
User Header Name	For header-based authentication, enter the name of the HTTP header that includes the user ID derived from the assertion.

8 In the Download SP Metadata section, click **Download**.

Save the service provider metadata file.

9 Click **Save**.

What to do next

Add the Unified Access Gateway service provider metadata file to the Web application configuration page in the VMware Identity Manager service.

Configuring a Web Reverse Proxy for Identity Bridging (Certificate to Kerberos)

Configure the Unified Access Gateway bridging feature to provide single sign-on (SSO) to On-Premises legacy non-SAML applications using certificate validation.

Prerequisites

Before starting the configuration process, make sure you have the following available:

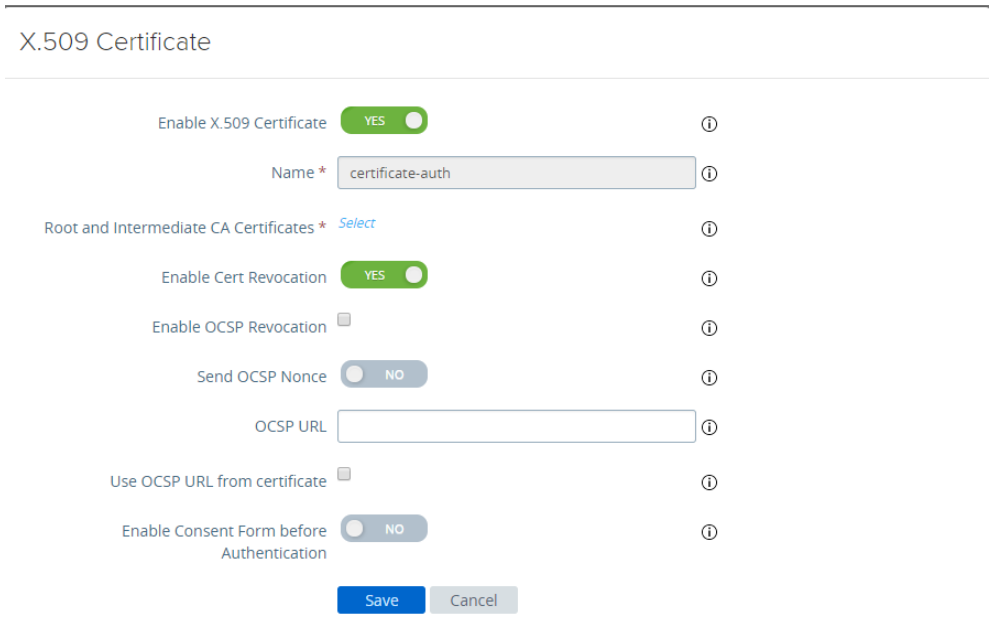
- Keytab file of a back end application, such as Sharepoint or JIRA
- Root CA certificate or the entire certificate chain with intermediate certificate for the domain.

Procedure

1. From Authentication Settings > X509 Certificate
   a. At **Root and Intermediate CA certificate**, click **Select** and upload the entire cert chain.
   b. At **Enable Cert Revocation**, set the toggle to **Yes**.
   c. Select the checkbox for **Enable OCSP Revocation**.

d Enter the OCSP responder URL in the **OCSP URL** field. Unified Access Gateway will send the OCSP request to the URL in this field and receive the response containing information indicating whether or not the certificate is revoked.

e Select the checkbox **Use OCSP URL from certificate** only if there is a use case to send the OCSP request to the OCSP URL in the client certificate. If this is not enabled, then it will default to the value in the OCSP URL field.



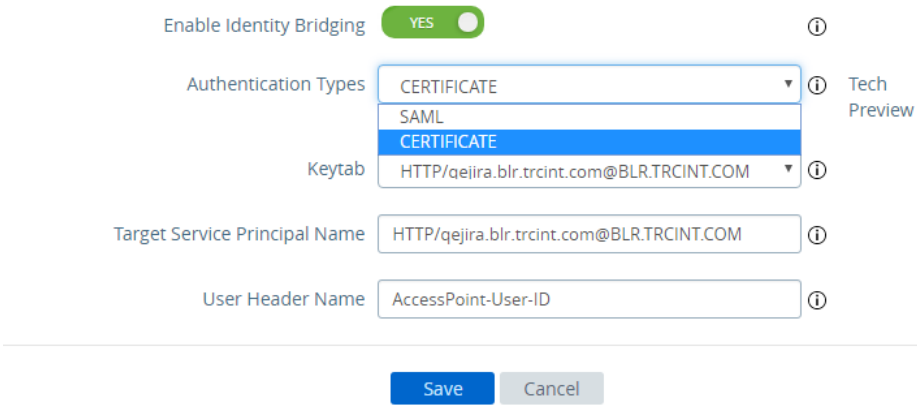
2 From Advanced Settings > Identity Bridging Settings > OSCP settings click **Add**.

a Click **Select** and upload the OCSP signing certificate.

3 Select the **Realm Settings** gearbox icon and configure the Realm settings as described in Configure Realm Settings.

4 From **General Settings > Edge Service Settings**, select the **Reverse Proxy Settings** gearbox icon.

5 Set **Enable Identity Bridging Settings** to **YES**, configure the following Identity Bridging settings, then click **Save**.



