Deploying and Configuring VMware Unified Access Gateway

02 JUL 2019
Unified Access Gateway 3.6

vmware®

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

https://docs.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 Workspace ONE UEM 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
- Using Unified Access Gateway Instead of a Virtual Private Network
- Unified Access Gateway System and Network Requirements
- Firewall Rules for DMZ-Based Unified Access Gateway Appliances
- System Requirements for Deploying VMware Tunnel with Unified Access Gateway
- Unified Access Gateway Load Balancing Topologies
- Unified Access Gateway High Availability
- DMZ Design for Unified Access Gateway with Multiple Network Interface Cards
- Upgrade with Zero Downtime
- Deploying Unified Access Gateway Without Network Protocol Profile (NPP)
- Join or Leave the Customer Experience Improvement Program

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 Horizon Connection Server 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 withHorizon Connection Server 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 VMware vSphere that is the same as the version supported for the VMware products and versions respectively.

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 1.8 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

Unified Access Gateway Sizing Options

- **Standard:** This configuration is recommended for Horizon deployment supporting up to 2000 Horizon connections, aligned with the Connection Server capacity. It is also recommended for Workspace ONE UEM Deployments (mobile use cases) up to 10,000 concurrent connections.

- **Large:** This configuration is recommended for Workspace ONE UEM Deployments, where Unified Access Gateway needs to support over 50,000 concurrent connections. This size allows Content Gateway, Per App Tunnel and Proxy, and Reverse Proxy to use the same Unified Access Gateway appliance.

- **Extra Large**: This configuration is recommended for Workspace ONE UEM Deployments. This size allows Content Gateway, Per App Tunnel and Proxy, and Reverse Proxy to use the same Unified Access Gateway appliance.

- **Note** VM options for Standard, Large, and Extra Large deployments:

    - Standard - 2 core and 4GB RAM

    - Large - 4 core and 16 GB RAM

    - Extra Large - 8 core and 32 GB RAM

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 Workspace ONE UEM 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.

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.

The following tables list the port requirements for the different services within Unified Access Gateway.

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

Table 1-1. Port Requirements for Horizon Connection Server

Port	Protocol	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 443 is internally forwarded to UDP 9443 on UDP Tunnel Server service on Unified Access Gateway.
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 Connection Server	Horizon Client XML-API, Blast extreme HTML access, Horizon Air Console Access (HACA)
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

Note 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 1-2. Port Requirements for Web Reverse Proxy

Port	Protocol	Source	Target	Description
443	TCP	Internet	Unified Access Gateway	For web traffic
Any	TCP	Unified Access Gateway	Intranet Site	Any configured custom port on which the Intranet is listening. For example, 80, 443, 8080 and so on.
88	TCP	Unified Access Gateway	KDC Server/AD Server	Required for Identity Bridging to access AD if SAML to Kerberos/Certificate to Kerberos is configured.
88	UDP	Unified Access Gateway	KDC Server/AD Server	Required for Identity Bridging to access AD if SAML to Kerberos/Certificate to Kerberos is configured.

Table 1-3. Port Requirements for Admin UI

Port	Protocol	Source	Target	Description
9443	TCP	Admin UI	Unified Access Gateway	Management interface

Table 1-4. Port Requirements for Content Gateway Basic Endpoint Configuration

Port	Protocol	Source	Target	Description
443* or any port > 1024	HTTPS	Devices (from Internet and Wi-Fi)	Unified Access Gateway Content Gateway Endpoint	If 443 is used, Content Gateway will listen on port 10443.
443* or any port > 1024	HTTPS	Workspace ONE UEM Device Services	Unified Access Gateway Content Gateway Endpoint	
443* or any port > 1024	HTTPS	Workspace ONE UEM Console	Unified Access Gateway Content Gateway Endpoint	If 443 is used, Content Gateway will listen on port 10443.
Any port where the repository is listening to.	HTTP or HTTPS	Unified Access Gateway Content Gateway Endpoint	Web-based content repositories such as (SharePoint/WebDAV/CMIS, and so on	Any configured custom port on which the Intranet site is listening to.
137–139 and 445	CIFS or SMB	Unified Access Gateway Content Gateway Endpoint	Network Share-based repositories (Windows file shares)	Intranet Shares

Table 1-5. Port Requirements for Content Gateway Relay Endpoint Configuration

Port	Protocol	Source	Target/Destination	Description
443* or any port > 1024	HTTP/ HTTPS	Unified Access Gateway Relay Server(Content Gateway Relay)	Unified Access Gateway Content Gateway Endpoint	If 443 is used, Content Gateway will listen on port 10443.
443* or any port > 1024	HTTPS	Devices (from Internet and Wi-Fi)	Unified Access Gateway Relay Server(Content Gateway Relay)	If 443 is used, Content Gateway will listen on port 10443.
443* or any port > 1024	TCP	Workspace ONE UEM Device Services	Unified Access Gateway Relay Server(Content Gateway Relay)	If 443 is used, Content Gateway will listen on port 10443.
443* or any port > 1024	HTTPS	Workspace ONE UEM Console		
Any port where the repository is listening to.	HTTP or HTTPS	Unified Access Gateway Content Gateway Endpoint	Web-based content repositories such as (SharePoint/WebDAV/CMIS, and so on	Any configured custom port on which the Intranet site is listening to.

Table 1-5. Port Requirements for Content Gateway Relay Endpoint Configuration (continued)

Port	Protocol	Source	Target/Destination	Description
443* or any port > 1024	HTTPS	Unified Access Gateway (Content Gateway Relay)	Unified Access Gateway Content Gateway Endpoint	If 443 is used, Content Gateway will listen on port 10443.
137–139 and 445	CIFS or SMB	Unified Access Gateway Content Gateway Endpoint	Network Share-based repositories (Windows file shares)	Intranet Shares

Note Since Content Gateway service runs as a non-root user in Unified Access Gateway, Content Gateway cannot run on system ports and therefore, custom ports should be > 1024.

Table 1-6. Port Requirements for VMware Tunnel

Port	Protocol	Source	Target/Destination	Verification	Note (See the Note section at the bottom of the page)
2020 *	HTTPS	Devices (from Internet and Wi-Fi)	VMware Tunnel Proxy	Run the following command after installation: `netstat – tlpn	grep [Port]`	
8443 *	TCP	Devices (from Internet and Wi-Fi)	VMware Tunnel Per-App tunnel	Run the following command after installation: `netstat – tlpn	grep [Port]`	1

Table 1-7. VMware Tunnel Basic Endpoint Configuration

Port	Protocol	Source	Target/Destination	Verification	Note (See the Note section at the bottom of the page)
SaaS: 443 : 2001 *	HTTPS	VMware Tunnel	Workspace ONE UEM Cloud Messaging Server	`curl –Ivv https://<AWCM URL>:<port>/awcm/status/ping` The expected response is HTTP 200 OK.	2
SaaS: 443 On-Prem: 80 or 443	HTTP or HTTPS	VMware Tunnel	Workspace ONE UEM REST API Endpoint ■ SaaS:`https://asXXX.awmdm.com` or `https://asXXX.airwatchportals.com` ■ On-Prem: Most commonly your DS or Console server	`curl –Ivv https://<API URL>/api/mdm/ping` The expected response is HTTP 401 unauthorized.	5

Table 1-7. VMware Tunnel Basic Endpoint Configuration (continued)

Port	Protocol	Source	Target/Destination	Verification	Note (See the Note section at the bottom of the page)
80,443, any TCP	HTTP, HTTPS, or TCP	VMware Tunnel	Internal Resources	Confirm that the VMware Tunnel can access internal resources over the required port.	4
514 *	UDP	VMware Tunnel	Syslog Server		
On-prem: 2020	HTTPS	Workspace ONE UEM Console	VMware Tunnel Proxy	On-Premises users can test the connection using the `telnet` command :`telnet <Tunnel Proxy URL> <port>`	6

Table 1-8. VMware Tunnel Cascade Configuration

Port	Protocol	Source	Target/Destination	Verification	Note (See the Note section at the bottom of the page)
SaaS: 443 On-Prem: 2001 *	TLS v1.2	VMware Tunnel Front-End	Workspace ONE UEM Cloud Messaging Server	Verify by using `wget` to `https://<AWCM URL>:<port>/awcm/status` and ensuring you receive an HTTP 200 response.	2
8443	TLS v1.2	VMware Tunnel Front-End	VMware Tunnel Back-End	Telnet from VMware Tunnel Front-End to the VMware Tunnel Back-End server on port	3
SaaS: 443 On-Prem: 2001	TLS v1.2	VMware Tunnel Back-End	Workspace ONE UEM Cloud Messaging Server	Verify by using `wget` to `https://<AWCM URL>:<port>/awcm/status` and ensuring you receive an HTTP 200 response.	2
80 or 443	TCP	VMware Tunnel Back-End	Internal websites/web apps		4

Table 1-8. VMware Tunnel Cascade Configuration (continued)

Port	Protocol	Source	Target/Destination	Verification	Note (See the Note section at the bottom of the page)
80, 443, any TCP	TCP	VMware Tunnel Back-End	Internal resources		4
80 or 443	HTTPS	VMware Tunnel Front-End and Back-End	Workspace ONE UEM REST API Endpoint ■ SaaS:`https://asXXX.awmdm.com` or `https://asXXX.airwatchportals.com` ■ On-Prem: Most commonly your DS or Console server	`curl –Ivv https://<API URL>/api/mdm/ping` The expected response is HTTP 401 unauthorized.	5

Table 1-9. VMware Tunnel Front-end and Back-end Configuration

Port	Protocol	Source	Target/Destination	Verification	Note (See the Note section at the bottom of the page)
SaaS: 443 On-Prem: 2001	HTTP or HTTPS	VMware Tunnel Front-End	Workspace ONE UEM Cloud Messaging Server	`curl –Ivv https://<AWCM URL>:<port>/awcm/status/ping` The expected response is HTTP 200 OK.	2
80 or 443	HTTPS or HTTPS	VMware Tunnel Back-End and Front-End	Workspace ONE UEM REST API Endpoint ■ SaaS:`https://asXXX.awmdm.com` or `https://asXXX.airwatchportals.com` ■ On-Prem: Most commonly your DS or Console server	`curl –Ivv https://<API URL>/api/mdm/ping` The expected response is HTTP 401 unauthorized. TheVMware Tunnel Endpoint requires access to the REST API Endpoint only during initial deployment.	5
2010 *	HTTPS	VMware Tunnel Front-end	VMware Tunnel Back-end	Telnet from VMware Tunnel Front-end to the VMware Tunnel Back-end server on port	3

Table 1-9. VMware Tunnel Front-end and Back-end Configuration (continued)

Port	Proto col	Source	Target/Destination	Verification	Note (See the Note section at the bottom of the page)
80, 443, any TCP	HTTP, HTTPS , or TCP	VMware Tunnel Back-end	Internal resources	Confirm that the VMware Tunnel can access internal resources over the required port.	4
514 *	UDP	VMware Tunnel	Syslog Server		
On-Prem: 2020	HTTPS	Workspace ONE UEM	VMware Tunnel Proxy	On-Premises users can test the connection using the `telnet` command :`telnet <Tunnel Proxy URL> <port>`	6

Note The following points are valid for the VMware Tunnel requirements.

* - This port can be changed if needed based on your environment's restrictions.

1   If port 443 is used, Per-App Tunnel will listen on port 8443.

> **Note** When VMware Tunnel and Content Gateway services are enabled on the same appliance, and TLS Port Sharing is enabled, the DNS names must be unique for each service. When TLS is not enabled only one DNS name can be used for both services as the port will differentiate the incoming traffic. (For Content Gateway, if port 443 is used, Content Gateway will listen on port 10443.)

2   For the VMware Tunnel to query the Workspace ONE UEM console for compliance and tracking purposes.

3   For VMware Tunnel Front-end topologies to forward device requests to the internal VMware Tunnel Back-end only.

4   For applications using VMware Tunnel to access internal resources.

5   The VMware Tunnel must communicate with the API for initialization. Ensure that there is connectivity between the REST API and the VMware Tunnel server. Navigate to **Groups & Settings > All Settings > System > Advanced > Site URLs** to set the REST API server URL. This page is not available to SaaS customers. The REST API URL for SaaS customers is most commonly your Console or Devices Services server URL.

6   This is required for a successful "Test Connection" to the VMware Tunnel Proxy from the Workspace ONE UEM console. The requirement is optional and can be omitted without loss of functionality to devices. For SaaS customers, the Workspace ONE UEM console might already have inbound connectivity to the VMware Tunnel Proxy on port 2020 due to the inbound Internet requirement on port 2020.

System Requirements for Deploying VMware Tunnel with Unified Access Gateway

To deploy VMware Tunnel with Unified Access Gateway, ensure that your system meets the following requirements:

Hypervisor Requirements

Unified Access Gateway that deploys the VMware Tunnel requires a hypervisor to deploy the virtual appliance. You must have a dedicated admin account with full privileges to deploy the OVF.

Supported Hypervisors

- VMware vSphere web client

  Note You must use specific versions of VMware products with specific versions of Unified Access Gateway. The Unified Access Gateway appliance must be deployed on a version of VMware vSphere that is the same as the version supported for the VMware products and versions respectively.

- Microsoft Hyper-V on Windows Server 2012 R2 or Windows Server 2016

Software Requirements

Ensure that you have the most recent version of Unified Access Gateway. VMware Tunnel supports backwards compatibility between Unified Access Gateway and the Workspace ONE UEM console. The backward compatibility allows you to upgrade your VMware Tunnel server shortly after upgrading your Workspace ONE UEM console. To ensure parity between Workspace ONE UEM console and VMware Tunnel, consider planning an early upgrade.

Hardware Requirements

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

To change the default settings, power off the VM in vCenter. Right-click the VM and select **Edit Settings**.

The default configuration uses 4 GB of RAM and 2 CPUs. You must change the default configuration to meet your hardware requirements. To handle all the device loads and maintenance requirements, consider running a minimum of two VMware Tunnel servers.

Table 1-10. Hardware Requirements

Number of Devices	Up to 40000	40000-80000	80000-120000	120000-160000
Number of Servers	2	3	4	5
CPU Cores	4 CPU Cores*	4 CPU Cores each	4 CPU Cores each	4 CPU Cores each

Table 1-10. Hardware Requirements (continued)

Number of Devices	Up to 40000	40000-80000	80000-120000	120000-160000
RAM (GB)	8	8	8	8
Hard Disk Space (GB)	10 GB for distro (Linux only) 400 MB for installer ~10 GB for log file space**			

*It is possible to deploy only a single VMware Tunnel appliance as part of a smaller deployment. However, consider deploying at least two load-balanced servers with four CPU Cores each regardless of the number of devices for uptime and performance purposes.

**10 GB for a typical deployment. Scale the log file size based on your log use and requirements for storing the logs.

Port Requirements for VMware Tunnel Proxy

VMware Tunnel Proxy can be configured using either of the following two configuration models:

- Basic Endpoint (single-tier) using a VMware Tunnel Proxy Endpoint

- Relay-Endpoint (multi-tier) using a VMware Tunnel Proxy Relay and VMware Tunnel Proxy Endpoint

Table 1-11. Port Requirements for VMware Tunnel Proxy Basic Endpoint Configuration

Source	Target or Destination	Protocol	Port	Verification	Notes
Devices (from Internet and Wi-Fi)	VMware Tunnel Proxy Endpoint	HTTPS	2020*	Run the following command after installation: `netstat -tlpn | grep [Port]`	Devices connect to the public DNS configured for VMware Tunnel over the specified port.
VMware Tunnel Proxy Endpoint	Workspace ONE UEM Cloud Messaging Server	HTTPS	SaaS:443 On-Premises:2001*	`curl -Ivv https://<AWCM URL>:<port>/ awcm/status/ ping` The expected response is `HTTP 200 OK`.	For the VMware Tunnel Proxy to query the Workspace ONE UEM console for compliance and tracking purposes. This needs to support a minimum of TLS 1.2.

Table 1-11. Port Requirements for VMware Tunnel Proxy Basic Endpoint Configuration (continued)

Source	Target or Destination	Protocol	Port	Verification	Notes
VMware Tunnel Proxy Endpoint	UEM REST API ■ SaaS‡: https://asXXX.awmdm.com or https://asXXX.airwatchportals.com ■ On-Premises†: Most commonly Device Services or Console server	HTTP or HTTPS	SaaS:443 On-Premises:2001*	`curl –Ivv https://<API URL>/api/mdm/ping` The expected response is HTTP 401 `unauthorized`	The VMware Tunnel Proxy must communicate with the UEM REST API for initialization. In the Workspace ONE UEM console, go to **Groups & Settings > All Settings > System > Advanced > Site URLs** to set the **REST API URL**. This page is not available to Workspace ONE UEM SaaS customers. For Workspace ONE UEM SaaS customers, the **REST API URL** is most commonly the **Console URL** or **Devices Services URL**.
VMware Tunnel Proxy Endpoint	Internal resources	HTTP, HTTPS, or TCP	80, 443, any TCP	Confirm that the VMware Tunnel Proxy Endpoint can access internal resources over the required port.	For applications using VMware Tunnel Proxy to access internal resources. Exact endpoints or ports are determined by where these resources are located.
VMware Tunnel Proxy Endpoint	Syslog Server	UDP	514*		
Workspace ONE UEM console	VMware Tunnel Proxy Endpoint	HTTPS	2020*	On-Premises† customers can test the connection using the telnet command: `telnet <Tunnel ProxyURL><port>`	This is required for a successful "Test Connection" to the VMware Tunnel Proxy Endpoint from the Workspace ONE UEM console.

Table 1-12. Port Requirements for VMware Tunnel Proxy Relay-Endpoint Configuration

Source	Target or Destination	Protocol	Port	Verification	Notes
Devices (from Internet and Wi-Fi)	VMware Tunnel Proxy Relay	HTTPS	2020*	Run the following command after installation: `netstat –tlpn	grep [Port]`	Devices connect to the public DNS configured for VMware Tunnel over the specified port.
VMware Tunnel Proxy Relay	Workspace ONE UEM Cloud Messaging Server	HTTP or HTTPS	SaaS:443 On-Premises:2001*	`curl –Ivv https://<AWCM URL>:<port>/awcm/status/ping` The expected response is HTTP 200 OK.	For the VMware Tunnel Proxy to query the Workspace ONE UEM console for compliance and tracking purposes. This needs to support a minimum of TLS 1.2.
VMware Tunnel Proxy Relay	UEM REST API ■ SaaS‡: https://asXXX.awmdm.com or https://asXXX.airwatchportals.com ■ On-Premises†: Most commonly Device Services or Console server	HTTP or HTTPS	SaaS:443 On-Premises:2001*	`curl –Ivv https://<API URL>/api/mdm/ping` The expected response is HTTP 401 unauthorized The VMware Tunnel Proxy Relay requires access to the UEM REST API only during initial deployment.	The VMware Tunnel Proxy must communicate with the UEM REST API for initialization. In the Workspace ONE UEM console, go to **Groups & Settings > All Settings > System > Advanced > Site URLs** to set the **REST API URL**. This page is not available to Workspace ONE UEM SaaS customers. For Workspace ONE UEM SaaS customers, the **REST API URL** is most commonly the **Console URL** or **Devices Services URL**.

Table 1-12. Port Requirements for VMware Tunnel Proxy Relay-Endpoint Configuration (continued)

Source	Target or Destination	Protocol	Port	Verification	Notes
VMware Tunnel Proxy Endpoint	UEM REST API ■ SaaS‡: https://asXXX.awmdm.com or https://asXXX.airwatchportals.com ■ On-Premises†: Most commonly Device Services or Console server	HTTP or HTTPS	SaaS:443 On-Premises:2001*	`curl –Ivv https://<API URL>/api/mdm/ping` The expected response is HTTP 401 unauthorized The VMware Tunnel Proxy Relay requires access to the UEM REST API only during initial deployment.	The VMware Tunnel Proxy must communicate with the UEM REST API for initialization. In the Workspace ONE UEM console, go to **Groups & Settings > All Settings > System > Advanced > Site URLs** to set the **REST API URL**. This page is not available to Workspace ONE UEM SaaS customers. For Workspace ONE UEM SaaS customers, the **REST API URL** is most commonly the **Console URL** or **Devices Services URL**.
VMware Tunnel Proxy Relay	VMware Tunnel Proxy Endpoint	HTTPS	2010*	Telnet from VMware Tunnel Proxy Relay to the VMware Tunnel Proxy Endpoint on port 2010.	To forward device requests from the Relay to the Endpoint server. This needs to support a minimum of TLS 1.2.
VMware Tunnel Proxy Endpoint	Internal resources	HTTP, HTTPS, or TCP	80, 443, any TCP	Confirm that the VMware Tunnel Proxy Endpoint can access internal resources over the required port.	For applications using VMware Tunnel Proxy to access internal resources. Exact endpoints or ports are determined by where these resources are located.