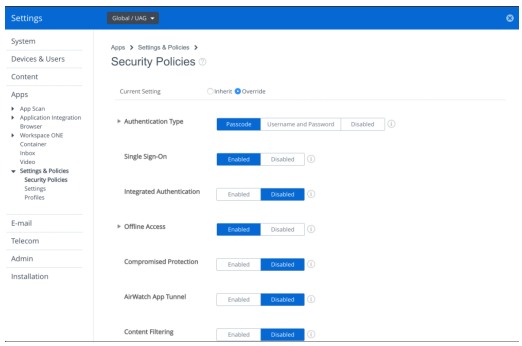
Option	Description
Authentication Types	Select CERTIFICATE from the drop down menu.
Keytab	In the drop-down menu, select the configured keytab for this reverse proxy.
Target Service Principal Name	Enter the Kerberos service principal name. Each principal is always fully qualified with the name of the realm. For example, **`myco_hostname@MYCOMPANY`**. Type the realm name in uppercase. If you do not add a name to the text box, the service principal name is derived from the host name of the proxy destination URL.
User Header Name	For header-based authentication, enter the name of the HTTP header that includes the user ID derived from the assertion or use the default, AccessPoint-User-ID.

6 Log in to the AirWatch console, select the appropriate Organization Group, and upload a certificate:

a Go to **All Settings > Apps > Security & Policies > Security Policies**.

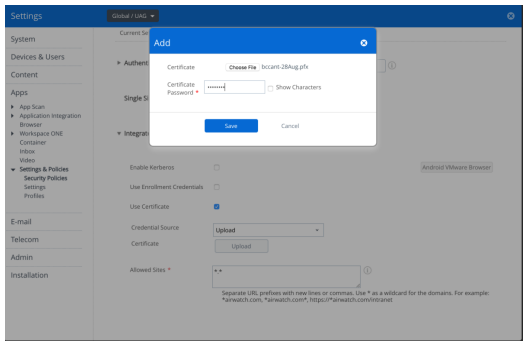
b Select the **Override** option.

c Enable **Integrated Authentication**.



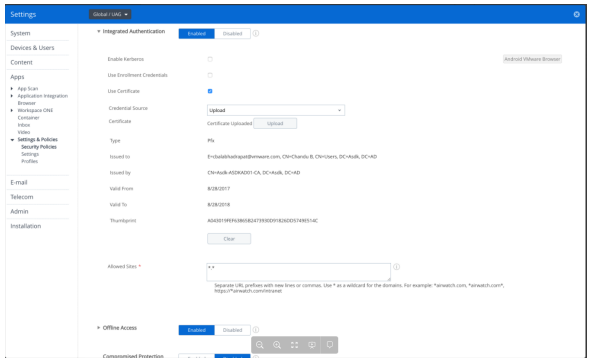
d Select **Use Certificate**.

e Select **Upload** as the Credential Source in the drop-down menu.



f Upload the user certificate in PFX format, enter the certificate password and click **Save**.

g Set **Allowed Sites** as ***** (asterisk).



h Click **Save**.

7 Enroll the device in the same Organization Group and environment as used in the previous step.

8 Use the AirWatch Browser to access the target website configured on the Unified Access Gateway (which is acting as the reverse-proxy).

Unified Access Gateway validates the presented certificate. If the certificate is valid, the browser displays the user interface page for the back end application. For troubleshooting details, see Troubleshooting Cert-to-Kerberos.

Add the Unified Access Gateway Service Provider Metadata File to VMware Identity Manager Service

The Unified Access Gateway service provider metadata file that you downloaded must be uploaded to the Web application configuration page in the VMware Identity Manager service.

The SSL certificate used must be the same certificate used across multiple load-balanced Unified Access Gateway servers.

Prerequisites

Unified Access Gateway Service Provider Metadata file saved to the computer

Procedure

1. Log in to the VMware Identity Manager admin console.
2. In the Catalog tab, click **Add Application** and select **create a new one**.
3. In the Application Details page, enter an end-user friendly name in the Name text box.
4. Select the **SAML 2.0 POST** authentication profile.

   You can also add a description of this application and an icon to display to end users in the Workspace ONE portal.
5. Click **Next** and in the Application Configuration page, scroll down to the **Configure Via** section.
6. Select the Meta-data XML radio button and paste the Unified Access Gateway service provider metadata text into the Meta-data XML text box.
7. (Optional) In the Attribute Mapping section, map the following attribute names to the user profile values. The FORMAT field value is Basic. The attribute names must be entered in lower case.

Name	Configured Value
upn	userPrincipalName
userid	Active Directory user ID

8. Click **Save**.

What to do next

Entitle users and groups to this application.

Note Unified Access Gateway supports only single domain users. If the identity provider is set up with multiple domains, the application can be entitled only to users in a single domain.

VMware Tunnel on Unified Access Gateway

Deploying VMware Tunnel using the Unified Access Gateway appliance provides a secure and effective method for individual applications to access corporate resources. Unified Access Gateway 3.0 supports deployment on either ESXi or Microsoft Hyper-V environments.

VMware Tunnel is composed of two independent components: Tunnel Proxy and Per-App Tunnel. You deploy VMware Tunnel using either of two network architecture models: single or multi-tier.