Table 1-12. Port Requirements for VMware Tunnel Proxy Relay-Endpoint Configuration (continued)

Source	Target or Destination	Protocol	Port	Verification	Notes
VMware Tunnel Proxy Endpoint	Syslog Server	UDP	514*		
Workspace ONE UEM console	VMware Tunnel Proxy Relay	HTTPS	2020*	On-Premises† customers can test the connection using the telnet command: `telnet <Tunnel ProxyURL><port>`	This is required for a successful "Test Connection" to the VMware Tunnel Proxy Relay from the Workspace ONE UEM console.

NOTES

- ▪ * This port can be changed based on your environment's restrictions.

- ▪ † On-Premises means the location of the Workspace ONE UEM console.

- ▪ ‡ For SaaS customers who need to whitelist outbound communication, refer to the VMware Knowledge Base article that lists up-to-date IP ranges: https://support.workspaceone.com/articles/115001662168-.

Port Requirements for VMware Per-App Tunnel

VMware Per-App Tunnel can be configured using either of the following two configuration models:

- ▪ Basic Endpoint (single-tier) using a VMware Per-App Tunnel Basic Endpoint

- ▪ Cascade (multi-tier) using a VMware Per-App Tunnel Front-End and VMware Per-App Tunnel Back-End

Table 1-13. Port Requirements for VMware Per-App Tunnel Basic Endpoint Configuration

Source	Destination	Protocol	Port	Verification	Notes
Devices (from Internet and Wi-Fi)	VMware Per-App Tunnel Basic Endpoint	TCP, UDP	8443*	Run the following command after installation: `netstat –tlpn | grep [Port]`	Devices connect to the public DNS configured for VMware Tunnel over the specified port. If 443 is used, Per-App Tunnel component listens on port 8443.
VMware Per-App Tunnel Basic Endpoint	Workspace ONE UEM Cloud Messaging Server	HTTPS	SaaS:443 On-Premises:2001*	Verify by using `wget` to `https://<AWCM URL>:<port>/awcm/status` and ensuring you receive an HTTP 200 response.	For the VMware Per-App Tunnel to query the Workspace ONE UEM console for compliance and tracking purposes. This needs to support a minimum of TLS 1.2.

Table 1-13. Port Requirements for VMware Per-App Tunnel Basic Endpoint Configuration (continued)

Source	Destination	Protocol	Port	Verification	Notes
VMware Per-App Tunnel Basic Endpoint	Internal websites/web apps/ resources	HTTP, HTTPS, or TCP	80, 443, any required TCP		For applications using VMware Per-App Tunnel to access internal resources. Exact endpoints or ports are determined by where these resources are located.
VMware Per-App Tunnel Basic Endpoint	UEM REST API ■ SaaS‡: https:// asXXX.awmdm.com or https:// asXXX.airwatchportals.com ■ On-Premises †: Most commonly Device Services or Console server	HTTP or HTTPS	80 or 443	`curl –Ivv https://<API URL>/api/mdm/ ping` The expected response is HTTP 401 unauthorized	The VMware Per-App Tunnel must communicate with the UEM REST API for initialization. In the Workspace ONE UEM console, go to **Groups & Settings > All Settings > System > Advanced > Site URLs** to set the **REST API URL**. This page is not available to Workspace ONE UEM SaaS customers. For Workspace ONE UEM SaaS customers, the **REST API URL** is most commonly the **Console URL** or **Devices Services URL**.

Table 1-14. Port Requirements for VMware Per-App Tunnel Cascade Configuration

Source	Destination	Protocol	Port	Verification	Notes
Devices (from Internet and Wi-Fi)	VMware Per-App Tunnel Front-End	TCP, UDP	8443*	Run the following command after installation: `netstat –tlpn | grep [Port]`	Devices connect to the public DNS configured for VMware Tunnel over the specified port. If 443 is used, Per-App Tunnel component listens on port 8443.
VMware Per-App Tunnel Front-End	Workspace ONE UEM Cloud Messaging Server	HTTPS	SaaS:443 On-Premises:2001*	Verify by using `wget` to `https://<AWCM URL>:<port>/awcm/status` and ensuring you receive an HTTP 200 response.	For the VMware Per-App Tunnel to query the Workspace ONE UEM console for compliance and tracking purposes. This needs to support a minimum of TLS 1.2.
VMware Per-App Tunnel Front-End	VMware Per-App Tunnel Back-End	TCP	8443	Telnet from VMware Per-App Tunnel Front-End to the VMware Per-App Tunnel Back-End on port 8443.	To forward device requests from the Front-End to the Back-End server. This needs to support a minimum of TLS 1.2.
VMware Per-App Tunnel Back-End	Workspace ONE UEM Cloud Messaging Server	HTTPS	SaaS:443 On-Premises:2001*	Verify by using `wget` to `https://<AWCM URL>:<port>/awcm/status` and ensuring you receive an HTTP 200 response.	For VMware Per-App Tunnel to query the Workspace ONE UEM console for compliance and tracking purposes. This needs to support a minimum of TLS 1.2.
VMware Tunnel Back-End	Internal websites/web apps/resources	HTTP, HTTPS, or TCP	80, 443, any required TCP		For applications using VMware Per-App Tunnel to access internal resources. Exact endpoints or ports are determined by where these resources are located.

Table 1-14. Port Requirements for VMware Per-App Tunnel Cascade Configuration (continued)

Source	Destination	Protocol	Port	Verification	Notes
VMware Per-App Tunnel Front-End	UEM REST API ■ SaaS‡: https://asXXX.awmdm.com or https://asXXX.airwatchportals.com ■ On-Premises †: Most commonly Device Services or Console server	HTTP or HTTPS	80 or 443	`curl –Ivv https://<API URL>/api/mdm/ping` The expected response is HTTP 401 `unauthorized`	The VMware Per-App Tunnel must communicate with the UEM REST API for initialization. In the Workspace ONE UEM console, go to **Groups & Settings > All Settings > System > Advanced > Site URLs** to set the **REST API URL**. This page is not available to Workspace ONE UEM SaaS customers. For Workspace ONE UEM SaaS customers, the **REST API URL** is most commonly the **Console URL** or **Devices Services URL**.
VMware Per-App Tunnel Back-End	UEM REST API ■ SaaS‡: https://asXXX.awmdm.com or https://asXXX.airwatchportals.com ■ On-Premises †: Most commonly Device Services or Console server	HTTP or HTTPS	80 or 443	`curl –Ivv https://<API URL>/api/mdm/ping` The expected response is HTTP 401 `unauthorized`	The VMware Per-App Tunnel must communicate with the UEM REST API for initialization. In the Workspace ONE UEM console, go to **Groups & Settings > All Settings > System > Advanced > Site URLs** to set the **REST API URL**. This page is not available to Workspace ONE UEM SaaS customers. Workspace ONE UEM SaaS customers, the **REST API URL** is most commonly the **Console URL**

Table 1-14. Port Requirements for VMware Per-App Tunnel Cascade Configuration (continued)

Source	Destination	Protocol	Port	Verification	Notes
					or **Devices Services URL**.

NOTES

- ■ * This port can be changed based on your environment's restrictions.

- ■ † On-Premises means the location of the Workspace ONE UEM console.

- ■ ‡ For SaaS customers who need to whitelist outbound communication, refer to the VMware Knowledge Base article that lists up-to-date IP ranges: https://support.workspaceone.com/articles/115001662168-.

For SaaS customers who need to whitelist outbound communication, refer to the following Knowledge Base article that lists up-to-date IP ranges that VMware currently owns: VMware Workspace ONE IP ranges for SaaS data centers.

Network Interface Connection Requirements

You can use one, two, or three network interfaces. Each should have a separate IP address. Many secure DMZ implementations use separated networks to isolate the different traffic types.

Configure the virtual appliance according to the network design of the DMZ in which it is deployed. Consult your network admin for information regarding your network DMZ.

- ■ With one network interface, 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.

- ■ With a three network interface, external, internal, and management traffic each have their own subnet.

Note With multiple network interface deployments, each network interface must be on a separate subnet.

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 1-1. MultipleUnified Access Gateway Appliances Behind a Load Balancer
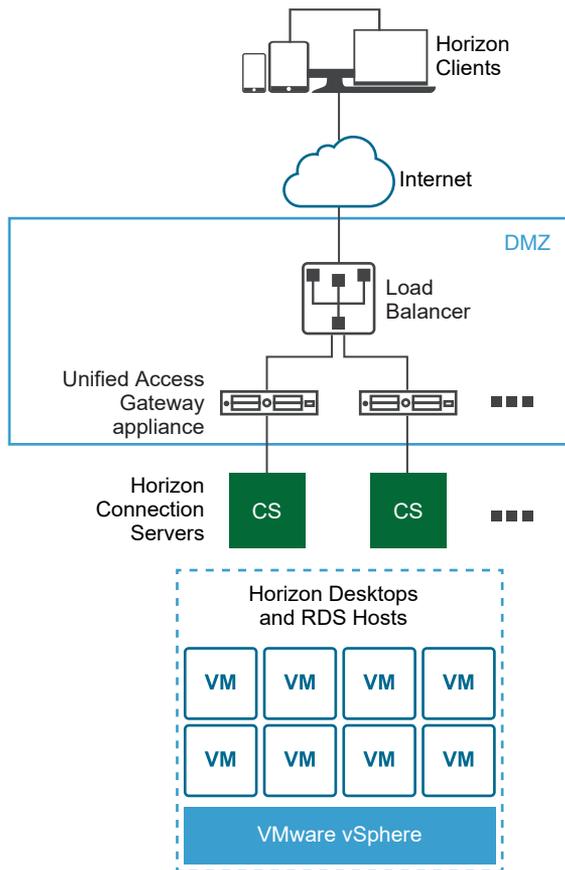
Horizon Protocols

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 4172, UDP 4172)

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.

Load Balancing Considerations for Content Gateway and Tunnel Proxy

Keep the following considerations in mind when you use a load balancer with Content Gateway and Tunnel Proxy:

- Configure the load balancers to Send Original HTTP Headers to avoid device connectivity problems. Content Gateway and Tunnel Proxy use information in the request's HTTP header to authenticate devices.

- The Per-App Tunnel component requires authentication of each client after a connection is established. Once connected, a session is created for the client and stored in memory. The same session is then used for each piece of client data so the data can be encrypted and decrypted using the same key. When designing a load balancing solution, the load balancer must be configured with IP/session-based persistence enabled. An alternative solution might be to use DNS round robin on the client side, which means the client can select a different server for each connection.

Health Monitoring

A load balancer monitors the health of each Unified Access Gateway appliance by periodically sending an `HTTPS GET /favicon.ico` request. For example, `https://uag1.myco-dmz.com/favicon.ico`. This monitoring is configured on the load balancer. It will perform this `HTTPS GET` and expect a "`HTTP/1.1 200 OK`" response from Unified Access Gateway to know that it is "healthy". If it gets a response other than "`HTTP/1.1 200 OK`" response or does not get any response, it will mark the particular Unified Access Gateway appliance as down and will not attempt to route client requests to it. It will continue to poll so that it can detect when it is available again.

Unified Access Gateway can be put into "quiesce" mode after which it will not respond to the load balancer health monitoring request with a "`HTTP/1.1 200 OK`" response. Instead it will respond with "`HTTP/1.1 503`" to indicate that the Unified Access Gateway service is temporarily unavailable. This setting is often used prior to scheduled maintenance, planned reconfiguration or planned upgrade of an Unified Access Gateway appliance. In this mode, the load balancer will not direct new sessions to this appliance because it will be marked as unavailable, but can allow existing sessions to continue until the user disconnects or the maximum session time is reached. Consequently this operation will not disrupt existing user sessions. The appliance will then be available for maintenance after a maximum of the overall session timer, which is typically 10 hours. This capability can be used to perform a rolling upgrade of a set of Unified Access Gateway appliances in a strategy resulting in zero user downtime for the service.

Unified Access Gateway High Availability

Unified Access Gateway for end-user computing products and services needs high availability for Workspace ONE and VMware Horizon on-prem deployments. However, using third-party load balancers adds to the complexity of the deployment and troubleshooting process. This solution reduces the need for a third-party load balancer in the DMZ front-ending Unified Access Gateway .

Note   This solution is not a generic purpose load balancer.

Unified Access Gateway continues to support third-party load balancers in front, for users who prefer this mode of deployment. For more information, see Unified Access Gateway Load Balancing Topologies. Unified Access Gateway High Availability is not supported for Amazon AWS and Microsoft Azure deployments.

Implementation

Unified Access Gateway requires the IPv4 virtual IP address and a group ID from the administrator. Unified Access Gateway assigns the virtual IP address to only one of the nodes in the cluster that is configured with the same Virtual IP address and Group ID. If the Unified Access Gateway holding the virtual IP address fails, the Virtual IP address gets reassigned automatically to one of the nodes available in the cluster. The HA and load distribution occurs among the nodes in the cluster that is configured with the same Group ID.

Multiple connections originating from the same source IP address are sent to the same Unified Access Gateway that processes the first connection from that client for Horizon and web reverse proxy. This solution supports 10,000 concurrent connections in the cluster.

Note Session affinity is required for these cases.

For VMware Tunnel (Per-App VPN) and Content Gateway services, HA and load distribution is done using least connection algorithm.

Note These connections are stateless and session affinity is not required.

Mode and Affinity

Different Unified Access Gateway services require different algorithms.

- For VMware Horizon and Web Reverse Proxy - Source IP Affinity is used with the round robin algorithm for distribution.

- For VMware Tunnel (Per-App VPN) and Content Gateway - There is no session affinity and least connection algorithm is used for distribution.

Methods that are used for distributing the incoming traffic:

1   Source IP Affinity: Maintains the affinity between the client connection and Unified Access Gateway node. All connections with the same source IP address are sent to the same Unified Access Gateway node.

2   Round Robin mode with high availability: Incoming connection requests are distributed across the group of Unified Access Gateway nodes sequentially.

3   Least Connection mode with high availability: A new connection request is sent to the Unified Access Gateway node with the fewest number of current connections from the clients.

Note Source IP affinity works only if the IP of the incoming connection is unique for each client connection. Example: If there is a network component, like a SNAT gateway between the clients and Unified Access Gateway then the source IP affinity does not work as the incoming traffic from multiple different clients to Unified Access Gateway have the same source IP address.

Note Virtual IP address must belong to same subnet as the `eth0` interface.

Prerequisites

- The Virtual IP address used for HA must be unique and available. Unified Access Gateway does not validate if it is unique during configuration. The IP address might show as assigned but it might not be reachable if a VM or physical machine is associated to the IP address.

- The Group ID must be unique in a given subnet. If the Group ID is not unique, an inconsistent virtual IP address might get assigned in the group. For example, two or more Unified Access Gateway nodes might end up trying to acquire the same virtual IP address. It might cause the Virtual IP address to get toggled between multiple Unified Access Gateway nodes.

- To set up HA for Horizon or web reverse proxy, ensure that the TLS server certificate on all the nodes of Unified Access Gateway are same.

Limitations

- IPv4 is supported for floating Virtual IP address. IPv6 is not supported.

- Only TCP high availability is supported.

- UDP high availability is not supported.

- With the VMware Horizon use case, only XML API traffic to Horizon Connection Server uses high availability. High availability is not used to distribute load for the protocol (display) traffic such as Blast, PCoIP, RDP. Therefore, the individual IP addresses of Unified Access Gateway nodes must also be accessible to VMware Horizon clients in addition to the Virtual IP address.

Required Configuration for HA on each Unified Access Gateway

For configuring HA on Unified Access Gateway, see, Configure High Availability Settings.

Configure High Availability Settings

To use the Unified Access Gateway high availability, you enable and configure the **High Availability Settings** in the admin user interface.

Procedure

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

2   In the **Advanced Settings** section, click the **High Availability Settings** gearbox icon.

3   In the **High Availability Settings** page, change **DISABLED** to **ENABLED** to enable high availability.

4 Configure the parameters.

| Option	Description
Virtual IP Address	A valid virtual IP address used by HA.
	Note The Virtual IP address used for HA must be unique and available. If a unique address it not set, then the IP address might show as assigned but it might not be reachable if a VM or physical machine is associated to the IP address.
Group ID	The Group ID for the HA. Enter a numerical value between 1-255.
	Note The Group ID must be unique in a given subnet. If a unique Group ID is not set, the effect might result in an inconsistent virtual IP address assigned in the group. For example, if an IP address of two or more gateways on Unified Access Gateway might end up trying to acquire the same virtual IP address.

5 Click **Save**.

- The different states of **High Availability Settings** indicate the following:

- **Not Configured**: Indicates **High Availability settings** are not configured.

- **Processing**: Indicates **High Availability Settings** are being processed to take effect.

- **Master**: Indicates that the node is elected as the master in the cluster and it distributes traffic.

- **Backup**: Indicates that the node is in the backup state in the cluster.

- **Fault**: Indicates that the node might have faults with the HA proxy configuration.

Unified Access Gateway Configured with Horizon

Multiple Unified Access Gateway are configured with the same Horizon settings and High Availability is enabled on each Unified Access Gateway .

There is a common external hostname used for XML API protocol. This common external hostname is mapped to the floating IP configured in HA settings on the nodes of Unified Access Gateway. The desktop traffic does not use high availability and the load is not distributed, hence this solution requires N + 1 VIP for Horizon where N is the number of Unified Access Gateway nodes deployed. On each Unified Access Gateway, the Blast, PCoIP, and Tunnel external URL must be external IP addresses or host names mapping to the corresponding Unified Access Gateway eth0 IP address. Clients that connect through a poor network and use the UDP connection for XML API arrives at the same Unified Access Gateway that was handed the first UDP XML API connection.

Figure 1-2. Unified Access Gateway Configured with Horizon
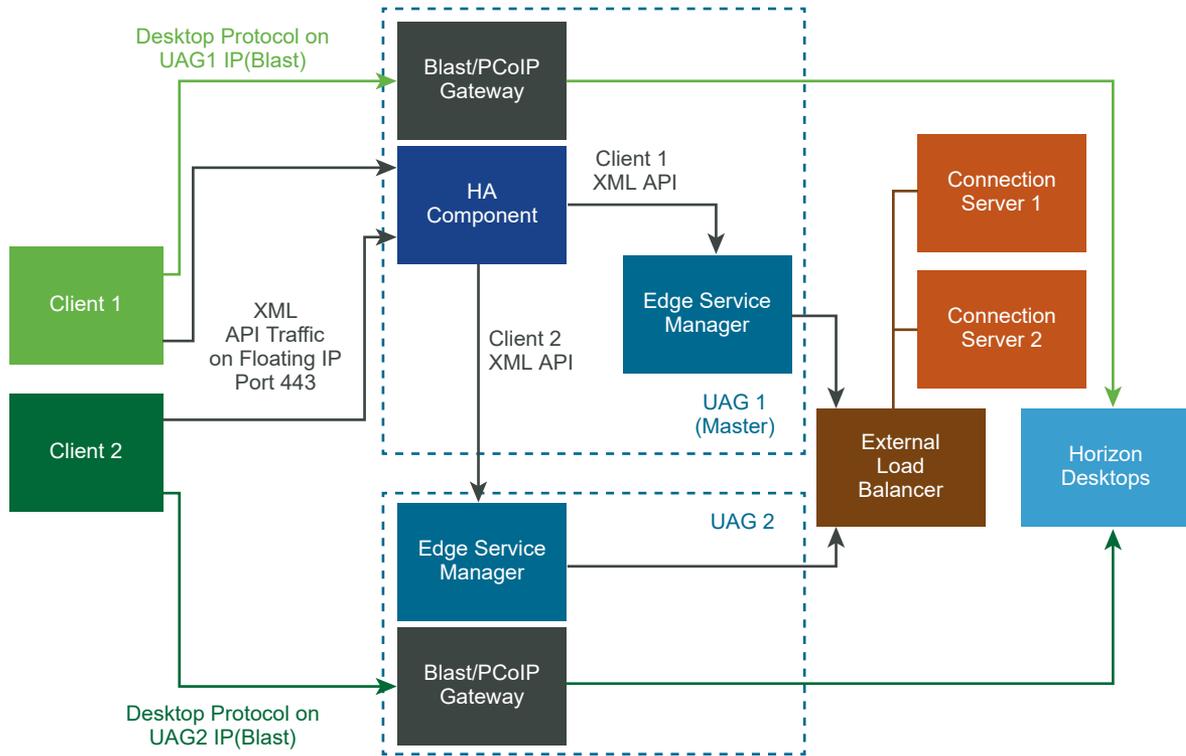
Mode and Affinity: The affinity is based on the source IP address. The first connection from the client is distributed using round robin mechanism. However subsequent connections from the same client are sent to the same Unified Access Gateway which handled the first connection.