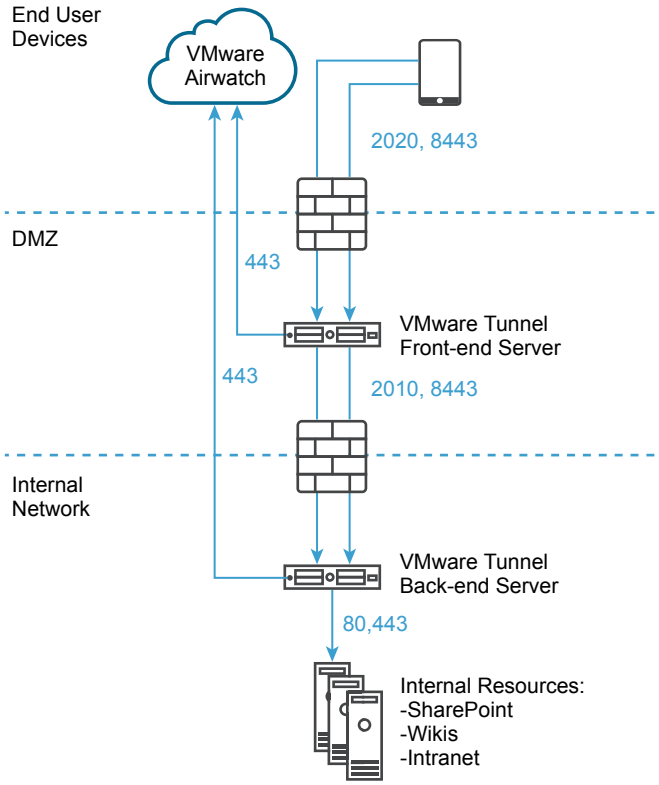
Both Tunnel Proxy and Per-App Tunnel deployment models can be used for a multi-tier network on the UAG appliance. The deployment consists of a front-end Unified Access Gateway server deployed in the DMZ and a back-end server deployed in the internal network.

The Tunnel Proxy component secures the network traffic between an end user device and a website through the VMware Browser or any AirWatch SDK-enabled application deployed from AirWatch. The mobile application creates a secure HTTPS connection with the Tunnel Proxy server and protects the sensitive data. Devices are authenticated to the Tunnel Proxy with a certificate issued via the SDK as configured in the AirWatch Admin Console. Typically, this component should be used when there are un-managed devices that need secured access to internal resources.

For fully enrolled devices, the Per-App Tunnel component allows devices to connect to internal resources without needing the AirWatch SDK. This component leverages the native Per-App VPN capabilities of the iOS, Android, Windows 10, and macOS operating systems. For more information on these platforms and VMware Tunnel component capabilities, please refer to the *VMware Tunnel Guide* at https://resources.air-watch.com/view/yr8n5s2b9d6qqbcfjbrw/en

Deploying the VMware Tunnel for your AirWatch environment involves setting up the initial hardware, configuring the VMware Tunnel hostname and port information in the AirWatch Admin Console, downloading and deploying the Unified Access Gateway OVF template, and manually configuring the VMware Tunnel. See Configure VMware Tunnel Settings for AirWatch for details.

Figure 4-8. VMware Tunnel Multi-Tier Deployment: Proxy and Per-App Tunnel



AirWatch v9.1 and above supports Cascade Mode as the Multi-Tier deployment model for VMware Tunnel. Cascade Mode requires a dedicated inbound port for each Tunnel component from the internet to the front-end Tunnel server. Both the front-end and back-end servers must be able to communicate with the AirWatch API and AWCM servers. VMware Tunnel Cascade mode supports the multi-tier architecture for the Per-App Tunnel component.

For more details, including those on Relay Endpoint Deployment for use with the Tunnel Proxy component, see the *VMware Tunnel* documentation at https://resources.air-watch.com/view/yr8n5s2b9d6qqbcfjbrw/en

Configure VMware Tunnel 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 **VMware Tunnel Settings** gearbox icon.

4 Change NO to **YES** to enable tunnel proxy.

5 Configure the following edge service settings resources.

Option	Description
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.
Organization Group ID	Enter the organization of the user.
Tunnel Server Hostname	Enter the VMware Tunnel external hostname configured in the AirWatch administrator console.

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

Option	Description
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 VMware Tunnel Proxy	Change NO to **YES** to use this proxy as an outbound proxy for VMware Tunnel. If not enabled, Unified Access Gateway uses this proxy for the initial API call to get the configuration from the AirWatch admin console.
Host Entries	Enter a comma separated list of host entries to be added in /etc/hosts file. Each entry includes an IP, a hostname, and an optional hostname alias in that order, separated by a space. For example, `10.192.168.1 example1.com, 10.192.168.2 example2.com example-alias`

Option	Description
TLS SNI Rules	This field displays only if TLS port 443 sharing is enabled during deployment. Specify the externalHostName:port that will be used for the service, for example "aw.uag.myco.com:8443" for Tunnel settings.
Trusted Certificates	Select the trusted certificate files to be added to the trust store.

7 Click **Save**.

For more information on deploying Unified Access Gateway with AirWatch, see the VMware Tunnel documentation https://my.air-watch.com/help/9.1/en/Content/Expert_Guides/EI/AW_Tunnel/C/Tunnel_Introduction.htm .

Deployment of VMware Tunnel for AirWatch using PowerShell

You can use PowerShell to deploy the VMware Tunnel for AirWatch.

For information on deploying VMware Tunnel with PowerShell, watch this video:

VMware AirWatch Tunnel PowerShell Deployment (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_airwatch_tunnel_powershell)

About TLS Port Sharing

Use the HA Proxy SNI redirection feature to facilitate sharing of port 443 with various components of Unified Access Gateway.

Unified Access Gateway currently runs VMware Tunnel, Content Gateway, Blast and Web reverse proxy services on TCP. Many users prefer to use port 443 for any incoming connections for their appliances, but this will not work as TCP traffic is routed from 443 to the Edge Service manager of Unified Access Gateway (port 6443), and VMware Tunnel and Content Gateway run on separate ports which must be opened externally.

Unified Access Gateway now uses the HA proxy SNI redirection feature to allow port 443 sharing between components. You enable TLS port sharing during deployment. For example, you can have an authenticated Web Reverse proxy instance and Content Gateway on the same appliance, with traffic for both services incoming on TCP 443, as long as the incoming hostname for Content Gateway matches the hostname configured in the TLS SNI rules for it.