VMware Tunnel (Per-App VPN) Connection with Basic Configuration

VMware Tunnel (Per-App VPN) is configured with basic settings in the Workspace ONE UEM console.

The Tunnel server hostname configured in the Workspace ONE UEM console for VMware Tunnel (Per-App VPN) settings resolves to the floating IP address configured for HA in Unified Access Gateway. The connections on this floating IP address are distributed among the configured nodes on Unified Access Gateway.

Figure 1-3. VMware Tunnel (Per-App VPN) Connection with Basic Configuration
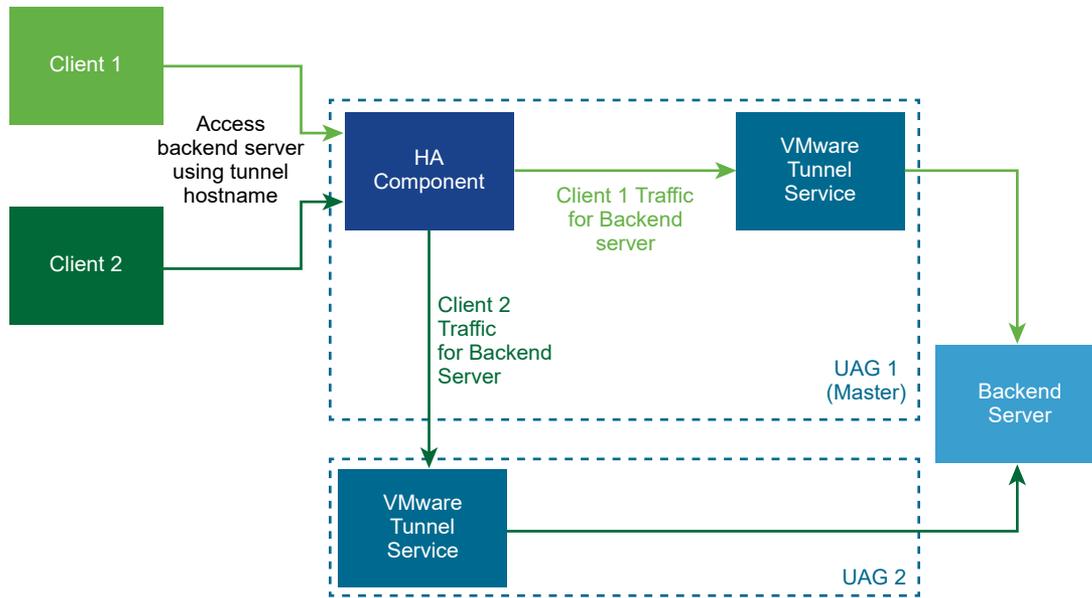
Mode and Affinity: Least connections algorithm is used for HA and load distribution. A new request is sent to the server with the fewest number of current connections to clients. Session affinity is not required as they are stateless connections.

VMware Tunnel (Per-App VPN) Connections in Cascade Mode

VMware Tunnel (Per-App VPN) is configured with cascade settings in the Workspace ONE UEM console.

Two Tunnel server host names are configured in the Workspace ONE UEMconsole for the front-end and for the back-end. We can deploy two sets of nodes on Unified Access Gateway for front-end and back-end respectively.

The front-end nodes on Unified Access Gateway are configured with a front-end Tunnel server hostname. The HA settings on front-end nodes on Unified Access Gateway are configured with an external floating IP address. The front-end Tunnel server hostname gets resolved to the external floating IP address. The connections on this external floating IP address are distributed among the front-end nodes on Unified Access Gateway.

The back-end nodes on Unified Access Gateway are configured with the back-end Tunnel server hostname. The HA settings on back-end nodes on Unified Access Gateway are configured with an internal floating IP address. The VMware Tunnel (Per-App VPN) service on front-end nodes on Unified Access Gateway forwards the traffic to back-end using the back-end tunnel server hostname. The back-end Tunnel server hostname gets resolved to the internal floating IP address. The connections on this internal floating IP address are distributed among the back-end nodes on Unified Access Gateway.

Figure 1-4. VMware Tunnel (Per-App VPN) Connections in Cascade Mode
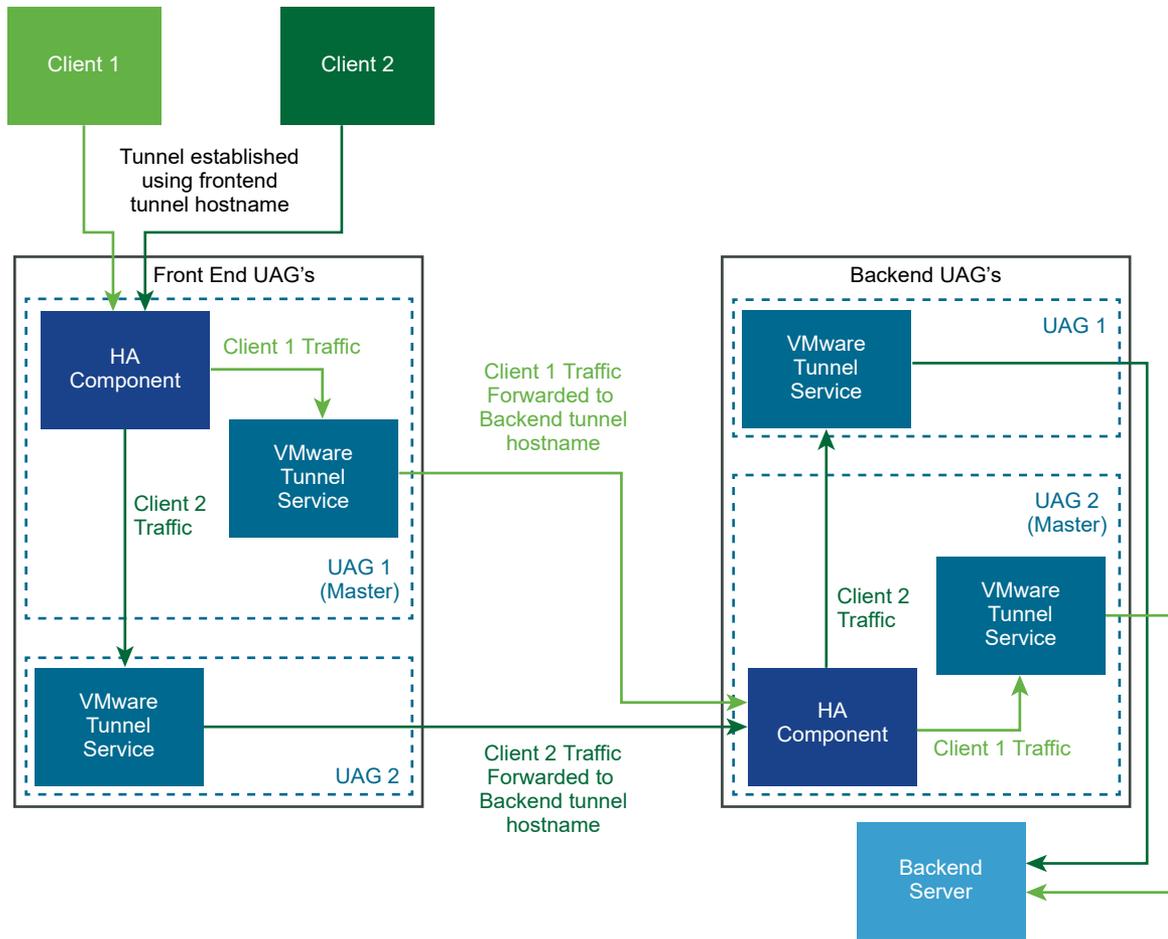
Mode and Affinity: Least connections algorithm is used for HA and load distribution. A new request is sent to the server with the fewest number of current connections to clients. Session affinity is not required as they are stateless connections.

Content Gateway Basic Configuration

Content Gateway is configured with Basic settings in the Workspace ONE UEM console.

The Content Gateway server host name configured in the Workspace ONE UEM console for Content Gateway settings resolves to the floating IP address configured for HA in Unified Access Gateway. The connections on this floating IP are load balanced among the configured nodes on Unified Access Gateway.

Figure 1-5. Content Gateway Basic Configuration
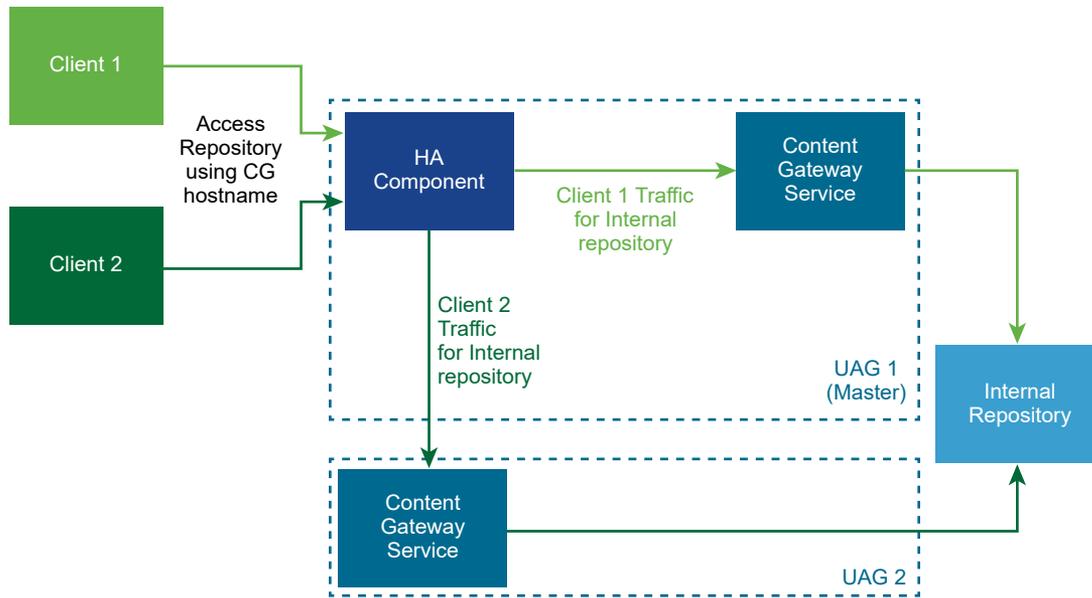
Mode and Affinity: Least connections algorithm is used for HA and load distribution. A new request is sent to the server with the fewest number of current connections to clients. Session affinity is not required as they are stateless.

Content Gateway with Relay and Endpoint Configuration

Content Gateway is configured with Relay and Endpoint configuration in the Workspace ONE UEM console.

Two Content Gateway server host names are configured in the Workspace ONE UEM console for Relay and Endpoint. Two sets of nodes on Unified Access Gateway are deployed for Relay and Endpoint.

The Relay nodes on Unified Access Gateway are configured with the Relay Content Gateway server hostname. The HA settings on Relay nodes on Unified Access Gateway are configured with an external floating IP address. The Relay Content Gateway server hostname gets resolved to the external floating IP address. The connections on this external floating IP are load balanced among the Relay nodes on Unified Access Gateway.

The Endpoint nodes onUnified Access Gateway are configured with the Endpoint Tunnel server hostname. The HA settings on Endpoint nodes on Unified Access Gateway are configured with an internal floating IP address. The Content Gateway service on the front end Unified Access Gateway forwards the traffic to Endpoint using the Endpoint Content Gateway server hostname. The Endpoint Content Gateway server hostname gets resolved to the internal floating IP address. The connections on this internal floating IP address are load balanced among the Endpoint nodes onUnified Access Gateway.

Figure 1-6. Content Gateway with Relay and Endpoint Configuration
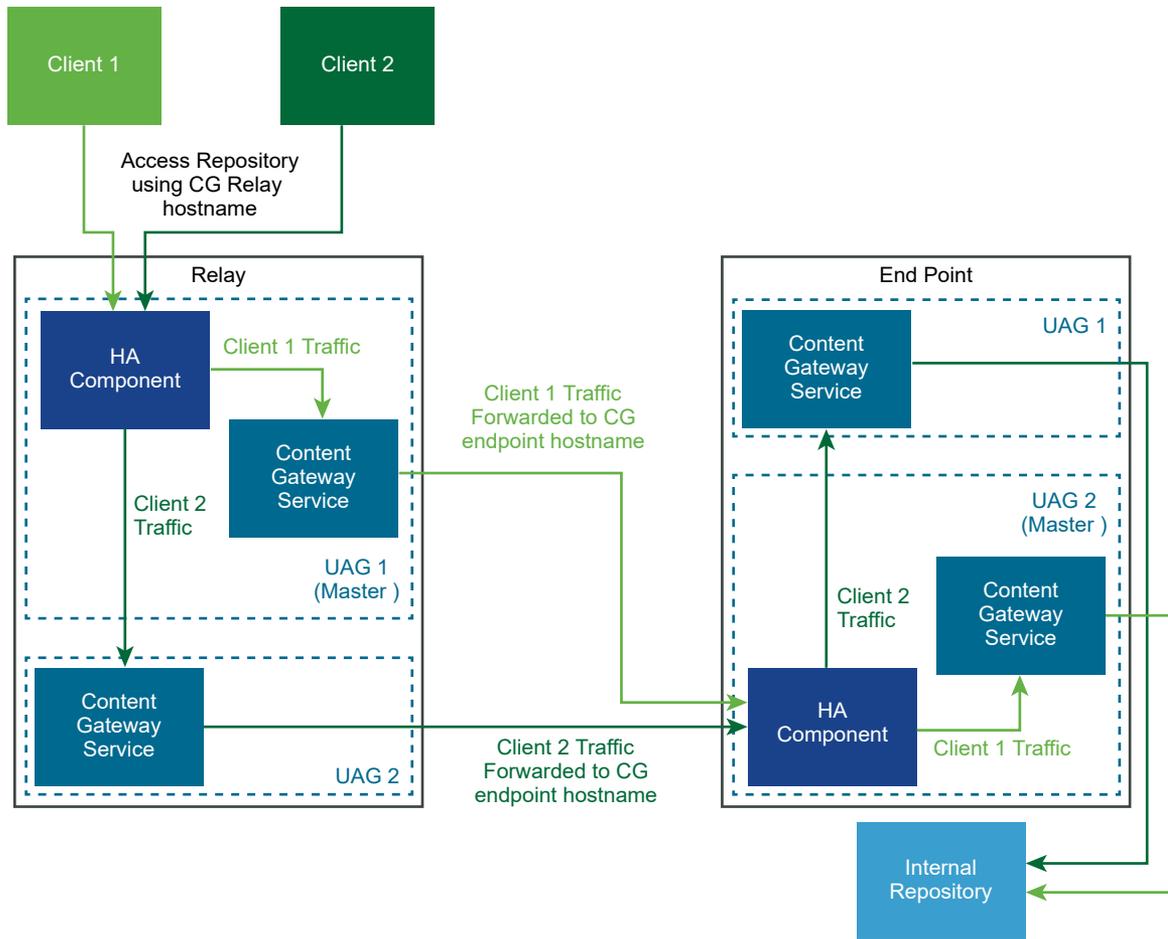
Mode and Affinity: Least connections algorithm is used for HA and load distribution. A new request is sent to the server with the fewest number of current connections to clients. Session affinity is not required as they are stateless connections.

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 1-7. Unified Access Gateway Single NIC Option
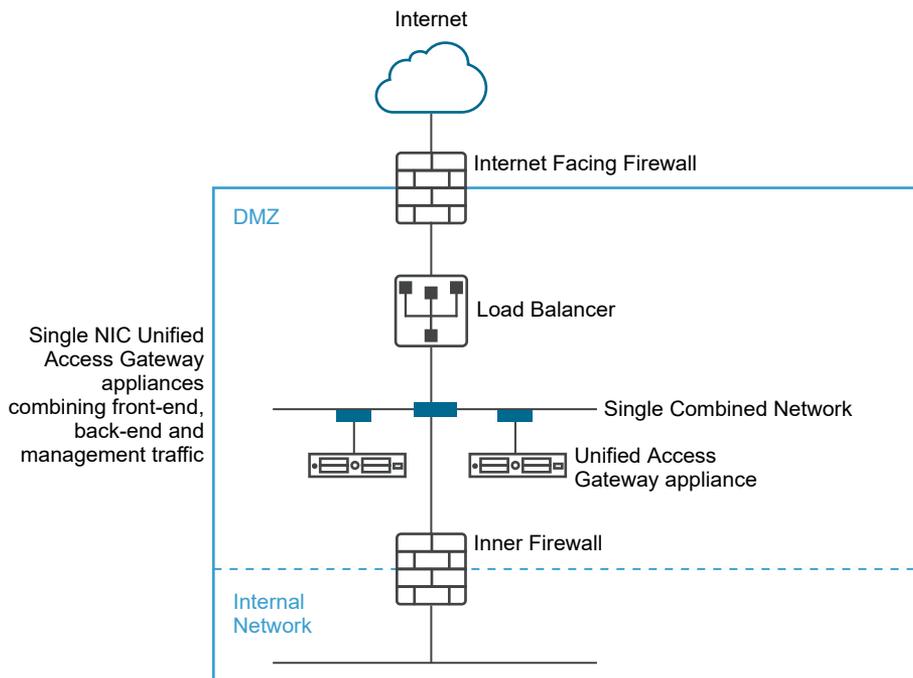
Separating Unauthenticated User Traffic from Back-End and Management Traffic

An alternative option 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 1-8. Unified Access Gateway Two NIC Option
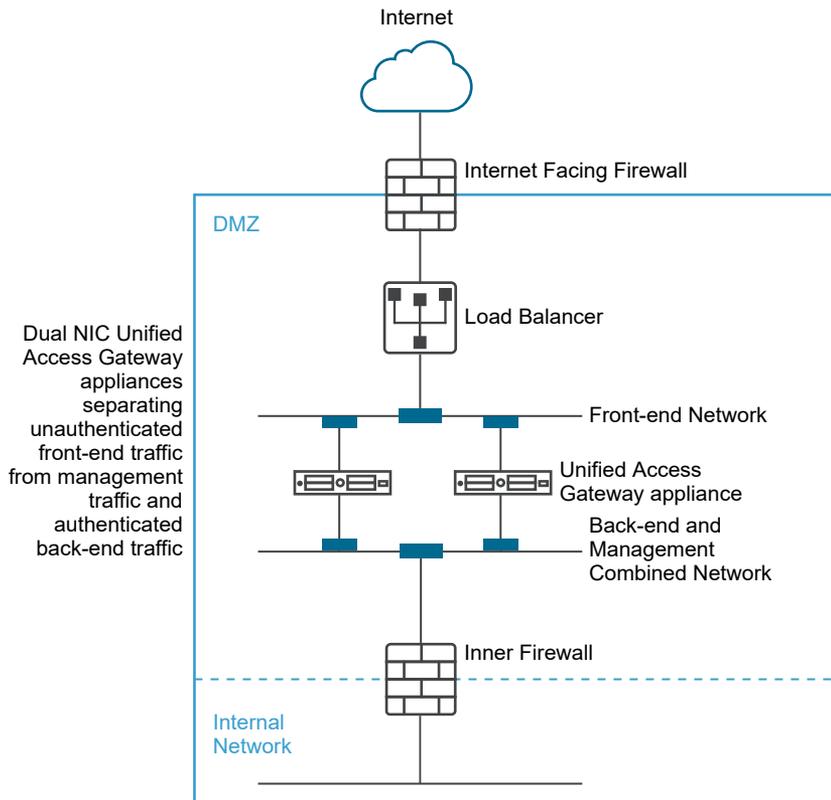
In a two NIC deployment, Unified Access Gateway must authorize the traffic going to the internal network through the inner firewall. Unauthorized traffic is not on this back-end network. Management traffic such as the REST API for Unified Access Gateway is only on this second network

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 1-9. Unified Access Gateway Three NIC Option
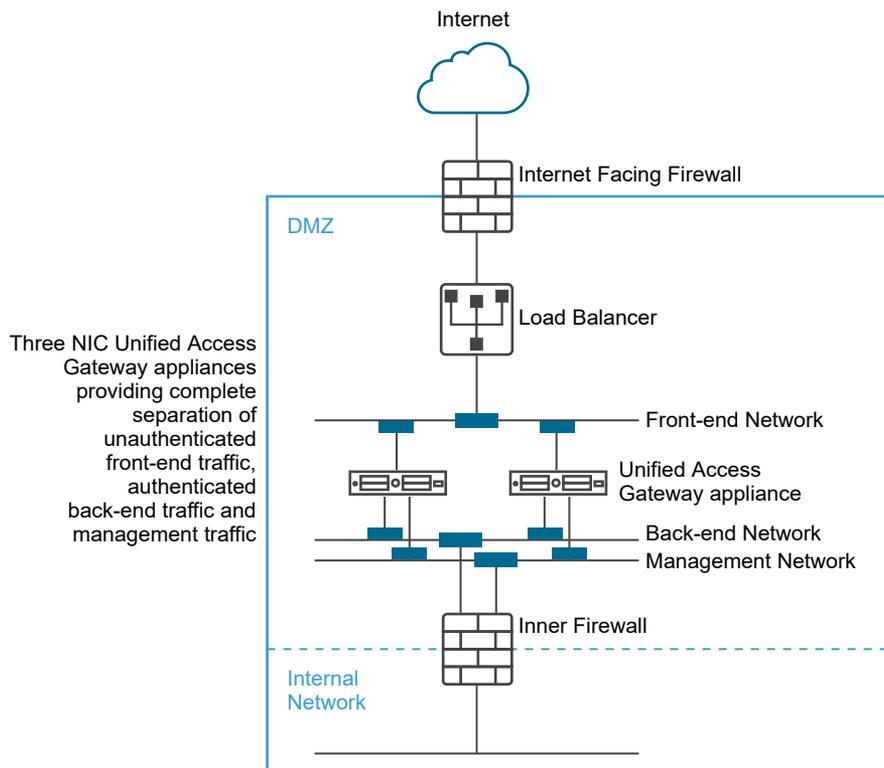
Upgrade with Zero Downtime

Zero downtime upgrade enables you to upgrade Unified Access Gateway with no downtime for the users.