If you deploy using the OVF template in the vSphere web client, check "Enable TLS port 443 sharing with HA proxy" from the Properties page. Alternatively, you can set the **tlsPortSharingEnabled** property to **true** when deploying with Powershell.

Note If TLS port sharing is enabled:

- You cannot later modify this setting from the Admin UI.
- You will get an error message if you attempt to import UAG settings from the Admin UI with a different value for this field. In this case, the port sharing property is ignored, but the rest of the UAG settings import successfully.
- You have the option to specify TLS SNI Rules along with the rest of the Edge service settings. This property is only available for VMware Tunnel and Content Gateway settings.

Content Gateway on Unified Access Gateway

Content Gateway is a component of the AirWatch Content Management solution that securely allows access to on-premise repository content on mobile devices.

Procedure

1. Navigate to **General Settings > Edge Service Settings > Content Gateway Settings** and click the gearbox icon.
2. Select **YES** to enable Content Gateway settings.
3. Configure the following settings and click **Save**.

Option	Description
Identifier	Indicates that this service is enabled.
API Server URL	The AirWatch API Server URL `[http[s]://]hostname[:port]` The destination URL must contain the protocol, host name or IP address, and port number. For example: `https://load-balancer.example.com:8443` Unified Access Gateway pulls Content Gateway configuration from API server.
API Server Username	Username to log into the API server.
API Server Password	Password to log into the API server.
Content Gateway Hostname	Hostname used to configure edge settings.
CG Configuration ID	AirWatch Content Gateway configuration ID.
Outbound Proxy Host	The host where the outbound proxy is installed. Unified Access Gateway makes a connection to API Server via outbound proxy if configured.
Outbound Proxy Port	Port of the outbound proxy.
Outbound Proxy Username	Username to log into the outbound proxy.
Outbound Proxy Password	Password to log into the outbound proxy.

Option	Description
NTLM Authentication	Specify whether the outbound proxy requires NTLM authentication.
Host Entries	Takes a comma-separated list of host entries to be added to the `/etc/hosts` file. Each entry should have an IP address, a hostname, and an optional hostname alias (in that order) separated by a space. For example: `10.192.168.1 example1.com`, `10.192.168.2 example2.com` example-alias)
TLS SNI Rule	This field displays only if TLS port 443 sharing is enabled during deployment. Specify the externalHostName:port that will be used for the service, for example "cg.uag.myco.com:10443" for Content Gateway.

Note

- HTTP traffic is not allowed for Content Gateway, on port 80 on Unified Access Gateway because TCP port 80 is used by edge service manager.
- When TLS port sharing is used with Content Gateway, the default internal listening port for Content Gateway is 10443.
  - The TLS SNI rule should be <CG_hostname>:**10443**
  - On the AirWatch console, the Content Gateway settings should be <CG_hostname>:**443**. Note that the CG_hostname is just the external hostname of the Unified Access Gateway appliance that a device uses to connect to.

For more information on Content Gateway, see https://my.air-watch.com/help/9.1/en/Content/Core_Guides/MCM/C/EI_CM_OvV.htm?tocpath=ARCHITECTURE%7CAirWatch%20Content%20Gateway%2C%20RFS%2C%20CRE%7C_____0

Configuring Unified Access Gateway Using TLS/SSL Certificates

5

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

Note Configuring the TLS/SSL certificates for the Unified Access Gateway appliance applies to Horizon, Horizon Air, and Web Reverse Proxy only.

Configuring TLS/SSL Certificates for Unified Access Gateway Appliances

TLS/SSL is required for client connections to Unified Access Gateway appliances. Client-facing Unified Access Gateway 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 a Unified Access Gateway 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 Unified Access Gateway. 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 Unified Access Gateway appliance needs a certificate.

When you submit a certificate signing request to a CA, provide the server name to associate with the certificate. Be sure that the Unified Access Gateway 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 Unified Access Gateway 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 is valid because it matches the host name specified by the client.

When you submit a certificate signing request to a CA, provide the external interface load balancer virtual IP address (VIP) as the common name and the SAN name. Be sure that the Unified Access Gateway appliance can resolve the server name you provide so that it matches the name associated with the certificate.

The certificate is used on port 443.

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 Unified Access Gateway 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 Unified Access Gateway appliance must be trusted by client machines and must also be applicable to all instances of Unified Access Gateway 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 Unified Access Gateway 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 Unified Access Gateway, 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 Unified Access Gateway 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 Unified Access Gateway 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 Unified Access Gateway 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 mycaservercertkey.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 Unified Access Gateway 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 certificate looks similar to this example.

Figure 5-1. Certificate File on a Single Line

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 Unified Access Gateway by using these `.pem` files with the PowerShell scripts attached to the blog post "Using PowerShell to Deploy VMware Unified Access Gateway," 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 a TLS/SSL server certificate, see Replace the Default TLS/SSL Server Certificate for Unified Access Gateway. For smart card certificates, see Configuring Certificate or Smart Card Authentication on the Unified Access Gateway Appliance.

Replace the Default TLS/SSL Server Certificate for Unified Access Gateway

To store a trusted CA-signed TLS/SSL server certificate on the Unified Access Gateway appliance, you must convert the certificate to the correct format and use the admin UI or the PowerShell scripts 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 Unified Access Gateway 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.

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 Unified Access Gateway 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.

Procedure

1. In the admin UI Configure Manually Section, click Select.
2. In the Advanced Settings > TLS Server Certificate Settings, click the gearbox icon.
3. Click **Select** for the Private Key and browse to the private key file. Click **Open** to upload the file.
4. Click **Select** for the Certificate Chain and browse to the certificate file. Click **Open** to upload the file.
5. Click **Save**.