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://UAG-IP-Address: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://UAG-IP-Address:443/favicon.ico`. Doing so will lead to incorrect status response and resource leaks.

  - If **High Availability** setting is enabled, then **Quiesce Mode (zero downtime)** applies to Web Reverse Proxy and Horizon only.

  - If third party load balancers are used, then **Quiesce Mode (zero downtime)** is applicable if they are configured to perform health check using GET `/favicon.ico`.

Procedure

1 In the admin UI Configure Manually 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 the next Unified Access Gateway appliance.

What to do next

- For a vSphere deployment:

  a Back up the JSON file by exporting the file.

  b Delete the old Unified Access Gateway appliance.

  c Deploy the new version of Unified Access Gateway appliance.

  d Import the JSON file you exported earlier.

- For a PowerShell deployment:

  a Delete the Unified Access Gateway appliance.

b Redeploy the Unified Access Gateway with the same INI file that was used during the first deployment. See Using PowerShell to Deploy the Unified Access Gateway Appliance.

Note If you see a Tunnel Server certificate error message after re-enabling the load balancer, apply the same SSL server certificate and private key PEM files that was used earlier on the Unified Access Gateway appliance. This is required because the JSON or INI file cannot contain private keys associated with an SSL server certificate since private keys cannot be exported, due to security reasons. With a PowerShell deployment, it is done automatically and you do not need to reapply the certificate.

Deploying Unified Access Gateway Without Network Protocol Profile (NPP)

The latest release of Unified Access Gateway does not accept netmask or prefix and default gateway settings from Network Protocol Profile.

You must provide this networking information while deploying your Unified Access Gateway instance.

In the case of static deployment, when configuring your Unified Access Gateway instance, specify the IPv4 or IPv6 address, the netmask or prefix for the respective NICs, and the IPv4/IPv6 default gateway. If you do not provide this information, it defaults to DHCPV4+DHCPV6 for the IP address allocation.

Note the following when configuring the networking properties:

- If you select STATICV4 for the `IPMode` of a NIC, you must specify the IPv4 address and netmask for that NIC.

- If you select STATICV6 for the `IPMode` of a NIC, you must specify the IPv6 address netmask for that NIC.

- If you select both STATICV4 and STATIC V6 for the `IPMode` of a NIC, you must specify the IPv4 and IPv6 address and netmask for that NIC.

- If you do not provide the address and netmask information, the values are allocated by DHCP server.

- IPv4 and IPv6 default gateway properties are optional and must be specified if Unified Access Gateway needs to communicate to an IP address that is not on a local segment of any NIC in Unified Access Gateway.

See Deploy Unified Access Gateway Using the OVF Template Wizard for more information about configuring networking properties.

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

<div style="text-align: right">2</div>

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

Note In both the above methods of deployment, if you do not provide the Admin UI password, you cannot add an Admin UI user later to enable access to either Admin UI or API. If you want to do so, you must redeploy your Unified Access Gateway instance with a valid password.

This chapter includes the following topics:

- Using the OVF Template Wizard to Deploy Unified Access Gateway
- Configuring Unified Access Gateway From the Admin Configuration Pages
- Update SSL Server Signed Certificates

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 version of the OVA supports the following Edge services:

- Horizon (pass-through auth only)

- VMware Per-App Tunnel

Important   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.

Unified Access Gateway Sizing Options

To simplify the deployment of the Unified Access Gateway appliance as the Workspace ONE security gateway, sizing options are added to the deployment configurations in the appliance. The deployment configuration offers a choice between a Standard or a Large virtual machine.

- **Standard:** This configuration is recommended for Horizon deployment supporting up to 2000 Horizon connections, aligned with the Connection Server capacity. It is also recommended for Workspace ONE UEM Deployments (mobile use cases) up to 10,000 concurrent connections.

- **Large:** This configuration is recommended for Workspace ONE UEM Deployments, where Unified Access Gateway needs to support over 50,000 concurrent connections. This size allows Content Gateway, Per App Tunnel and Proxy, and Reverse Proxy to use the same Unified Access Gateway appliance.

- **Extra Large**: This configuration is recommended for Workspace ONE UEM Deployments. This size allows Content Gateway, Per App Tunnel and Proxy, and Reverse Proxy to use the same Unified Access Gateway appliance.

- **Note**   VM options for Standard, Large, and Extra Large deployments:

  - Standard - 2 core and 4GB RAM

  - Large - 4 core and 16 GB RAM

  - Extra Large - 8 core and 32 GB RAM

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 website 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.

- In case of a Hyper-V deployment, and if you are upgrading Unified Access Gateway with static IP, delete the older appliance before deploying the newer instance of Unified Access Gateway.

- To upgrade your older appliance to a new instance of Unified Access Gateway with zero downtime for users, see the Upgrade with Zero Downtime section.

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 prompts and take the following guidelines into consideration as you complete the wizard. Both ESXi and Hyper-V deployments have two options to assign the IP assignment for Unified Access Gateway. If you are upgrading, then for Hyper-V, delete the old box with the same IP address before deploying the box with the new address. For ESXi, you can turn off the old box and deploy a new box with same IP address using static assignment.

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 or IPV6 network, you can use one, two, or three network interfaces (NICs). 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. Along with the number of NICs, you can also choose **Standard** or **Large** deployment options for Unified Access Gateway. **Note** VM options for **Standard** and **Large** deployments: ■ **Standard** - 2 core and 4GB RAM ■ **Large** - 4 core and 16 GB RAM
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.

Option	Description
Setup Networks/Network Mapping	If you are using a 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 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.
	b If you are using more than one NIC, select the next row **ManagementNetwork**, select the destination network, and then you can enter the IP addresses for the DNS server, gateway, and netmask for that network.
	If you are using only one NIC, all the rows are mapped to the same network.
	c If you have a third NIC, also select the third row and complete the settings.
	If you are using only two NICs, for this third row **BackendNetwork**, select the same network that you used for **ManagementNetwork**.
	Note Ignore the **IP protocol** drop-down menu if it is displayed, and do not make any selection here. The actual selection of IP protocol (IPv4/IPv6/both) depends on what IP mode is specified for IPMode for NIC 1 (eth0), NIC 2 (eth1), and NIC 3 (eth2) when customizing Networking Properties.

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. For each of the NICs, for STATICV4, you must enter the IPv4 address for the NIC. For STATICV6, you must enter the IPv6 address for the NIC. If you leave the text boxes empty, the IP address allocation defaults to DHCPV4+DHCPV6.
	Important The latest release of Unified Access Gateway does not accept netmask or prefix values and default gateway settings from the Network Protocol Profile (NPP). To configure Unified Access Gateway with static IP allocation, you must configure the netmask/prefix under network properties. These values do not be populated from NPP.
	IPMode for NIC1 (eth0): STATICV4/STATICV6/DHCPV4/DHCPV6/ AUTOV6/STATICV4+STATICV6/STATICV4+DHCPV6/ STATICV4+AUTOV6/DHCPV4+AUTOV6/DHCPV4+STATICV6/ DHCPV4+DHCPV6/DHCPV4+AUTOV6 . **IPMode for NIC2(eth1): STATICV4/STATICV6/DHCPV4/DHCPV6/ AUTOV6/STATICV4+STATICV6/STATICV4+DHCPV6/ STATICV4+AUTOV6/DHCPV4+AUTOV6/DHCPV4+STATICV6/ DHCPV4+DHCPV6/DHCPV4+AUTOV6** . **IPMode for NIC3 (eth2): STATICV4/STATICV6/DHCPV4/DHCPV6/ AUTOV6/STATICV4+STATICV6/STATICV4+DHCPV6/ STATICV4+AUTOV6/DHCPV4+AUTOV6/DHCPV4+STATICV6/ DHCPV4+DHCPV6/DHCPV4+AUTOV6** . **Comma-separated list of forward rules in the form {tcp|udp}/listening-port-number/destination-ip-address:destination-port-nu**. For example, for IPv4, `tcp/5262/10.110.92.129:9443, tcp/5263/10.20.30.50:7443`. **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**. For example, `20.2.0.0/16  10.2.0.1,20.9.0.0/16 10.2.0.2,10.2.0.1/32` **Note** If **ipv4-gateway-address** is not specified, then the respective route that is added has a gateway of 0.0.0.0 **NIC 1 (eth0) IPv6 address**. Enter the IPv6 address for the NIC if you entered STATICV6 for the NIC mode. **NIC 1 (eth0) IPv4 Netmask**. Enter the IPv4 netmask for the NIC. **NIC 1 (eth0) IPv6 Prefix**. Enter the IPv6 prefix for the NIC. **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` **IPv4 Default Gateway**. Enter a IPv4 default gateway if Unified Access Gateway needs to communicate to an IP address that is not on a local segment of any NIC in Unified Access Gateway.

Option	Description
	■ **IPv6 Default Gateway**. Enter a IPv6 default gateway if Unified Access Gateway needs to communicate to an IP address that is not on a local segment of any NIC in Unified Access Gateway.
	■ **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**. For example, `20.2.0.0/16 10.2.0.1,20.9.0.0/16 10.2.0.2,10.2.0.1/32`
	Note If **ipv4-gateway-address** is not specified, then the respective route that is added has a gateway of 0.0.0.0
	■ **NIC 2 (eth1) IPv6 address**. Enter the IPv6 address for the NIC if you entered STATICV6 for the NIC mode.
	■ **NIC 2 (eth1) IPv4 Netmask**. Enter the IPv4 netmask for this NIC.
	■ **NIC 2 (eth1) IPv6 Prefix**. Enter the IPv6 prefix for this NIC.
	■ **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**. For example, `20.2.0.0/16 10.2.0.1,20.9.0.0/16 10.2.0.2,10.2.0.1/32`
	Note If **ipv4-gateway-address** is not specified, then the respective route that is added has a gateway of 0.0.0.0
	■ **NIC 3 (eth2) IPv6 address**. Enter the IPv6 address for the NIC if you entered STATICV6 for the NIC mode.
	■ **NIC 3 (eth2) IPv4 Netmask**. Enter the IPv4 netmask for this NIC.
	■ **NIC 3 (eth2) IPv6 Prefix**. Enter the IPv6 prefix for this NIC.
	■ **VM root user password**. Enter the password for the root user to log in to the VM console.
	■ **Admin UI password**. Enter the password for the admin user to configure Unified Access Gateway from the Admin UI and also access the REST APIs.
	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.

Results

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`.

  Important You must complete the Unified Access Gateway configuration post-deployment using the Admin UI. If you do not provide the Admin UI password, you cannot add an Admin UI user later to enable access to either the Admin UI or the API. You must redeploy your Unified Access Gateway instance with a valid Admin UI password if you want to add an Admin UI user.

  Note If you are not able to access the Admin UI login 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"`.

  Note After powering on the appliance for the first time post deployment, you must not shut down or reboot the appliance until the appliance boots completely for the first time.

- If you have deployed using vSphere or PowerShell, perform a health check and ensure that the newly deployed instance returns a 200 OK response.

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 When you launch the Unified Access Gateway Admin console for the first time, you are prompted to change the password you set when you deployed the appliance.

The General Settings page and Advanced Settings page 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 called 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

- Account Settings

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

- Download Unified Access Gateway log 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
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.
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. Maximum number of two URLs can be provided. URLs are separated by a comma. Example: `syslog://server1.example.com:514, syslog://server2.example.com:514`
Syslog Audit URL	Enter the Syslog server URL that is used for logging Unified Access Gateway audit events. This value can be a URL or a host name or IP address. If you do not set the syslog server URL, no audit events are logged. Maximum number of two URLs can be provided. URLs are separated by a comma. Example: `syslog://server1.example.com:514, syslog://server2.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**.

Option	Default Value and Description
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.
Client Connection Idle Timeout	Specify the time (in seconds) a client connection can stay idle before the connection is closed. The default value is 360 seconds (6 minutes). A value of Zero indicates that there is no idle timeout.
Authentication Timeout	Specify the authentication timeout in seconds. The default is 300000.
Clock Skew Tolerance	Enter the permitted time difference in seconds between an Unified Access Gateway clock and the other clocks on the same network. The default is 600 seconds.
Join CEIP	If enabled, sends Customer Experience Improvement Program ("CEIP") information to VMware. See Join or Leave the Customer Experience Improvement Program for details.
Enable SNMP	Enable **YES** to enable SNMP service. Enable simple network management protocol to collect system statistics, memory, and VMware Tunnel server MIB information by Unified Access Gateway. **Note** You must enable SNMP before configuring Tunnel. If you enable SNMP after configuring Tunnel, you must re-save the Tunnel settings for the SNMP settings to take effect. The list of available Management Information Base (MIB), ■ UCD-SNMP-MIB::systemStats ■ UCD-SNMP-MIB::memory ■ VMWARE-TUNNEL-SERVER-MIB::vmwTunnelServerMIB
DNS	Enter Domain Name System addresses that are added to /etc/resolv/conf configuration file. It must contain a valid DNS search address. Click '+' to add a new DNS address.
DNS Search	Enter Domain Name System search that is added to /etc/resolv/conf configuration file. It must contain a valid DNS search address. Click '+' to add a new DNS search entry.
NTP Servers	NTP servers for network time protocol synchronization. You can enter valid IP addresses and hostnames. Any per-interface NTP servers obtained from `systemd-networkd.service` configuration or through DHCP will take precedence over these configurations. Click '+' to add a new NTP server.
FallBack NTP Servers	Fallback NTP servers for network time protocol synchronization. If NTP server information is not found, these fallback NTP server host names or IP addresses will be used. Click '+' to add a new fallback NTP server.

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.

Change Network Settings

You can modify the network settings such as the IP address, Subnet Mask, Default Gateway, and the IP allocation mode for the configured networks from the admin UI.

Note the following limitations when you modify the network settings:

- IPv4 is the only supported IP mode, IPv6 is not supported.

- When the IP address is changed on a management network IP dynamically, browser redirection is not supported to the new IP address.

- When the IP address, subnet mask, or default gateway is changed for an internet facing network interface, all the current sessions are lost.

Prerequisites

- Ensure that you have administrator privileges.

- If you are changing the IP to a static IP address, Subnet Mask or Default Gateway you must know the address, subnet mask, and default gateway beforehand.

Procedure

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

2 Under **Advanced Settings**, click the gearbox icon next to **Network Settings**.

   A list of configured networks and their settings is displayed.

3 In the Network Settings window, click the gearbox icon next to the network whose settings you want to change and enter the following information:

   The IPv4 configuration

Label	Description
IPv4 Allocation Mode	Select whether the IP should be allocated statically or dynamically. This parameter must be specified for static IP allocation.
IPv4 Address	IP address of the network. You do not need to specify the IP address if you select Dynamic IP allocation. This parameter must be specified for static IP allocation.
IPv4 Netmask	IPv4 netmask of the network. You do not need to specify the IPv4 netmask if you select Dynamic IP allocation.
IPv4 Default Gateway	IPv4 default gateway address of Unified Access Gateway. You do not need to specify the default gateway IP address if you select Dynamic IP allocation.
IPv4 Static Routes	IPv4 custom routes for the network. Click '+' to add a new static route.
	Comma-separated list of IPv4 custom routes for NIC in the form ipv4-network-address/bits ipv4-gateway-address. For example, 20.2.0.0/16 10.2.0.1,20.9.0.0/16 10.2.0.2,10.2.0.1/32.
	Note If ipv4-gateway-address is not specified, then the respective route that is added has a gateway of 0.0.0.0

The IPv6 configurations cannot be modified.

Label	Description
IPv6 Allocation Mode	Specifies whether the IP is allocated statically, dynamically or automatically.
IPv6 Address	IP address of the network.
IPv6 Prefix	The IPv6 prefix of the network.
IPv6 Default Gateway	IPv6 default gateway address of Unified Access Gateway.

4   Click **Save**.

If the settings are changed successfully, a success message is displayed. An error message is displayed if the network settings cannot be updated.

Configure User Account Settings

As a superuser administrator who has complete access to the Unified Access Gateway system,you can you can add and delete users, change passwords, and modify roles for the users from the admin configuration pages.

The account settings, including the details of the low-privileged administrator, cannot be exported from or imported into the appliance settings. To configure a new low-privileged account on a new instance of Unified Access Gateway, configure manually through the admin UI.

Add a Low Privilege Administrator

You can now configure and add a low-privilege administrator who can perform a limited number of tasks such as read-only operations, system monitoring and so on.

Note   Currently, you can add only one low-privilege administrator to an instance of Unified Access Gateway.

Procedure

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

2   Under Advanced Settings, select the Account Settings gearbox icon.

3   In the Account Settings window, click **Add**.

The role is automatically set to ROLE_MONITORING.

4   In the Account Settings window, enter the following information:

a   A unique user name for the user.

b   (Optional) Select the **Enabled** box if you want to enable the user immediately after adding the user.

c   Enter a password for the user. 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 ! @ # $ % * ( ).

d   Confirm the password.

5 Click **Save**.

Results

The administrator you added is listed under Account Settings.

What to do next

The low-privilege administrator can log in to the system to change the password or perform monitoring tasks.

Modify User Account Settings

As a superuser administrator, you can change the password for a user, and enable or disable a user.

You can also change your own password, but you cannot disable your own account.

Procedure

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

2 In the Advanced Settings section, click Account Settings.

A list of users is displayed.

3 Click the gearbox icon next to the user whose account you want to modify.

4 Edit the following values.

  a Select or deselect the **Enable** box depending on whether you want to enable or disable the user.

  b To reset the user password, enter a new password, and confirm the password. If you are logged in as admin, you must enter your old password also.

   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 ! @ # $ % * ( ).

5 Click **Save**.

Reset the Admin Password using the Unified Access Gateway Console

If the admin user password set during deployment is forgotten, the user can login to the Unified Access Gateway console using the root user credentials and reset the Admin UI password.