   If the certificate is accepted, a success message displays.

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 Unified Access Gateway 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 and SSL v3.0 are disabled.

Prerequisites

- Familiarize yourself with the Unified Access Gateway REST API. The specification for this API is available at the following URL on the virtual machine where Unified Access Gateway 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 Unified Access Gateway 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 Unified Access Gateway 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 Unified Access Gateway, 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 Unified Access Gateway 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 chapter includes the following topics:

Configuring Certificate or Smart Card Authentication on the Unified Access Gateway Appliance

You can configure x509 certificate authentication in Unified Access Gateway 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 Unified Access Gateway service. Unified Access Gateway 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 the Online Certificate Status Protocol (OCSP) is supported. OCSP is a certificate validation protocol that is used to get the revocation status of a certificate.

You can configure OCSP in the certificate authentication adapter configuration.

You can also set up authentication so that Unified Access Gateway 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 through Unified Access Gateway to the VMware Identity Manager service. You can configure smart card authentication to be performed on the Unified Access Gateway appliance only if Unified Access Gateway is being used with Horizon 7.

Configure Certificate Authentication on Unified Access Gateway

You enable and configure certificate authentication from the Unified Access Gateway 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 Unified Access Gateway SAML metadata is added on the service provider and the service provider SAML metadata is copied the Unified Access Gateway appliance.
- (Optional) List of Object Identifier (OID) of valid certificate policies for certificate authentication.
- For revocation checking, 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.
***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.

Option	Description
Enable Cert Revocation	Change NO to **YES** to enable certificate revocation checking. Revocation checking prevents users who have revoked user certificates from authenticating.
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.
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.
Use OCSP URL from certificate	Check this box to use the OCSP URL.
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.

5 Click **Save**.

What to do next

When X.509 Certificate authentication is configured and Unified Access Gateway appliance is set up behind a load balancer, make sure that Unified Access Gateway 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 Unified Access Gateway and the client in order to pass the certificate to Unified Access Gateway.

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.

What to do next

Add the root certificate, intermediate certificate, or both to a server truststore file.

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.

What to do next

Add the CA certificate to a server truststore file.

Configure RSA SecurID Authentication in Unified Access Gateway

After the Unified Access Gateway appliance is configured as the authentication agent in the RSA SecurID server, you must add the RSA SecurID configuration information to the Unified Access Gateway 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 Unified Access Gateway instance. The value you enter must match the value you used when you added the Unified Access Gateway 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 for Unified Access Gateway

You can configure Unified Access Gateway so that users are required to use RADIUS authentication. You configure the RADIUS server information on the Unified Access Gateway 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, Unified Access Gateway 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 Unified Access Gateway 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 Unified Access Gateway. 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

Option	Action
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 Unified Access Gateway

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 Unified Access Gateway 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 Unified Access Gateway 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 Unified Access Gateway

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.
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.

Option	Description
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 Unified Access Gateway SAML Metadata

You must generate SAML metadata on the Unified Access Gateway 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, Unified Access Gateway is the identity provider and the server is the service provider.

Prerequisites

- Configure the clock (UTC) on the Unified Access Gateway appliance so that the appliance has the correct time. For example, open a console window on the Unified Access Gateway 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 Unified Access Gateway 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 Unified Access Gateway metadata.

  Note VMware recommends that you create and use a specific SAML signing certificate when you have more than one Unified Access Gateway 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 Unified Access Gateway 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 Unified Access Gateway 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 Unified Access Gateway can be used as an identity provider.

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

Copy Service Provider SAML Metadata to Unified Access Gateway

After you create and enable a SAML authenticator so that Unified Access Gateway 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 Unified Access Gateway appliance. This exchange of data establishes trust between the identity provider (Unified Access Gateway) and the back-end service provider, such as View Connection Server.

Prerequisites

Verify that you have created a SAML authenticator for Unified Access Gateway 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 Unified Access Gateway 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**.

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

Troubleshooting Unified Access Gateway Deployment

7

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

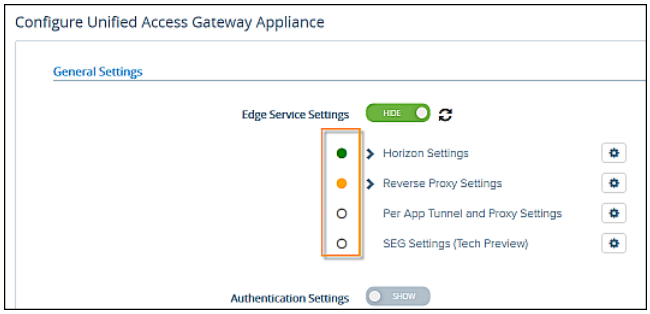
You can use troubleshooting procedures to investigate the causes of such problems and attempt to correct them yourself, or you can obtain assistance from VMware Technical Support.

This chapter includes the following topics:

Monitoring the Health of Deployed Services

You can quickly see that services you deployed are configured, up and running successfully from the admin UI for Edge Settings.

Figure 7-1. Health Check



A circle displays before the service. The color coding is as follows.

- Blank circle means that the setting is not configured.
- A red circle means that the service is down.
- An amber circle means that the service is partially running.
- A green circle means that the service is running without any issues.

Troubleshooting Deployment Errors

You might experience difficulty when you deploy Unified Access Gateway 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 Unified Access Gateway 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 Unified Access Gateway. 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 (or Unified Access Gateway 3.0 or later) and that the RSA Authentication Manager server is accessible on the network from Unified Access Gateway. Rerun the apdeploy Powershell command to redeploy the Unified Access Gateway 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.