Prerequisites

You must have the password for logging in to the virtual machine as the root user or a user with root privileges. The user must be a part of the *root* group.

Procedure

1 Log in to the operating system of the Unified Access Gateway console as the root user.

2   Enter the following commands to reset the password of the administrator.

`adminpwd`

`New password for user "admin": ********`

`Retype new password: ********`

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

The following message is displayed.

`adminpwd: password for "admin" updated successfully`

3   Enter the following commands to reset the password of an administrator with less privileges.

`adminpwd [-u <username>]`

`New password for user "jdoe": ********`

`Retype new password: ********`

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

The following message is displayed.

`adminpwd: password for "jdoe" updated successfully`

Results

The admin user password is reset successfully.

What to do next

User can now log in to the Unified Access Gateway interface using the administrator password that is just set. User will be asked to change the password while logging in for the first time after password reset using the `adminpwd` CLI command.

Note   User must log in on first attempt after changing the password.

Delete a User

As a super-user administrator, you can delete a non-root user.

You cannot delete a root administrator.

Procedure

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

2   Under Advanced Settings, select the Account Settings gearbox icon.

A list of users is displayed.

3   Click the 'x' button next to the user you want to delete.

> **Caution**   The user is deleted immediately. This action cannot be undone.

Results

The user account is deleted and a message is displayed.

Configure JSON Web Token Settings

You can now add public keys for validation of JSON web tokens.

Procedure

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

2   Under Advanced Settings, select the JWT Settings gearbox icon.

3   In the JWT Settings window, click **Add**.

4   In the Account Settings window, enter the following information:

    a   A name to identify this setting for validation.

    b   Click '+' to select and add a public key of your certificate to use for JWT artifact validation. The file must be in PEM format.

> **Note**   If a public key is not uploaded, validation is not enabled in Unified Access Gateway.

5   Click **Save**.

Results

The details of the parameters are listed under JWT Settings.

Update SSL Server Signed Certificates

You can replace your signed certificates when they expire or substitute the default certificates with CA-signed certificates.

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.

Note the following considerations when you upload a certificate:

- You can replace the default certificate with a CA-signed PEM certificate for both the administrator and the user.

- When you upload a CA-signed certificate on the admin interface, the SSL connector on the admin interface is updated and restarted to ensure the uploaded certificate takes effect. If the connector fails to restart with the uploaded CA-signed certificate, a self-signed certificate is generated and applied on the admin interface and the user is notified that the previous attempt to upload a certificate was unsuccessful.

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 either **Admin Interface** or **Internet Interface** to apply the certificate to either of the interfaces. You can also select both to apply the certificate to both the interfaces.

4 Select a Certificate Type of **PEM** or **PFX**.

5 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.

6 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 an alias for the PFX certificate.

       You can use the alias to distinguish when multiple certificates are present.

7 Click **Save**.

Results

A confirmation message is displayed when the certificate is updated successfully.

What to do next

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

- If you uploaded a CA-signed certificate for the **Admin Interface**, close the browser and reopen the Admin UI in a new browser window.

- If a CA-signed certificate is in effect on the admin interface and you upload a self-signed certificate, the Admin UI may not behave as expected. Clear the browser cache and open the Admin UI in a new window.

Using PowerShell to Deploy Unified Access Gateway

<div align="right">

3

</div>

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
- Using PowerShell to Deploy the Unified Access Gateway Appliance

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.

- VMware vSphere ESXi 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.

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.

Important   With a PowerShell deployment, you can provide all the settings in the INI file, and the Unified Access Gateway instance is production-ready as soon as it is booted up. If you do not want to change any settings post-deployment, you need not provide the Admin UI password.

However, both Admin UI and the API are not available if the Admin UI password is not provided during deployment.

Note

- If you do not provide the Admin UI password at the time of deployment, you cannot add a user later to enable access to either the Admin UI or the API. You must redeploy your Unified Access Gateway instance with a valid password if you want to add an Admin UI user.

- Unified Access Gateway 3.5 and later includes an optional `sshEnabled` INI property. Setting `sshEnabled=true` in the `[General]` section of the PowerShell INI file automatically enables `ssh` access on the deployed appliance. VMware does not generally recommend enabling `ssh` on Unified Access Gateway except in certain specific situations and where access can be restricted. This capability is mainly intended for Amazon AWS EC2 deployments where an alternative console access is not available.

  If `sshEnabled=true` is not specified or is set to `false` then the `ssh` is not enabled.

  Enabling `ssh` access on Unified Access Gateway for vSphere, Hyper-V or Microsoft Azure deployments is not generally required as console access with those platforms can be used. If root console access is required for Amazon AWS EC2 deployment, then set `sshEnabled=true`. In cases where `ssh` is enabled, TCP port 22 access must be restricted in firewalls or security groups to source IP addresses of individual administrators. EC2 supports this restriction in the EC2 Security Group associated with the Unified Access Gateway network interfaces.

Prerequisites

- For a Hyper-V deployment, and if you are upgrading Unified Access Gateway with static IP, delete the older appliance before deploying the newer instance of Unified Access Gateway.

- 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 *uagdeploy-XXX.zip* files into a folder on the Windows machine.

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

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

4 Create a INI configuration file for the 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.

```
[General]
netManagementNetwork=
netInternet=
netBackendNetwork=
name=
dns = 192.0.2.1 192.0.2.2
dnsSearch = example1.com example2.com
ip0=10.108.120.119
diskMode=
```

```
source=
defaultGateway=10.108.120.125
target=
ds=
authenticationTimeout=300000
fipsEnabled=false
uagName=UAG1
locale=en_US
ipModeforNIC3=DHCPV4_DHCPV6
tls12Enabled=true
ipMode=DHCPV4_DHCPV6
requestTimeoutMsec=10000
ipModeforNIC2=DHCPV4_DHCPV6
tls11Enabled=true
clientConnectionIdleTimeout=180
tls10Enabled=false
adminCertRolledBack=false
honorCipherOrder=false
cookiesToBeCached=none
healthCheckUrl=/favicon.ico
quiesceMode=false
syslogUrl=10.108.120.108:514
isCiphersSetByUser=false
tlsPortSharingEnabled=true
ceipEnabled=true
bodyReceiveTimeoutMsec=15000
monitorInterval=60
cipherSuites=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH
_AES_128_CBC_SHA
adminPasswordExpirationDays=90
httpConnectionTimeout=120
isTLS11SetByUser=false
sessionTimeout=36000000
ssl30Enabled=false
snmpEnabled= TRUE | FALSE
ntpServers=ip1 ip2

[WebReverseProxy1]
proxyDestinationUrl=https://10.108.120.21
trustedCert1=
instanceId=view
healthCheckUrl=/favicon.ico
userNameHeader=AccessPoint-User-ID
proxyPattern=/(.*)
landingPagePath=/
hostEntry1=10.108.120.21 HZNView.uagqe.auto.com

[Horizon]
proxyDestinationUrl=https://enterViewConnectionServerUrl
trustedCert1=
gatewayLocation=external
disableHtmlAccess=false
healthCheckUrl=/favicon.ico
proxyDestinationIPSupport=IPV4
smartCardHintPrompt=false
```

```
queryBrokerInterval=300
proxyPattern=(/|/view-client(.*)|/portal(.*)|/appblast(.*))
matchWindowsUserName=false
windowsSSOEnabled=false

[SSLCert]
pemPrivKey=
pemCerts=
pfxCerts=
pfxCertAlias=

[SSLCertAdmin]
pemPrivKey=
pemCerts=
pfxCerts=
pfxCertAlias=

[JWTSettings1]
publicKey1=
publicKey2=
publicKey3=
name=JWT_1

[JWTSettings2]
publicKey1=
publicKey2=
name=JWT_2
```

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.

a   (Optional) If there is a warning for the script, run the following command to unblock the warning: `unblock-file -path .\uagdeploy.ps1`

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

```
.\uagdeploy.ps1 -iniFile uag1.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.

Results

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

What to do next

If you want to upgrade Unified Access Gateway while preserving the existing settings, edit the `.ini` file to change the source reference to the new version and rerun the `.ini` file: `uagdeploy.ps1 uag1.ini`. This process can take up to 3 minutes.