Error message: "Unable to retrieve client certificate from session: sessionId"

- Check that the user certificate is installed properly in the browser.
- Check that the default TLS protocol versions 1.1 and 1.2 are enabled on the browser and on Unified Access Gateway.

Unable to deploy the Unified Access Gateway ova using VMware vSphere Web Client launched on the Chrome browser

You must install the client integration plugin on the browser you use to deploy an ova file on the vSphere Web Client. After installing the plugin on the Chrome browser, an error message displays indicating that the browser is not installed and and will not allow you to enter the ova file URL in the source location. This is a problem with the Chrome browser and is not related to the Unified Access Gateway ova. Please use a different browser to deploy the Unified Access Gateway ova.

Troubleshooting Cert-to-Kerberos

You might experience difficulty when you configure Cert-to-Kerberos in your environment. You can use a variety of procedures for diagnosing and fixing these problems.

Error creating Kerberos context: clock skew too great

This error message:

```
ERROR:"wsportal.WsPortalEdgeService[createKerberosLoginContext: 119][39071f3d-9363-4e22-
a8d9-5e288ac800fe]: Error creating kerberos context.
Identity bridging may not work
javax.security.auth.login.LoginException: Clock skew too great"
```

displays when the Unified Access Gateway time and the AD server time are significantly out of sync. Reset the time on the AD server to match the exact UTC time on Unified Access Gateway.

Error creating Kerberos context: name or service not known

This error message:

```
wsportal.WsPortalEdgeService[createKerberosLoginContext: 133][]: Error creating kerberos context.
Identity bridging may not work
javax.security.auth.login.LoginException: Name or service not known
```

displays when the Unified Access Gateway is unable to reach the configured realm or unable to connect to KDC with the user details in the keytab file. Confirm the following:

- the keytab file is generated with the correct SPN user account password and uploaded to Unified Access Gateway
- the back end application IP address and hostname are added correctly in host entries.

Error Message: unable to retrieve client certificate from session: <sessionId>

If this message displays:

- Check the X.509 certificate settings and determine whether or not it is configured

- If X.509 certificate settings is configured: check the client certificate installed on the client side browser to see if is issued by the same CA uploaded in the field "Root and Intermediate CA Certificates" in the X.509 certificate settings.

Error Message: Internal error. Please contact your administrator

Check the `/opt/vmware/gateway/logs/authbroker.log` for the message

`"OSCP validation of CN=clientCert, OU=EUC, O=<org name>, ST=<state name>, C=IN failed with "Could not send OCSP request to responder: Connection refused (Connection refused) , will attempt CRL validation"`

This indicates that the OCSP URL configured in "X.509 Certificate" is not reachable or incorrect.

Error when OCSP certificate is invalid

`"revocation.RevocationCheck: OSCP validation of CN=clientCert failed with "Could not verify signing certificate for OCSP responder:http://asdkad01/ocsp". will attempt CRL validation."`

displays when an invalid certificate for OCSP is uploaded or if the OCSP certificate is revoked.

Error when OCSP response verification fails

`"WARN ocsp.BouncyCastleOCSPHandler: Failed to verify OCSP response: CN=asdkAD01.Asdk.ADrevocation.RevocationCheck: 08/23 14:25:49,975" [tomcat-http--26] WARN revocation.RevocationCheck: OSCP validation of CN=clientCert failed with "Could not verify signing certificate for OCSP responder: http://asdkad01/ocsp". will attempt CRL validation."`

sometimes displays when OCSP response verification fails.

Error in receiving Kerberos token for user: user@domain.com, error: Kerberos Delegation Error: Method name: gss_acquire_cred_impersonate_name: Unspecified GSS failure. Minor code may provide more information

`"Kerberos Delegation Error: Method name: gss_acquire_cred_impersonate_name: Server not found in Kerberos database"`

If this message displays, check if:

- Trust between the domains is working.
- Target SPN name is configured correctly.

Troubleshooting Endpoint Compliance

You might experience difficulty when you deploy the Endpoint Compliance Check Provider in your environment. You can use a variety of procedures for diagnosing and fixing problems with your deployment.

Note `Esmanager.log` logs info about the MAC address of the device that is used for compliance check. This is useful in identifying the MAC address used for endpoint compliance check if the device has more than one NIC or switch to different networks.

Unified Access Gateway displays "Bad client credentials"

Unified Access Gateway makes the OPSWAT API call to validate the client-key and client secret provided. If the credentials are not correct then the settings are not saved, resulting in a

```
Bad client credentials
```

error.

Verify that the correct client key and client secret are in the Username and Password fields.

To generate client credentials, register your application here https://gears.opswat.com/o/app/register.

Unified Access Gateway displays "DNS is not able to resolve the host `https://gears.opswat.com` "

Use the ping command to discover the IP address for `gears.opswat.com` for your region.

Then, use the IP address from the ping command to create a `/etc/hosts` entry for `https://gears.opswat.com`. Navigate to Horizon settings from the Admin UI and provide the value in **Host Entries** for the View edge service.

Unified Access Gateway displays "The request timed out while connecting to the host `https://gears.opswat.com` "

This can happen if the host entry of `gears.opswat.com` is configured incorrectly in UAG or `https://gears.opswat.com` does not accept the connect request.

Troubleshooting Certificate Validation in the Admin UI

If you encounter errors when validating the PEM format of a certificate, look up the error message here for more information.

Here is a list of possible scenarios where errors are generated.

Error	Issue
Invalid PEM format. Could be due to wrong BEGIN format. See log for more details.	The PrivateKey BEGIN certificate is invalid.
Invalid PEM format. Exception message: -----END RSA PRIVATE KEY not found. See log for more details.	The PrivateKey END certificate is invalid.
Invalid PEM format. Exception message: problem creating RSA private key: java.lang.IllegalArgumentException: failed to construct sequence from byte[]: corrupted stream - out of bounds length found. See log for more details.	Thee PrivateKey in the certificate is corrupted.
Failed to parse certificates from PEM string. See log for more details.	The PublicKey BEGIN certificate is invalid.
Malformed PEM data encountered. See log for more details.	The PublicKey END certificate is invalid.
Malformed PEM data encountered. See log for more details.	The PublicKey in the certificate is corrupted.
There are no target/end certificates to build the chaining.	There is no target/end certificate.
Not able to build cert chain path, an intermediate/root certificate might be missing.	There is no certificate chain to build.
Ambiguous Error: Found more than one cert chain not sure which one to return	There is more than one certificate chain.

Troubleshooting Root Login Issues

If you log in as root to the Unified Access Gateway console with the correct username and password and get a "Login incorrect" error, check for keyboard mapping issues and reset the root password.

There are several reasons why a login error occurs:

- the keyboard used does not map certain password characters correctly according to the keyboard definition of Unified Access Gateway
- the password expired. The root password expires 365 days after deploying the ova.
- the password was not set correctly when the appliance was deployed. This is a known issue with older versions of Unified Access Gateway.
- the password has been forgotten.

To test that the keyboard is mapping characters correctly, try entering the password in response to the "Login:" username prompt. This allows you to see each password character and may identify where characters are being misinterpreted.

For all other causes, reset the root password of the appliance.

Note To reset the root password you must:

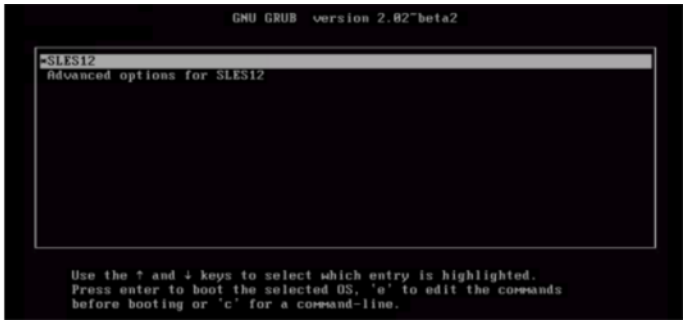
- have login access to vCenter
- know the vCenter login password
- have permission to access the appliance console

If you have set up a Grub 2 boot loader menu password for the appliance, you will need to enter this as part of this procedure.

Procedure

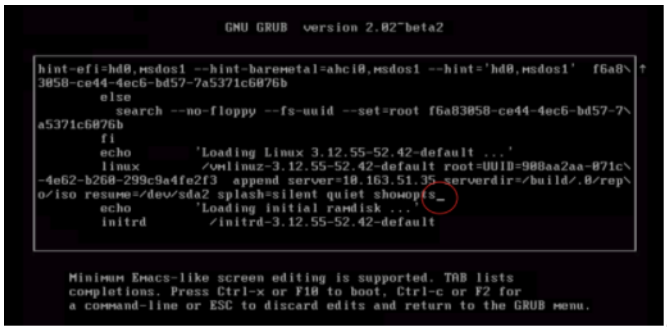
1 Restart the appliance from vCenter and immediately connect to the console.

2 As soon as the boot menu displays, press the space bar to disable auto boot.

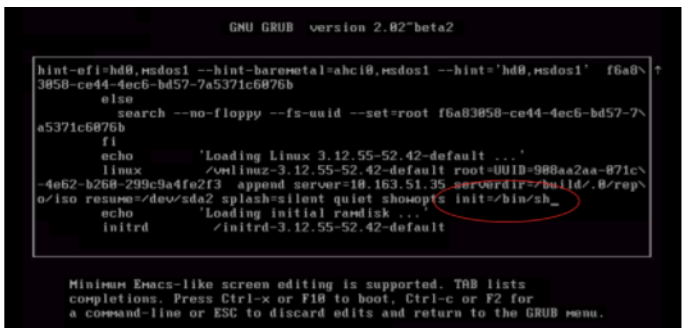


3 Use the arrow keys to highlight **SLES12** then type **e** to edit the commands. If you are running Unified Access Gateway 3.1 and have a Grub 2 password set up, enter the username ("root") and the Grub 2 password. The password is set by default and is the same as the root password which you configured when you deployed Unified Access Gateway.

   If you are running another version of Unified Access Gateway, you will not be prompted for the username and password unless you explicitly logged into the console and set the Grub2 password. See About the Grub2 Password for details.

4 Move the cursor down near the bottom of the displayed text and then up so that it is positioned after the showopts text. 

5 Enter a space character followed by `init=/bin/sh`

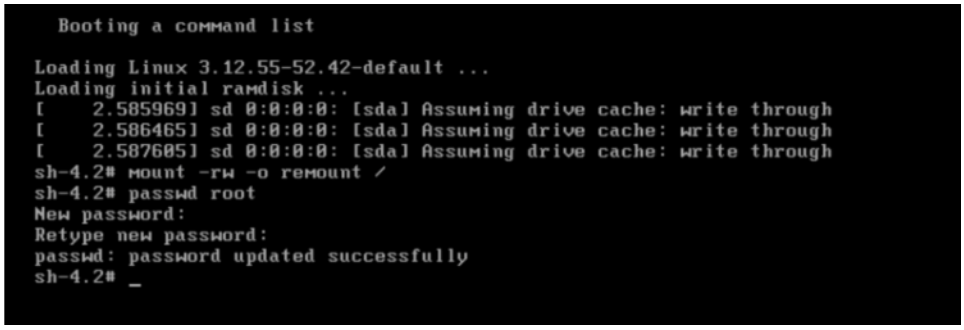


6 Press **Ctrl-X** or **F10** to boot the appliance. At the command prompt enter

   a `mount –rw –o remount /`

   b `passwd root`

7 Enter a new root password twice.



8 From vCenter reboot the appliance by powering off and on (power reset).

   - After the appliance boots, log in as root with the newly set password.