```
[General]
name=UAG1
source=C:\temp\euc-unified-access-gateway-3.2.1-7766089_OVF10.ova
```

If you want to upgrade with zero service interruption, see Upgrade with Zero Downtime.

Deployment Use Cases for Unified Access Gateway

<div style="text-align: right">4</div>

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 Workspace ONE UEM.

This chapter includes the following topics:

- Deployment with Horizon and Horizon Cloud with On-Premises Infrastructure
- Endpoint Compliance Checks for Horizon
- Deployment as Reverse Proxy
- Deployment for Single Sign-on Access to On-Premises Legacy Web Apps
- Workspace ONE UEM Components on Unified Access Gateway
- Additional Deployment Use Cases

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.

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.

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

Figure 4-1. Unified Access Gateway in DMZ Topology
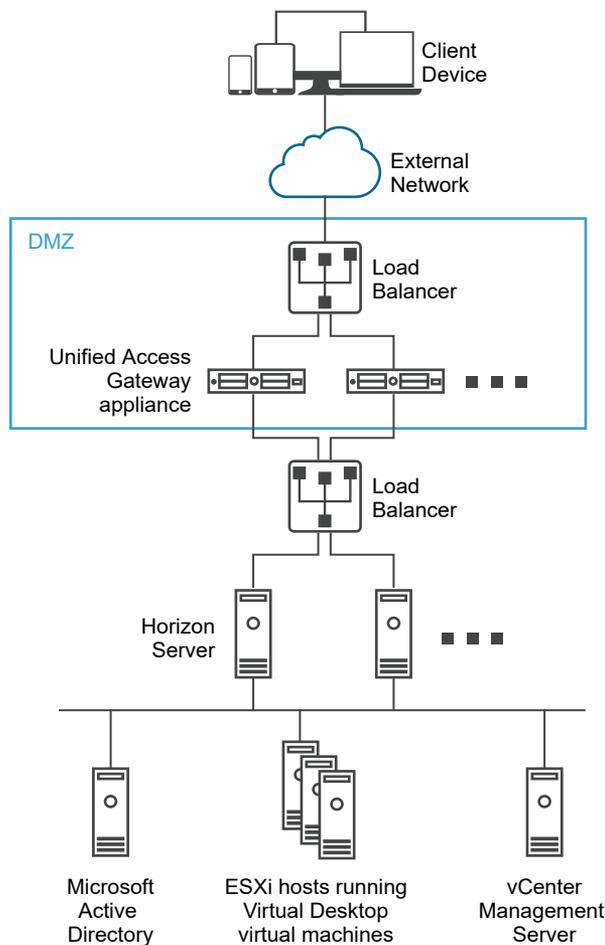
You must verify the requirements for seamless Unified Access Gateway deployment with Horizon.

- Unified Access Gateway appliance points to a load balancer in front of the Horizon servers, the selection of the server instance is dynamic.

- By default, port 8443 must be available for Blast TCP/UDP. However, port 443 can also be configured for Blast TCP/UDP.

  Note If you configure Unified Access Gateway to use both IPv4 and IPv6 mode, then the Blast TCP/UDP must be set to port 443. You can enable Unified Access Gateway to act as a bridge for IPv6 Horizon clients to connect to an IPv4 backend Connection Server or agent environment. See Support for IPv4 and IPv6 Dual Mode for Horizon Infrastructure.

- 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.

It is recommended that users deploying Horizon 7 use Unified Access Gateway appliance instead of Horizon security server.

Note Horizon Connection Server, does not work with an enabled web reverse proxy when there is an overlap in the proxy pattern. Therefore, if both Horizon and a web reverse proxy instance are configured and enabled with proxy patterns on the same Unified Access Gateway instance, remove the proxy pattern '/' from Horizon settings and retain the pattern in the web reverse proxy to prevent the overlap. Retaining the '/' proxy pattern in the web reverse proxy instance ensures that when a user clicks the URL of Unified Access Gateway, the correct web reverse proxy page is displayed. If only Horizon settings are configured, the above change is not required.

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 4-2. Unified Access Gateway Appliance Pointing to a Load Balancer
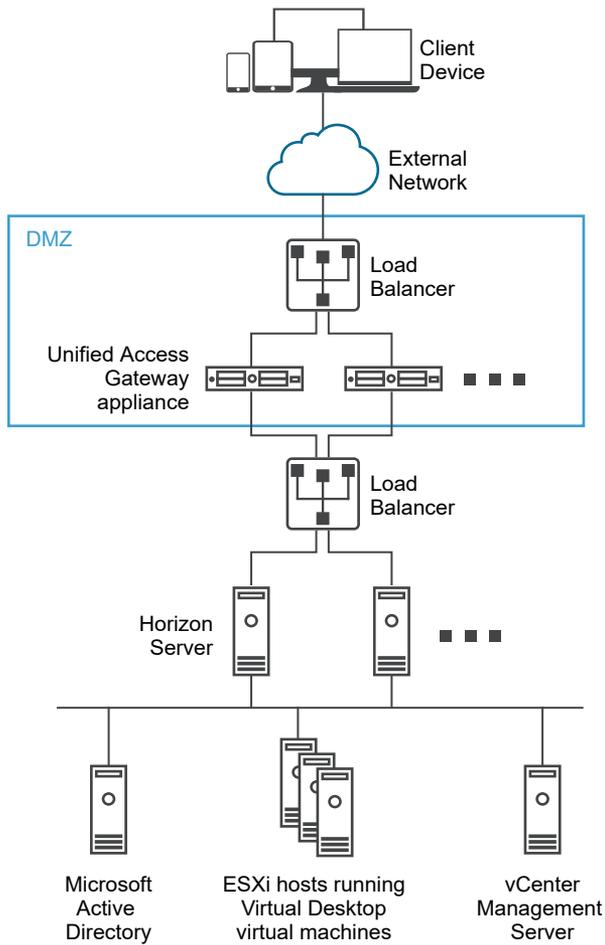
Alternatively you can have one or more Unified Access Gateway appliances pointing to an individual server instance. In both approaches, use a load balancer in front of two or more Unified Access Gateway appliances in the DMZ.

Figure 4-3. Unified Access Gateway Appliance Pointing to a Horizon Server Instance
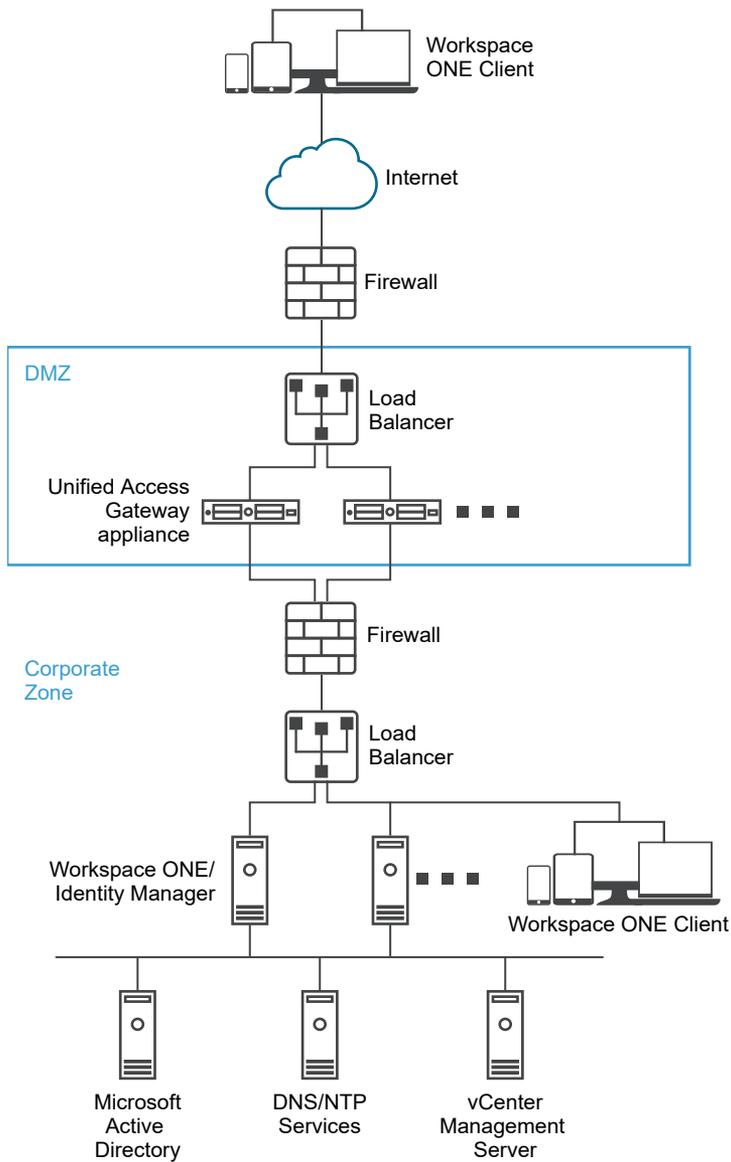
Authentication

User authentication is similar to Horizon 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 Horizon Connection Server. Unified Access Gateway is not required to communicate directly with Active Directory. This communication serves as a proxy through the Horizon 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 Horizon 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 by 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.

Support for IPv4 and IPv6 Dual Mode for Horizon Infrastructure

You can use Unified Access Gateway to act as a bridge for IPv6 Horizon clients to connect to an IPv4 back end Connection Server or agent environment.

You can deploy Unified Access Gateway in twonic mode with the front-end NIC in mixed IPv4/IPv6 mode and the Horizon back end or management NIC in IPv4 mode. The Horizon back end environment might consist of Connection Servers, agent desktops, or other server-side infrastructure.

Note   When you configure Unified Access Gateway in IPv4/IPv6 mode, ensure that the Blast External URL for TCP/UDP is set to 443. See Deployment with Horizon and Horizon Cloud with On-Premises Infrastructure and Configure Horizon Settings.

Note   Horizon IPv6 to IPv4 bridging feature is not supported for PCoIP or Blast UDP.

The following Horizon client and server IP modes are supported.

Table 4-1. Supported Horizon Settings (IP Modes)

Horizon Client Mode	Horizon Server Mode	Supported
IPv4	IPv4	Yes
IPv6	IPv4	Yes
IPv6	IPv6	Yes
IPv4	IPv6	No

When installing a Horizon client, if you select **Automatic Selection** or **Dual**, connection occurs over IPv4 or IPv6, depending on the current network.

Advanced Edge Service Settings

Unified Access Gateway uses different variables to differentiate between edge services, configured web proxies, and proxy destination URLs.

Proxy Pattern and Unsecure Pattern

Unified Access Gateway uses proxy pattern to forward incoming HTTP requests to the right edge service such as Horizon or to one of the configured web reverse proxy instances such as VMware Identity Manager. It is therefore used as a filter to decide if a reverse proxy is needed to process incoming traffic.

If a reverse proxy is selected, then the proxy uses a specified unsecure pattern to decide whether to allow the incoming traffic to go to the back end without being authenticated or not.

The user must specify a proxy pattern, specifying an unsecure pattern is optional. The unsecure pattern is used by web reverse proxies such as VMware Identity Manager which have their own login mechanism and want certain URLs such as log in page paths, javascripts, or image resources, to be passed to the back end without being authenticated.

Note   An unsecure pattern is a subset of the proxy pattern and therefore some paths might be repeated between both of them for a reverse proxy.

Each edge service can have a different pattern. For example, the `Proxy Pattern` for Horizon can be configured as `(/|/view-client(.*)|/portal(.*)|/appblast(.*))` and the pattern for VMware Identity Manager can be configured as `(/|/SAAS(.*)|/hc(.*)|/web(.*)|/catalog-portal(.*))`.

Note   Horizon Connection Server does not work with an enabled web reverse proxy when there is an overlap in the proxy pattern. Therefore, if both Horizon and a web reverse proxy instance such as VMware Identity Manager are configured and enabled with proxy patterns on the same Unified Access Gateway instance, remove the proxy pattern '/' from Horizon settings and retain the pattern in VMware Identity Manager to prevent the overlap.

Retaining the '/' proxy pattern in the web reverse proxy instance (VMware Identity Manager) ensures that when a user clicks the URL of Unified Access Gateway, the VMware Identity Manager page is displayed.

If only Horizon settings are configured, the above change is not required.

Proxy Host Pattern

If there are multiple web reverse proxy instances configured, and there is an overlap in Proxy Patterns, Unified Access Gateway uses the `Proxy Host Pattern` to differentiate between them. Configure `Proxy Host Pattern` as the FQDN of the reverse proxy.

For example, a host pattern for Sharepoint can be configured as *sharepoint.myco.com* and a pattern for JIRA can be configured as *jira.myco.com*.

Host Entries

Configure this text box only if Unified Access Gateway is not able to reach the back end server or application. When you add the IP address and hostname of the back end application to the Host Entries, that information is added to the `/etc/hosts` file of Unified Access Gateway. This field is common across all the edge service settings.

Proxy Destination URL

This is the back end server application URL of the edge service settings for which Unified Access Gateway is the proxy. For example:

- For Horizon Connection Server, the connection server URL is the proxy destination URL.

- For web reverse proxy, the application URL of the configured web reverse proxy is the proxy destination URL.

Single Reverse Proxy Configuration

When Unified Access Gateway receives a single incoming request with a URI, the proxy pattern is used to decide whether to forward the request or drop it.

Multiple Reverse Proxy Configuration

1   When Unified Access Gateway is configured as a reverse proxy, and an incoming request arrives with a URI path, Unified Access Gateway uses the proxy pattern to match the correct web reverse proxy instance. If there is a match, the matched pattern is used. If there are multiple matches, then the filtering and matching process is repeated in step 2. If there is no match, the request is dropped and an HTTP 404 is sent back to the client.

2   The proxy host pattern is used to filter the list that was already filtered in step 1. The HOST header is used to filter the request and find the reverse proxy instance. If there is a match, the matched pattern is used. If there are multiple matches, then the filtering and matching process is repeated in step 3.

3   Note the following:

- The first match from the filtered list in step 2 is used. This match might not always be the correct web reverse proxy instance. Therefore, ensure that the combination of proxy pattern and proxy host pattern for a web reverse proxy instance is unique if there are multiple reverse proxies setup in a Unified Access Gateway.

- The host name of all the configured reverse proxies should resolve to same IP address as the external address of the Unified Access Gateway instance.

See Configure Reverse Proxy With VMware Identity Manager for more information and instructions about configuring a reverse proxy.

Example: Two Reverse Proxies Configured With Clashing Proxy Patterns, Distinct Host Patterns

Suppose the proxy pattern for the first reverse proxy is /(.*) with the host pattern as host1.domain.com and the pattern for the second reverse proxy is (/app2(.*)|/app3(.*)|/) with the host pattern as host2.domain.com.

- If a request is made with the path set to https://host1.domain.com/app1/index.html, then the request is forwarded to the first reverse proxy.

- If a request is made with the path set to https://host2.domain.com/app2/index.html, then the request is forwarded to the second reverse proxy.

Example: Two Reverse Proxies With Mutually Exclusive Proxy Patterns

Suppose the proxy pattern for the first reverse proxy is `/app1(.*)` and for the second reverse proxy is `(/app2(.*)|/app3(.*)|/)`.

- If a request is made with the path set to `https://<uag domain name>/app1/index.html`, then the request is forwarded to the first reverse proxy.

- If a request is made with the path set to `https://<uag domain name>/app3/index.html` or `https://<uag domain name>/` , then the request is forwarded to the second reverse proxy.

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.

Prerequisites

If you want to have both Horizon and a web reverse proxy instance such as VMware Identity Manager configured and enabled on the same Unified Access Gateway instance, see Advanced Edge Service Settings.

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, ensure that the server certificates are 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.
Enable PCOIP	Change NO to **YES** to specify whether the PCoIP Secure Gateway is enabled.
Disable PCOIP Legacy Certificate	Change **NO** to **YES** to specify to use the uploaded SSL server certificate instead of Legacy certificate. Legacy PCoIP clients will not work if this parameter is set to **YES**.

Option	Description
PCOIP External URL	URL used by Horizon clients to establish the Horizon PCoIP session to this Unified Access Gateway appliance. It must contain an IPv4 address and not a hostname. For example, `10.1.2.3:4172`. The default is the Unified Access Gateway IP address and port 4172.
Enable Blast	To use the Blast Secure Gateway, change NO to **YES**.
Connection Server IP mode	Select IPv4, IPv6, or IPv4+IPv6 from the drop-down menu. Default is IPv4.

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. Currently, RSA SecurID and RADIUS authentication methods are supported.
	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.
	Note
	■ With the PowerShell deployment, for RSA SecurID authentication, configure this option to use `securid-auth AND sp-auth` to display the passcode screen.
	■ With the vSphere deployment, for RSA SecurID authentication, configure this option to use `securid-auth` to display the passcode screen.
	■ 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 your 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 `uagdeploy` PowerShell command to redeploy the Unified Access Gateway configured for RSA SecurID.
Enable Windows SSO	This is enabled when Auth Methods is to set to RADIUS. Change NO to **YES** to enable RADIUS authentication.
RADIUS Class Attributes	This is enabled when Auth Methods is to set to RADIUS. Click '+' to add a value for the class attribute. Enter the name of the class attribute to be used for user authentication. Click '-' to remove a class attribute.
	Note If this field is left blank, then the additional authorization is not performed.
Smart Card Hint Prompt	Change NO to **YES** to enable password hint for certificate authentication.

Option	Description
Health Check URI Path	The URI path for the connection server that Unified Access Gateway connects to, for health status monitoring.
Blast External URL	URL used by Horizon clients to establish the Horizon Blast or BEAT session to this Unified Access Gateway appliance. For example, `https://uag1.myco.com` or `https://uag1.myco.com:443`. If the TCP port number is not specified, the default TCP port is 8443. If the UDP port number is not specified, the default UDP port is also 8443.
Enable UDP Server	Connections are established through the UDP Tunnel server if there is a low bandwidth.
Blast Proxy Certificate	Proxy certificate for Blast. Click **Select** to upload a certificate in the PEM format and add to the BLAST trust store. Click **Change** to replace the existing certificate. If the user manually uploads the same certificate for the Unified Access Gateway to the load balancer and needs to use a different certificate for Unified Access Gateway and Blast Gateway, establishing a Blast desktop session would fail as the thumbprint between the client and the Unified Access Gateway does not match. The custom thumbprint input to Unified Access Gateway or Blast Gateway resolves this by relaying the thumbprint to establish the client session.
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	URL used by Horizon clients to establish the Horizon Tunnel session to this Unified Access Gateway appliance. For example, `https://uag1.myco.com` or `https://uag1.myco.com:443`. If the TCP port number is not specified, the default TCP port is 443.
Tunnel Proxy Certificate	Proxy certificate for Horizon Tunnel. Click **Select** to upload a certificate in the PEM format and add to the Tunnel trust store. Click **Change** to replace the existing certificate. If the user manually uploads the same certificate for the Unified Access Gateway to the load balancer and needs to use a different certificate for Unified Access Gateway and Horizon Tunnel, establishing a Tunnel session would fail as the thumbprint between the client and the Unified Access Gateway does not match. The custom thumbprint input to Unified Access Gateway or Horizon Tunnel resolves this by relaying the thumbprint to establish the client session.
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). It has a default value of `(/|/view-client(.*)|/portal(.*)|/appblast(.*))`.
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.

Option	Description
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. **Note** In Horizon 7 if you enable the **Hide server information in client user interface** and **Hide domain list in client user interface** settings and select two-factor authentication (RSA SecureID or RADIUS) for the Connection Server instance, do not enforce Windows user name matching. Enforcing Windows user name matching prevents users from entering domain information in the user name text box and login always fails. For more information, see the topics about two-factor authentication in the Horizon 7 Administration document.
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.
Trusted Certificates	Add a trusted certificate to this edge service. Click '+' to select a certificate in PEM format and add to the trust store. Click "-" to remove a certificate from the trust store. By default, the alias name is the filename of the PEM certificate. Edit the alias text box to provide a different name.
Response Security Headers	Click '+' to add a header. Enter the name of the security header. Enter the value. Click '-' to remove a header. Edit an existing security header to update the name and the value of the header. **Important** The header names and values are saved only after you click **Save**. Some standard security headers are present by default. The headers configured are added to the Unified Access Gateway response to client only if the corresponding headers are absent in the response from the configured back-end server. **Note** Modify security response headers with caution. Modifying these parameters might impact the secure functioning of Unified Access Gateway .
Host Entries	Enter the details to be added in `/etc/hosts` file. Each entry should include 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`. Click the '+' sign to add multiple host entries. **Important** The host entries are saved only after you click **Save**.
Disable HTML Access	If set to YES, disables web access to Horizon. See Endpoint Compliance Checks for Horizon for details.

7 Click **Save**.

Monitoring Unified Access Gateway in Horizon Console

Unified Access Gateway integration with Horizon Admin console provides visibility on status, statistics, and session information in the Horizon Admin UI. You can monitor the system health of Unified Access Gateway.

The new tab **Gateway** in the Horizon Admin Console provides a functionality to register and unregister Unified Access Gateway.

Figure 4-4. Dashboard
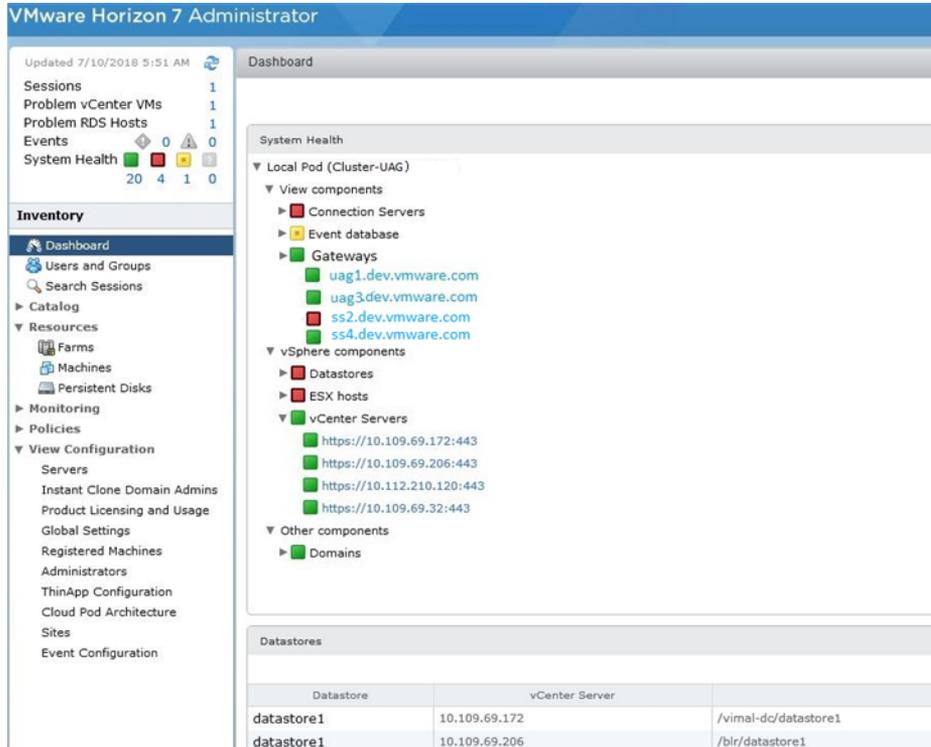
Dashboard screen displays the details of the registered Unified Access Gateway for version 3.4 or later, vSphere components, domains, desktops, and datastore usage.

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 4-2. 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.

Table 4-2. BEAT Port Options (continued)

Blast External URL	TCP Port Used by Client	UDP Port Used by Client	Description
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.

Results

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 start Horizon applications.

Note A single instance of Unified Access Gateway can handle up to 15000 simultaneous TCP connections. If the expected load is more than 15000, multiple instances of Unified Access Gateway must be configured behind the load balancer.

See Advanced Edge Service Settings for information about the settings used when configuring reverse proxy.

Figure 4-5. Unified Access Gateway Appliance Pointing to VMware Identity Manager
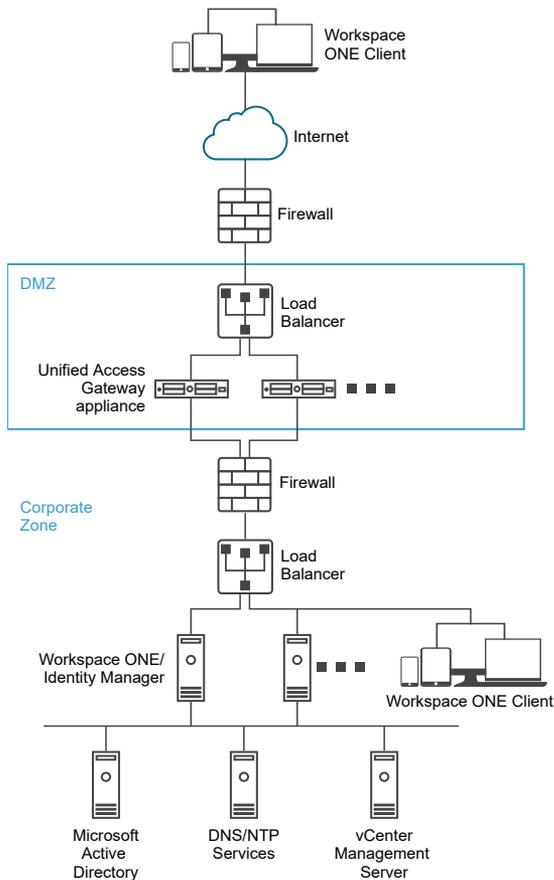
Understanding Reverse Proxy

Unified Access Gateway provides access to the app portal for remote users to single-sign-on and access their resources. The app portal is a back-end application such as Sharepoint, JIRA, or VIDM, for which Unified Access Gateway is acting as the reverse proxy.

Note Horizon Connection Server, does not work with an enabled web reverse proxy when there is an overlap in the proxy pattern. Therefore, if both Horizon and a web reverse proxy instance are configured and enabled with proxy patterns on the same Unified Access Gateway instance, remove the proxy pattern '/' from Horizon settings and retain the pattern in the web reverse proxy to prevent the overlap. Retaining the '/' proxy pattern in the web reverse proxy instance ensures that when a user clicks the URL of Unified Access Gateway, the correct web reverse proxy page is displayed. If only Horizon settings are configured, the above change is not required.

Note the following points when enabling and configuring reverse proxy:

- You must enable the authentication of the reverse proxy on an Edge Service manager. Currently, RSA SecurID and RADIUS authentication methods are supported.

- You must generate the identity provider metadata (IDP 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.

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

Figure 4-6. Multiple Reverse Proxies Configured
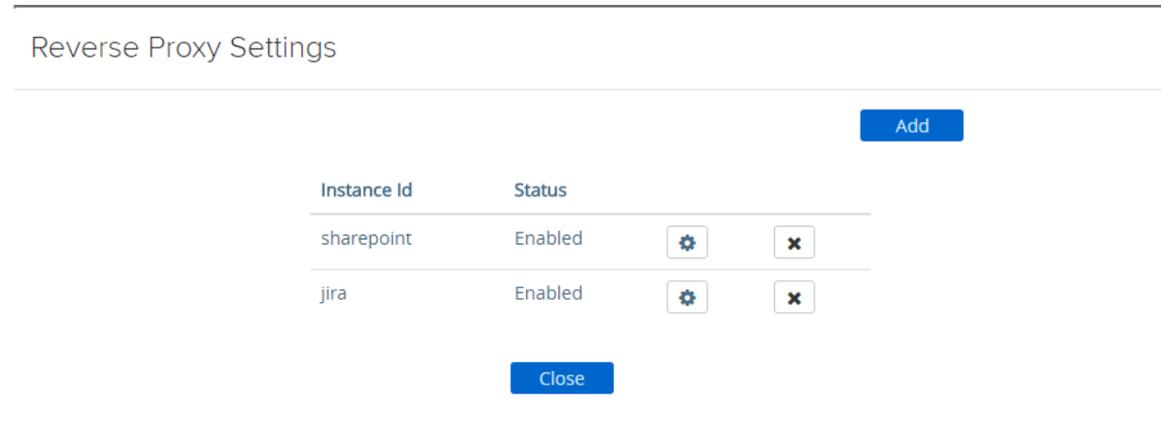
Configure Reverse Proxy With VMware Identity Manager

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

Prerequisites

Note the following requirements for deployment with VMware Identity Manager:

- Split DNS. Externally, the host name should get resolved to the IP address of Unified Access Gateway. Internally, on Unified Access Gateway, the same host name should get resolved to the actual web server either through internal DNS mapping or through a host name entry on Unified Access Gateway.

  Note If you are deploying only with Web Reverse proxy, there is no need to configure identity bridging.

- 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.

- The combination of proxy pattern and proxy host pattern for a web reverse proxy instance must be unique if there are multiple reverse proxies setup in a Unified Access Gateway instance.

■ The host names of all configured reverse proxies should resolve to the same IP address which is the IP address of the Unified Access Gateway instance.

■ See Advanced Edge Service Settings for information about the advanced edge service settings.

Procedure

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

2 In the **General Settings > Edge Service Settings**, 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, which is usually the back end URL. For example, for VMware Identity Manager, add the IP address, the VMware Identity Manager host name and the external DNS on the client machine. On the Admin UI, add the IP address, the VMware Identity Manager host name and the internal DNS.
Proxy Destination URL Thumbprints	Enter a list of acceptable SSL server certificate thumbprints for the `proxyDestination` URL. If you specify *****, any certificate is accepted. A thumbprint is in the format *[alg=]xx:xx*, where *alg* can either be the default, *sha1*, 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 configure 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. RSA SecurID, RADIUS, and Device Certificate Auth methods are supported.
Health Check URI Path	Unified Access Gateway connects to this URI path to check the health of your web application.
SAML SP	Required when you configure Unified Access Gateway as an 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 with Unified Access Gateway, their names must be unique.
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>`.

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(.*)|/SAAS/auth/wsfed/services(.*)|/`
	`SAAS/auth/wsfed/active/logon(.*))`

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.
Trusted Certificates	Add a trusted certificate to this edge service. Click '+' to select a certificate in PEM format and add to the trust store. Click '-' to remove a certificate from the trust store. By default, the alias name is the filename of the PEM certificate. Edit the alias text box to provide a different name.

Option	Description
Response Security Headers	Click '+' to add a header. Enter the name of the security header. Enter the value. Click '-' to remove a header. Edit an existing security header to update the name and the value of the header.
	Important The header names and values are saved only after you click **Save**. Some standard security headers are present by default. The headers configured are added to the Unified Access Gateway response to client only if the corresponding headers are absent in the response from the configured back-end server.
	Note Modify security response headers with caution. Modifying these parameters might impact the secure functioning of Unified Access Gateway .
Host Entries	Enter the details to be added in `/etc/hosts` file. Each entry should include 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`. Click the '+" sign to add multiple host entries.
	Important The host entries are saved only after you click **Save**.

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.

Configure Reverse Proxy With VMware Workspace ONE UEM API

When using On-Premise installations of Workspace ONE UEM, the API server is typically installed behind a firewall without incoming internet access. To securely use Workspace ONE Intelligence automation capabilities, you can configure a web reverse proxy edge service within the Unified Access Gateway to allow access only to the API service so actions can be taken on devices, users, and other resources.

Prerequisites

▪ The UEM API service must have a fully qualified domain name (FQDN) as hostname.

▪ Unified Access Gateway must use internal DNS. This means that the proxy Destination URL must use FQDN.

- The combination of proxy pattern and proxy host pattern for a web reverse proxy instance must be unique if there are multiple reverse proxies setup in a Unified Access Gateway instance.

- The host names of all configured reverse proxies should resolve to the same IP address which is the IP address of the Unified Access Gateway instance.

- For more information on Advanced Edge Service Settings, see Advanced Edge Service Settings.

Procedure

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

2 In the **General Settings > Edge Service Settings**, 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, which is usually the back end URL. For example, for the Workspace ONE UEM API server, it may be a different URL/IP Address than your console login. You can verify this by checking in the UEM settings pages under **Settings > System > Advanced > API > REST API > REST API URL**.
Proxy Destination URL Thumbprints	Enter a list of acceptable SSL server certificate thumbprints for the `proxyDestination` URL. If you specify *****, any certificate is accepted. A thumbprint is in the format *[alg=]xx:xx*, where *alg* can either be the default, `sha1`, 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 Workspace ONE UEM API, use: `(/API(.*)|/api(.*)|/Api(.*)|)`. **Note** When you configure 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. RSA SecurID, RADIUS, and Device Certificate Auth methods are supported.
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>`. **Note** While using the Unified Access Gateway behind a load balancer, enter the Load Balancer URL in this field.
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.
Trusted Certificates	Add a trusted certificate to this edge service. Click '+' to select a certificate in PEM format and add to the trust store. Click '-' to remove a certificate from the trust store. By default, the alias name is the filename of the PEM certificate. Edit the alias text box to provide a different name.
Host Entries	Enter the details to be added in `/etc/hosts` file. Each entry should include 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`. Click the '+" sign to add multiple host entries. **Important** The host entries are saved only after you click **Save**.

8 Click **Save**.

What to do next

To configure the Workspace UEM API Connector for use with Workspace ONE Intelligence, see the *Getting Started with Automations* topic of the *Workspace ONE Intelligence* documentation. Use the external URL configured for your Unified Access Gateway instead of the UEM REST API internal server URL.

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.

Note Horizon Connection Server, does not work with an enabled web reverse proxy when there is an overlap in the proxy pattern. Therefore, if both Horizon and a web reverse proxy instance are configured and enabled with proxy patterns on the same Unified Access Gateway instance, remove the proxy pattern '/' from Horizon settings and retain the pattern in the web reverse proxy to prevent the overlap. Retaining the '/' proxy pattern in the web reverse proxy instance ensures that when a user clicks the URL of Unified Access Gateway, the correct web reverse proxy page is displayed. If only Horizon settings are configured, the above change is not required.

Figure 4-7. Unified Access Gateway Identity Bridging Mode
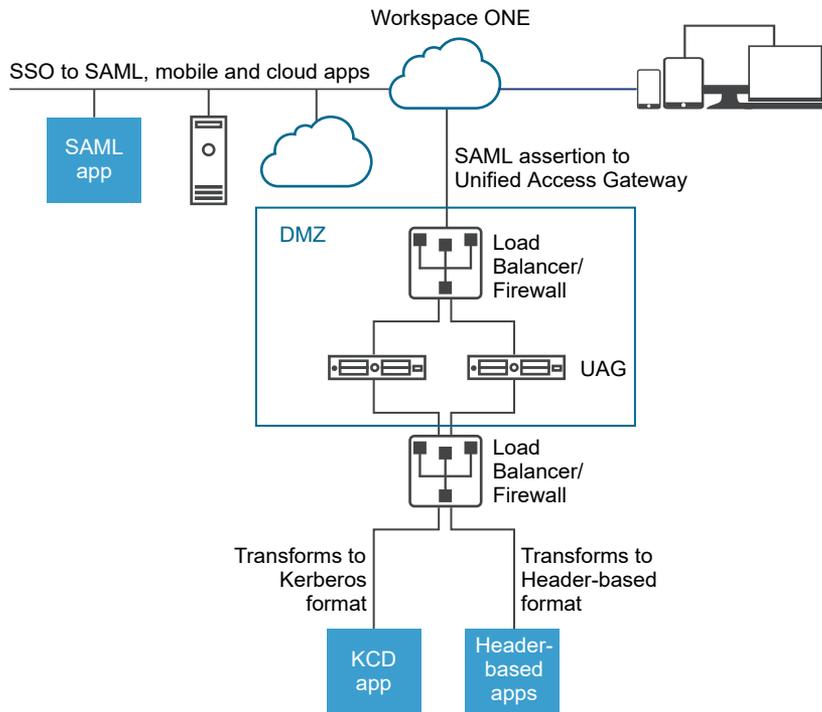
Identity Bridging Deployment Scenarios

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 4-8. Unified Access Gateway Identity Bridging with Workspace ONE in the Cloud
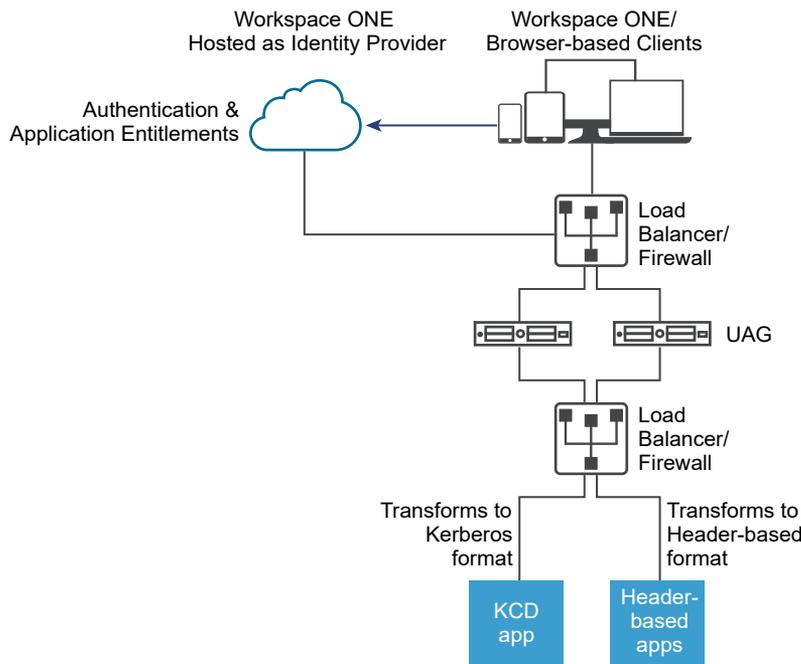
Using Identity Bridging with Workspace ONE Clients On Premises

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 4-9. Unified Access Gateway Identity Bridging On-Premises
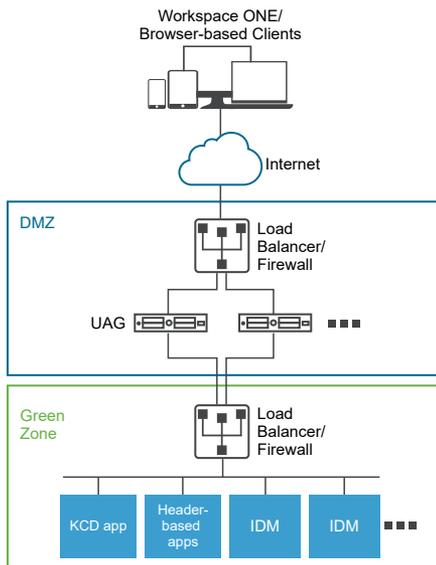
Using Identity Bridging with Certificate to Kerberos

You can configure Identity Bridging to provide single sign-on (SSO) to On-Premises legacy non-SAML applications using certificate validation. See Configure a Web Reverse Proxy for Identity Bridging (Certificate to Kerberos).

Configuring Identity Bridging Settings

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

Note This release of identity bridging supports cross-domain with a single domain setup. This means the user and the SPN account can be in different domains.

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.

- Ensure that the following ports are open:

  - Port 443 for incoming HTTP requests

  - TCP/UDP port 88 for Kerberos communication with Active Directory

  - Unified Access Gateway uses TCP to communicate with back-end applications. The appropriate port on which the back-end is listening, for example, TCP port 8080.

Note

- Configuring identity bridging for both SAML and Certificate to Kerberos for two different reverse proxy instances on the same Unified Access Gateway instance is not supported.

- Web Reverse Proxy instances with certificate authority and without certificate-based authentication that does not have identity bridging enabled on the same appliance is not supported.

Header-Based Authentication Using SAML

SAML responses from IDP to SP (in the case of identity bridging, Unified Access Gateway) contain SAML assertions, which have SAML attributes. The SAML attributes are configurable in the IDP to point to various parameters such as user name, email and so on.

In the header-based authentication using SAML, the value of a SAML attribute can be sent as an HTTP header to the back-end proxied destination. SAML attribute name defined in Unified Access Gateway is the same as that as in the IDP. For example, if an identity provider has the attribute defined as `Name: userName Value: idmadmin`, then, SAML attribute name in Unified Access Gateway must be defined as `"userName"`.

SAML attribute that does not match the attribute defined in the IDP is ignored. Unified Access Gateway supports both multiple SAML attributes and multi-valued SAML attributes. Sample excerpts of the SAML assertion expected from an Identity provider are mentioned in the following for each case. For example,

1. SAML response expected from IDP for multiple SAML attributes