About the Grub2 Password

You can use the Grub2 password for your root login.

Starting with Unified Access Gateway 3.1, the Grub2 edit password will be set by default.

The username is root and the password is the same as the root password which you configured while deploying Unified Access Gateway. This password will never be reset unless you explicitly reset it by logging in to the machine.

Note Manually changing the root password by logging into the machine using any commands will not reset the Grub2 password. They are mutually exclusive. Only during deployment will the same password be set for both (with UAG 3.1 version and later).

Collecting Logs from the Unified Access Gateway Appliance

Download the AP-Log Archive.zip file from the support settings in the Admin UI. The ZIP file contains all logs from your Unified Access Gateway appliance.

Set the Logging Level

You can manage the log level settings from the admin UI. Go to the Support Settings page and select Log Level Settings. The log levels that can be generated are INFO, WARNING, ERROR, and DEBUG. The logging level is set by default to INFO.

A description of the type of information that the log levels collect follows.

Table 7-1. Logging Levels

Level	Type of Information Collected
INFO	The INFO level designates information messages that highlight the progress of the service.
ERROR	The ERROR level designates error events that might still allow the service to continue running.
WARNING	The WARNING level designates potentially harmful situations but are usually recoverable or can be ignored.
DEBUG	Designates events that would generally be useful to debug problems, to view or manipulate the internal state of the appliance, and to test the deployment scenario in your environment.

Collect Logs

Download the log ZIP files from the Support Settings section of the admin UI.

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 7-2. Files That Contain System Information to Aid in Troubleshooting

File Name	Description	Linux Command (if applicable)
`rpm-version.log`	Version of the UAG appliance (2.8, 2.9, 3.0 etc).	
`ipv4-forwardrules`	IPv4 forwarding rules configured on the appliance.	
`df.log`	Contains information about disk space usage on the appliance.	`df -a -h --total`
`netstat.log`	Contains information on open ports and existing TCP connections.	`netstat -an`
`netstat-s.log`	Network stats (bytes sent/received etc) from the time of creation of the appliance.	`netstat -s`
`netstat-r.log`	Static routes created on the appliance.	`netstat -r`
`uag_config.json`, `uag_config.ini`	Entire configuration of the Unified Access Gateway appliance, showing all of the settings as a json and an ini file.	
`ps.log`	Includes processes running at the time of downloading logs.	`ps -elf --width 300`
`ifconfig.log`	Network interface configuration for the appliance.	`ifconfig -a`
`free.log`	RAM availability at the time of downloading logs.	`free`
`top.log`	Sorted list of processes by memory usage at the time of downloading logs .	`top -b -o %MEM -n 1`

Table 7-3. Log Files for Unified Access Gateway

File Name	Description	Linux Command (if applicable)
`w.log`	Information about uptime, the users currently on the machine, and their processes.	`w`
`service.log`	List of services currently running on the appliance	`service --status-all`
`supervisord.log`	Supervisor (manager for the Edge Service manager, admin and a AuthBroker) log.	

Table 7-3. Log Files for Unified Access Gateway (Continued)

File Name	Description	Linux Command (if applicable)
esmanager-x.log, esmanager-std-out.log	Edge service manager log(s), showing back end processes performed on the appliance.	
authbroker.log	Contains log messages from the AuthBroker process, which handles Radius and RSA SecurID authentication.	
admin.log, admin-std-out.log	Admin GUI logs. Contains log messages from the process that provides the Unified Access Gateway REST API on port 9443.	
bsg.log	Contains log messages from the Blast Secure Gateway.	
SecurityGateway_xxx.log	Contains log messages from the PCoIP Secure Gateway.	
utserver.log	Contains log messages from the UDP Tunnel Server.	
appliance-agent.log	Contains log messages from the VMware Tunnel agent (which starts up server and proxy).	
haproxy.conf	Contains log messages from the HA proxy configuration for TLS port sharing, if configured.	
vami.log	Contains log messages from running vami commands to set network interfaces during deployment.	
aw-content-gateway.log, aw-content-gateway-wrapper.log, aw-0.content-gateway-YYYY-mm.dd.log.zip	Contains log messages from AirWatch Content Gateway.	
admin-zookeeper.log	Contains log messages related to the data layer that is used to store the Unified Access Gateway configuration.	
tunnel.log	Contains log messages from the tunnel process that is used as part of the XML API processing. You must have Tunnel enabled in the Horizon settings in order see this log.	

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

Export Unified Access Gateway Settings

Export Unified Access Gateway configuration settings in both JSON and INI formats from the Admin UI.

You can export all Unified Access Gateway configuration settings and save them in JSON or INI format. You can use the exported INI file to deploy Unified Access Gateway using Powershell scripts.

Procedure

1 Navigate to **Support Settings > Export** Unified Access Gateway Settings.

2 Click **JSON** or **INI** to export the Unified Access Gateway settings in the format you want. To save the settings in both formats, click the **Log Archive** button.

   The files are saved by default in your Downloads folder.