```
<saml:AttributeStatement>
     <saml:Attribute Name="userName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
               <saml:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">idmadmin</saml:AttributeValue>
     </saml:Attribute>
     <saml:Attribute Name="userEmail" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
               <saml:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">63ecfabf-a577-46c3-b4fa-caf7ae49a6a3</
saml:AttributeValue>
     </saml:Attribute>
</saml:AttributeStatement>
```

In the preceding example, an assertion contains two attributes, `"userName"` and `"userEmail"`. If header-based authentication is configured only for `"userName"`, with the header name being `"HTTP_USER_NAME"`, then the header is sent as: `"HTTP_USER_NAME: idmadmin"` Since `"userEmail"` is not configured on Unified Access Gateway for header-based authentication, it is not sent as a header.

2. SAML response expected from IDP for multi-valued SAML attribute

```
<saml:AttributeStatement>
     <saml:Attribute Name="group" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <saml:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">All Employees</saml:AttributeValue>
            <saml:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">All Contractors</saml:AttributeValue>
            <saml:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">All Executives</saml:AttributeValue>
            <saml:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">All</saml:AttributeValue>
     </saml:Attribute>
</saml:AttributeStatement>
```

In the preceding example, an attribute `"group"` contains four values, namely `"All Employees"`, `"All Contractors"`, `"All Executives"`, and `"All"`. If header-based authentication is configured only for `"group"`, with the header name being `"HTTP_GROUP"`, the header is sent as `"HTTP_GROUP: All Employees, All Contractors, All Executives, All"` with a comma-separated list of all the attribute values as the header value.

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 Unified Access Gateway version 3.0, you can delete previously defined realms.

Important In case of a cross domain set up, add details of all the realms including primary and secondary or sub-domains and associated KDC information. Ensure that trust is enabled between 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.

You can also generate the keytab file using the command-line. For example:

```
ktpass /princ HOST/username@domain.com /ptype KRB5_NT_PRINCIPAL /pass * /out C:\Temp
\kerberos.keytab /mapuser uagkerberos /crypto All
```

See the Microsoft documentation for detailed information about the `ktpass` command.

Prerequisites

You must have 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 Management Appliance Configuration Templates section, click **Add**.

2   In the Identity Bridging Settings section, click **Configure**.

3   In the Kerberos KeyTab Settings page, click Add **New KeyTab**.

4   Enter a unique name as the identifier.

5   (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.

     Ensure 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, keytab upload fails.

6 In the **Select Keytab file** text box, 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.

7 Click **Save**.

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

To configure a web reverse proxy for identity bridging (SAML to Kerberos), you must have saved the identity provider metadata file to Unified Access Gateway.

You can then enable identity bridging on the admin console and configure the external host name for the 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

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

If you are 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 console, click **Select** under **Configure Manually**.

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 a Web Reverse Proxy for Identity Bridging (SAML to Kerberos)

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

You must have configured the following Identity Bridging Settings on the Unified Access Gateway admin console. You can find these settings under the **Advanced Settings** section.

- 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.

Ensure that TCP/UDP port 88 is open since Unified Access Gateway uses this port for the Kerberos communication with Active Directory.

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 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 the web reverse proxy.
Instance Id	Unique name for the web reverse proxy instance.
Proxy Destination URL	Specify the internal URI 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	Enter the matching URI paths that forward to the destination URL. For example, enter as `(/|/SAAS(.*)|/hc(.*)|/web(.*)|/catalog-portal(.*))`. Note: When you configure multiple reverse proxies, provide the hostname in the proxy host pattern

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

Option	Description
Auth Methods	The default is to use pass-through authentication of the user name and password. The authentication methods you configured in Unified Access Gateway are listed in the drop-down menus. RSA SecurID, RADIUS, and Device Certificate Auth methods are supported.
Health Check URI Path	Unified Access Gateway connects to this URI path to check the health of your web application.
SAML SP	Required when you configure Unified Access Gateway as an 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 with Unified Access Gateway, their names must be unique.
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>`.
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(.*)|/SAAS/auth/wsfed/services(.*)|/SAAS/auth/wsfed/active/logon(.*))`
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.
Trusted Certificates	Add a trusted certificate to this edge service. Click '+' to select a certificate in PEM format and add to the trust store. Click '-' to remove a certificate from the trust store. By default, the alias name is the filename of the PEM certificate. Edit the alias text box to provide a different name.

Option	Description
Response Security Headers	Click '+' to add a header. Enter the name of the security header. Enter the value. Click '-' to remove a header. Edit an existing security header to update the name and the value of the header. **Important** The header names and values are saved only after you click **Save**. Some standard security headers are present by default. The headers configured are added to the Unified Access Gateway response to client only if the corresponding headers are absent in the response from the configured back-end server. **Note** Modify security response headers with caution. Modifying these parameters might impact the secure functioning of Unified Access Gateway .
Host Entries	Enter the details to be added in `/etc/hosts` file. Each entry should include 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`. Click the '+" sign to add multiple host entries. **Important** The host entries are saved only after you click **Save**.

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

8 Configure the following Identity Bridging settings.

Option	Description
Authentication Types	Select SAML.
SAML Attributes	List of SAML attributes that is passed as request headers. This option is visible only when **Enable Identity Bridging** is set to **Yes** and **Authentication Types** is set to **SAML**. Click '+' to a SAML attribute as part of the header.
Identity Provider	From the drop-down menu, select the identity provider.
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.

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

Save the service provider metadata file.

10 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.

Add the 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

You must have saved the Unified Access Gateway Service Provider Metadata file 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.

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

Configure the Workspace ONE UEM console to fetch and use CA certificates before you configure the Unified Access Gateway bridging feature to provide single sign-on (SSO) to On-Premises legacy non-SAML applications using certificate validation.

Enable Workspace ONE UEM Console to Fetch and Use CA Certificates

You can add a user template in the CA server and configure the settings in the Workspace ONE UEM console to enable Workspace ONE UEM to fetch and use the CA certificates.

Procedure

1 Add a User Template

Add a user template in the CA server as a first step to enable Workspace ONE UEM to fetch certificates.

2 Add a Certificate Authority in the Console

Add a Certificate Authority (CA) in the Workspace ONE UEM console.

3 Add a Certificate Authority Request Template

Add a CA request template after you have added a Certificate Authority in the Workspace ONE UEM console.

4 Update Security Policies to Use the Fetched CA Certificate

Update the security policies in the Workspace ONE UEM console to use the CA fetched certificate.

Add a User Template

Add a user template in the CA server as a first step to enable Workspace ONE UEM to fetch certificates.

Procedure

1 Log in to the server where the CA is configured.

2 Click **Start** and type `mmc.exe`.

3 In the **MMC** window, go to **File > Add/Remove Snap-in**.

4 In the **Add or Remove Snap-ins** window, select **Certificate Templates** and click **Add**.

5 Click **OK**.

6 In the **Certificates templates** window, scroll down and select **User > Duplicate Template**,

7 In the **Properties of new Template** window, select the **General** tab and provide a name for the **Template Display Name** .

The **Template Name** is automatically populated with this name, without the space.

8 Select the **Subject Name** tab and select **Supply in the request**.

9 Click **Apply** and then click **OK**.

10 In the **MMC** window, go to **File > Add/Remove Snap-in**.

11 In the **Add or Remove Snap-ins** window, select **Certificate Authority** and click **Add**.

12 In the **MMC** window, select **Certificate Authority > Certificate Template**.

13 Right-click **Certificate Authority** and select **New > Certificate Template to Issue**.

14 Select the template you created in Step 6.

What to do next

Verify that the template you added is displayed in the list.

Log in to the Workspace ONE UEM console and add a CA.

Add a Certificate Authority in the Console
Add a Certificate Authority (CA) in the Workspace ONE UEM console.

Prerequisites

■ You must have added a user template in the CA server.

■ You must have the name of the CA Issuer. Log in to the Active Directory(AD) server and run the `certutil` command from the command prompt to get the CA Issuer name.

■ Specify the *Username* for the CA to be of type *service account*.

Procedure

1 Log in to the Workspace ONE UEM console and select the appropriate Organization Group.

2 Go to **All Settings** and click **Enterprise Integration > Certificate Authorities** from the drop-down menu.

3 Click the **Certificate Authorities** tab and click **Add**.

4 Enter the following information for the Certificate Authority:

Option	Description
Name	A valid name for the CA
Authority Type	Microsoft ADCS
Protocol	ADCS
Server Hostname	Hostname of AD Server
Authority Name	CA Issuer Name
Authentication	Service Account
Username	User name with a service account in the form *domain\username*.
Password	Password for the user name
Additional Options	None

5 Click **Save**.

Add a Certificate Authority Request Template

Add a CA request template after you have added a Certificate Authority in the Workspace ONE UEM console.

Prerequisites

1 You must have added a user template in the CA server.

2 You must have added a CA in the Workspace ONE UEM console.

Procedure

1 Log in to Workspace ONE UEM console, go to **All Settings** and click **Enterprise Integration > Certificate Authorities** from the drop-down list.

2 Click the **Request Templates** tab and click **Add**.

3 Enter the following information for the template:

Option	Description
Name	A valid name for the certificate template
Description (optional)	Description of the template
Certificate Authority	The certificate authority added earlier
Issuing Template	Name of the user template created in the CA server
Subject Name	To add the Subject Name, keep the cursor on the value field (after the default value 'CN='), and click the '+' button, and select the appropriate email address
Private Key Length	2048
Private Key Type	Select *Signing*
SAN Type	Click **Add** and choose *User Principal Name*
Automatic Certificate Renewal (optional)	
Enable Certificate Revocation (optional)	
Publish Private Key (optional)	

4 Click **Save**.

Update Security Policies to Use the Fetched CA Certificate

Update the security policies in the Workspace ONE UEM console to use the CA fetched certificate.

Prerequisites

Procedure

1 Log in to the Workspace ONE UEM console, go to **All Settings** and click **Apps > Security & Policies > Security Policies** from the drop-down menu.

2 Select **Override** for Current Settings.

3 Enable **Integrated Authentication**.

    a   Select **Use Certificate**.

    b   Set the **Credential Source** to **Defined Certificate Authority**.

    c   Specify the **Certificate Authority** and **Certificate Template** set earlier.

4 Set **Allowed Sites** to *.

5 Click **Save**.

Configure 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 that you have the following files and certificates 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 user

- You must have added and uploaded a certificate in the Workspace ONE UEM console. See Enable Workspace ONE UEM Console to Fetch and Use CA Certificates.

See the relevant product documentation to generate the root and user certificates and the keytab file for non-SAML applications.

Ensure that TCP/UDP port 88 is open since Unified Access Gateway uses this port for Kerberos communication with Active Directory.

Procedure

1 From **Authentication Settings > X509 Certificate**, go to:

    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 check box for **Enable OCSP Revocation**.

d   Enter the OCSP responder URL in the **OCSP URL** text box.

Unified Access Gateway sends the OCSP request to the specified URL and receives a response that contains information indicating whether or not the certificate is revoked.

e   Select the check box **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 defaults to the value in the OCSP URL text box.

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.

What to do next

When you use the Workspace ONE Web to access the target website, the target website acts 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 specific error messages and troubleshooting information, see Troubleshooting Errors: Identity Bridging.

Workspace ONE UEM Components on Unified Access Gateway

You can deploy VMware Tunnel using the Unified Access Gateway appliance. Unified Access Gateway supports deployment on either ESXi or Microsoft Hyper-V environments. VMware Tunnel provides a secure and effective method for individual applications to access corporate resources. Content Gateway (CG) is a component of the Workspace ONE UEM Content Management solution that securely allows access to On-Premise repository content on mobile devices.

DNS Requirements for VMware Tunnel and Content Gateway

When VMware Tunnel and Content Gateway services are enabled on the same appliance, and TLS Port Sharing is enabled, the DNS names must be unique for each service. When TLS is not enabled only one DNS name can be used for both services as the port will differentiate the incoming traffic.

Deploying 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 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 single or multi-tier network architecture models.

Both Tunnel Proxy and Per-App Tunnel deployment models can be used for a multi-tier network on the Unified Access Gateway 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 Workspace ONE Web or any Workspace ONE SDK enabled application deployed from Workspace ONE UEM. 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 Workspace ONE UEM console. Typically, this component should be used when there are unmanaged devices that need secured access to internal resources.

For fully enrolled devices, the Per-App Tunnel component enables devices to connect to internal resources without needing the Workspace ONE SDK. This component uses 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, refer to the latest Tunnel documentation from the Workspace ONE UEM documentation page.

Deploying the VMware Tunnel for your Workspace ONE UEM environment involves the following:

1   Set up the initial hardware.

2   Configure the VMware Tunnel hostname and port information in the Workspace ONE UEM console. See Firewall Rules for DMZ-Based Unified Access Gateway Appliances.

3   Download and deploy the Unified Access Gateway OVF template.

4   Manually configure the VMware Tunnel.

Figure 4-10. VMware Tunnel Multi-Tier Deployment: Proxy and Per-App Tunnel
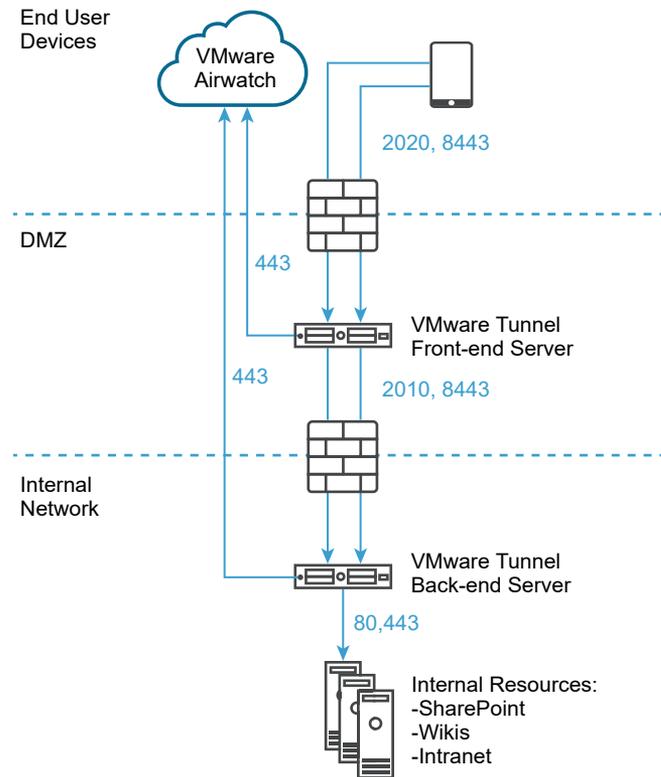
AirWatch v9.1 and above supports Cascade Mode as the Multi-Tier deployment model for VMware Tunnel. Cascade Mode requires a dedicated inbound port for each Tunnel component from the internet to the front-end Tunnel server. Both the front-end and back-end servers must be able to communicate with the Workspace ONE UEM API and AWCM servers. VMware Tunnel **Cascade** mode supports the multi-tier architecture for the Per-App Tunnel component.

For load balancing considerations for Content Gateway and Tunnel Proxy, see Unified Access Gateway Load Balancing Topologies.

Go to the VMware Workspace ONE UEM documentation page for a complete list of Workspace ONE UEM guides and release notes.

Configure VMware Tunnel Proxy

Configure VMware Tunnel Proxy using the configuration wizard. The options configured in the wizard are packaged in the installer, which you can download from the Workspace ONE UEM console and move to your Tunnel servers.

Configure the VMware Tunnel Proxy in the UEM console under **Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel > Proxy**. The wizard walks you through the installer configuration step-by-step. The options configured in the wizard are packaged in the installer, which you can download from the Workspace ONE UEM console and move to your Tunnel servers. Changing the details in this wizard typically requires a reinstall of the VMware Tunnel with the new configuration.

To configure the VMware Tunnel Proxy, you need the details of the server where you plan to install. Before configuration, determine the deployment model, one or more hostnames and ports, and which features of VMware Tunnel to implement, such as access log integration, SSL offloading, enterprise certificate authority integration, and so on.

Note The wizard dynamically displays the appropriate options based on your selections, the configuration screens may display different text boxes and options.

Procedure

1   Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel > Proxy**.

- If this is your first time configuring VMware Tunnel, then select **Configure** and follow the configuration wizard screens.

- If this is not your first time configuring VMwareTunnel, select **Override**, then select **Enabled VMware Tunnel** toggle switch, and then select **Configure**.

2   On the **Deployment Type** screen, select **Enable Proxy (Windows & Linux)** toggle switch, and then select the components that you want to configure using the **Proxy Configuration Type** drop-down menu.

3   In the drop-down menus that display, select whether you are configuring a **Relay-Endpoint**, or the **Proxy Configuration Type** deployment. Select the information icon to see an example for the selected type.

4   Select **Next**.

5   On the **Details** screen, configure the following settings. The options that are displayed on the **Details** screen depends on the configuration type you have selected in the the **Proxy Configuration Type** drop-down menu.

- **Basic Proxy Configuration Type**, enter the following information:

Setting	Description
Hostname	Enter the FQDN of the public host name for the Tunnel server, for example, tunnel.acmemdm.com. This hostname must be publicly available as it is the DNS that devices connect to from the Internet.
Relay Port	The proxy service is installed on this port. Devices connect to the <relayhostname>:<port> to use the VMware Tunnel proxy feature. The default value is 2020.
Relay Host Name	(Relay-Endpoint Only). Enter the FQDN of the public host name for the Tunnel relay server, for example, tunnel.acmemdm.com. This hostname must be publicly available as it is the DNS that devices connect to from the Internet.

Setting	Description
Enable SSL Offloading	Select this checkbox if you want to use SSL Offloading to ease the burden of encrypting and decrypting traffic from the VMware Tunnel server.
Use Kerberos Proxy	Enable Kerberos proxy support to allow access to Kerberos authentication for your target back end Web services. This feature does not currently support Kerberos Constrained Delegation (KCD). For more information, see Configure Kerberos Proxy Settings. The Endpoint server must be on the same domain as KDC for the Kerberos Proxy to communicate successfully with the KDC.

◆ If you choose **Relay-Endpoint Proxy Configuration Type**, enter the following information:

Setting	Description
Relay Host Name	(Relay-Endpoint Only). Enter the FQDN of the public host name for the Tunnel relay server, for example, tunnel.acmemdm.com. This hostname must be publicly available as it is the DNS that devices connect to from the Internet.
Endpoint Host Name	The internal DNS of the Tunnel endpoint server. This value is the hostname that the relay server connects to on the relay-endpoint port. If you plan to install the VMware Tunnel on an SSL offloaded server, enter the name of that server in place of the **Host Name**. When you enter the **Host Name**, do not include a protocol, such as http://, https://, etc.
Relay Port	The proxy service is installed on this port. Devices connect to the <relayhostname>:<port> to use the VMware Tunnel proxy feature. The default value is 2020.
Endpoint Port	(Relay-Endpoint only). This value is the port used for communication between the VMware Tunnel relay and VMware Tunnel endpoint. The default value is 2010. If you are using a combination of Proxy and Per-App Tunnel, the relay endpoint installs as part of the Front-End Server for Cascade mode. The ports should be different values.
Enable SSL Offloading	Select this checkbox if you want to use SSL Offloading to ease the burden of encrypting and decrypting traffic from the VMware Tunnel server.
Use Kerberos Proxy	Enable Kerberos proxy support to allow access to Kerberos authentication for your target back end Web services. This feature does not currently support Kerberos Constrained Delegation (KCD). For more information, see Configure Kerberos Proxy Settings. The Endpoint server must be on the same domain as KDC for the Kerberos Proxy to communicate successfully with the KDC. In the **Realm** field, enter the Realm of the KDC server.

6 Select **Next**.

7 On the **SSL** screen, you can configure Public SSL Certificate that secures client-server communication from enabled application on a device to the VMware Tunnel. By default, this setup uses a AirWatch certificate for secure server-client communication.

    a   Select **Use Public SSL Certificate** option if you prefer to use a third-party SSL certificate for encryption between Workspace ONE Web or SDK-enabled apps and the VMware Tunnel server.

    b   Select **Upload** to upload a .PFX or .P12 certificate file and enter the password. This file must contain both your public and private key pair. CER and CRT files are not supported.

8 Select **Next**.

9 On the **Authentication** screen, configure the following settings to select the certificates that devices use to authenticate to the VMware Tunnel.

By default, all the components uses AirWatch issued certificates. To use Enterprise CA certificates for client-server authentication, select the **Enterprise CA** option.

    a   Select **Default** to use AirWatch issued certificates. The default AirWatch issued client certificate does not automatically renew. To renew these certificates, re-publish the VPN profile to devices that have an expiring or expired client certificate. View the certificate status for a device by navigating to **Devices > Device Details > More > Certificates**.

    b   Select **Enterprise CA** in place of AirWatch issued certificates for authentication between the Workspace ONE Web, Per-App Tunnel-enabled apps, or SDK-enabled apps and the VMware Tunnel requires that a certificate authority and certificate template are set up in your Workspace ONE UEM environment before configuring VMware Tunnel.

    c   Select the **Certificate Authority** and **Certificate Template** that are used to request a certificate from the CA.

    d   Select **Upload** to upload the full chain of the public key of your certificate authority to the configuration wizard.

        The CA template must contain CN=UDID in the subject name. Supported CAs are ADCS, RSA, and SCEP.

        Certificates auto-renew based on your CA template settings.

10 Click **Add** to add an Intermediate Certificate.

11 Select **Next**.

12 On the **Miscellaneous** screen, you can enable access logs for the proxy or Per-App Tunnel components. Enable **Access Logs** toggle switch to configure the feature.

If you intend to use this feature you must configure it now as part of the configuration, as it cannot be enabled later without reconfiguring Tunnel and rerunning the installer. For more information on these settings, see #unique_76 and Configure Advanced Settings for VMware Tunnel.

a Enter the URL of your syslog host in the **Syslog Hostname** field. This setting displays after you enable Access Logs.

b Enter the port over which you want to communicate with the syslog host in the **UDP Port** field.

13 Select **Next,** review the summary of your configuration, confirm that all hostnames, ports and settings are correct, and select **Save**.

The installer is now ready to download on the VMware Tunnel **Configuration** screen.

14 On the **Configuration** screen, select the **General** tab. The **General** tab allows you to do the following:

a You can select **Test Connection** to verify the connectivity.

b You can select **Download Configuration XML** to retrieve the existing VMware Tunnel instance configuration as a XML file.

c You can select the **Download Unified Access Gateway** hyperlink. This button downloads the non-FIPS OVA file. The download file also includes the PowerShell script and .ini template file for the PowerShell deployment method. You must download the VHDX or FIPS OVA from My Workspace ONE.

d For legacy installer methods, you can select **Download Windows Installer**.

This button downloads a single BIN file used for deploying the VMware Tunnel server. Configuration XML file required for installation can be downloaded from the Workspace ONE UEM console after confirming the certificate password.

15 Select **Save**.

Single-Tier Deployment Model

If you are using the single-tier deployment model, use the basic-endpoint mode. The basic endpoint deployment model of VMware Tunnel is a single instance of the product installed on a server with a publicly available DNS.

Basic VMware Tunnel is typically installed in the internal network behind a load balancer in the DMZ that forwards traffic on the configured ports to the VMware Tunnel, which then connects directly to your internal Web applications. All deployment configurations support load balancing and reverse proxy.

The basic endpoint Tunnel server communicates with API and AWCM to receive a whitelist of clients allowed to access VMware Tunnel. Both proxy and Per-App Tunnel components support using an outbound proxy to communicate with API/AWCM in this deployment model. When a device connects to VMware Tunnel, it is authenticated based on unique X.509 certificates issued by Workspace ONE UEM. Once a device is authenticated, the VMware Tunnel (basic endpoint) forwards the request to the internal network.

If the basic endpoint is installed in the DMZ, the proper network changes must be made to allow the VMware Tunnel to access various internal resources over the necessary ports. Installing this component behind a load balancer in the DMZ minimizes the number of network changes to implement the VMware Tunnel and provides a layer of security because the public DNS is not pointed directly to the server that hosts the VMware Tunnel.
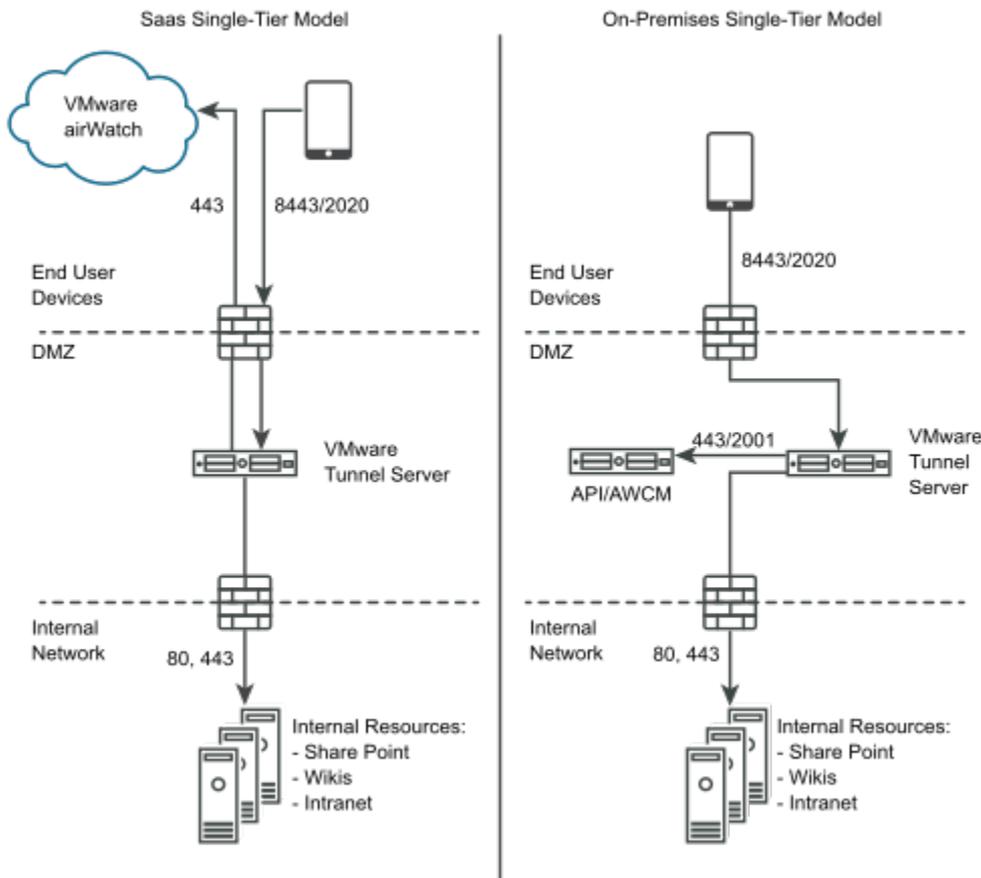
Cascade Mode Deployment

The cascade deployment model architecture includes two instances of the VMware Tunnel with separate roles. In cascade mode, the front-end server resides in the DMZ and communicates to the back-end server in your internal network.

Only the Per-App Tunnel component supports the cascade deployment model. If you use only the Proxy component, you must use the Relay-Endpoint model. For more information, see Relay-Endpoint Deployment.

Devices access the front-end server for cascade mode using a configured hostname over configured ports. The default port for accessing the front-end server is port 8443. The back-end server for cascade mode is installed in the internal network hosting your intranet sites and web applications. This deployment model separates the publicly available front-end server from the back-end server that connects directly to internal resources, providing an extra layer of security.

The front-end server facilitates authentication of devices by connecting to AWCM when requests are made to the VMware Tunnel. When a device makes a request to the VMware Tunnel, the front-end server determines if the device is authorized to access the service. Once authenticated, the request is forwarded securely using TLS over a single port to the back-end server.

The back-end server connects to the internal DNS or IP requested by the device.

Cascade mode communicates using TLS connection (or optional DTLS connection). You can host as many front-end and back-end servers as you like. Each front-end server acts independently when searching for an active back-end server to connect devices to the internal network. You can set up multiple DNS entries in a DNS lookup table to allow load balancing.

Both the front-end and back-end servers communicate with the Workspace ONE UEM API server and AWCM. The API server delivers the VMware Tunnel configuration and the AWCM delivers device authentication, whitelisting, and traffic rules. The front-end and back-end server communicates with API/AWCM through direct TLS connections unless you enable outbound proxy calls. Use this connection if the front-end server cannot reach the API/AWCM servers. If enabled, front-end servers connect through the back-end server to the API/AWCM servers. This traffic, and the back-end traffic, route using server-side traffic rules. For more information, see Network Traffic Rules for Per-App Tunnel

The following diagram illustrates the Multi-Tier deployment for the Per-App Tunnel component in cascade mode:
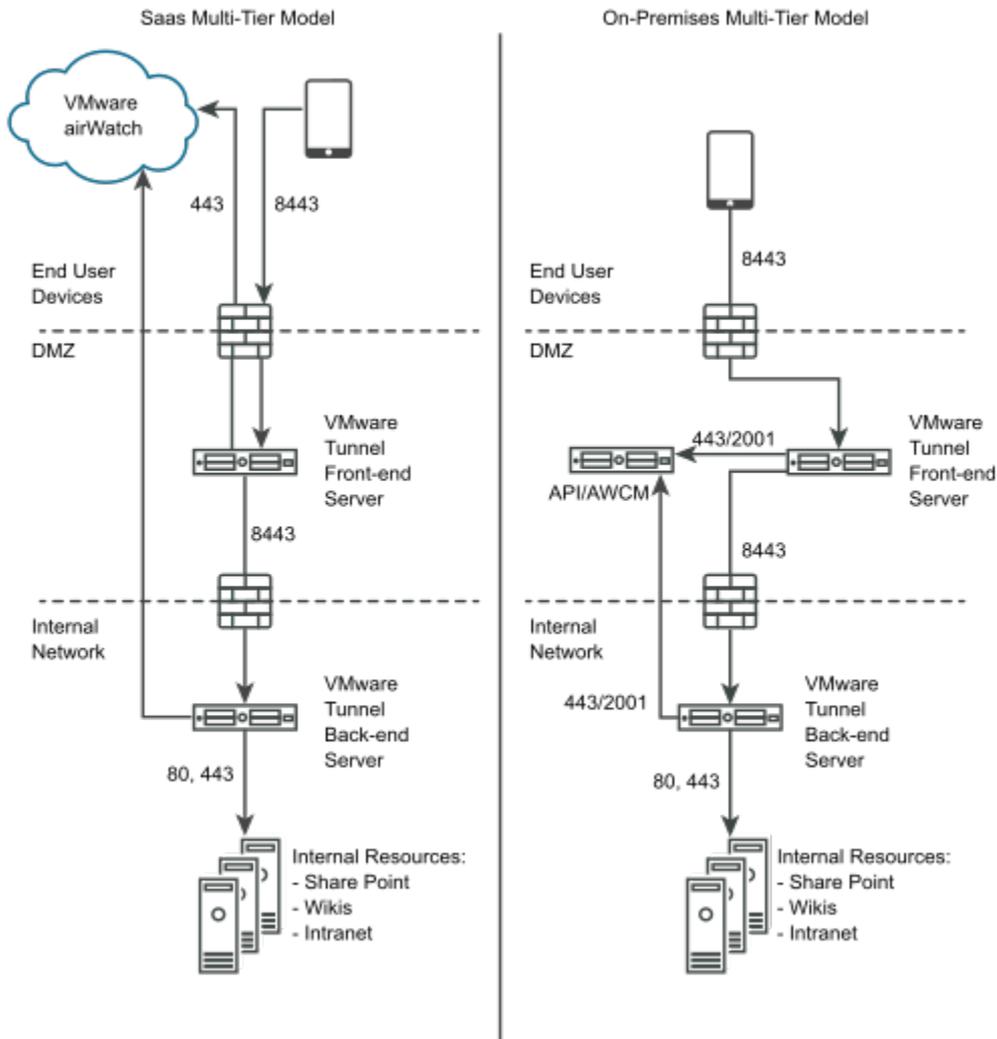
Relay-Endpoint Deployment

If you are using a multi-tier deployment model and the Proxy component of the VMware tunnel, use the relay-endpoint deployment mode. The relay-endpoint deployment mode architecture includes two instances of the VMware Tunnel with separate roles. The VMware Tunnel relay server resides in the DMZ and can be accessed from public DNS over the configured ports.

If you are only using the Per-App Tunnel component, consider using a cascade mode deployment. For more information, see Cascade Mode Deployment.

The ports for accessing the public DNS are by default port 8443 for Per-App Tunnel and port 2020 for proxy. The VMware Tunnel endpoint server is installed in the internal network hosting intranet sites and Web applications. This server must have an internal DNS record that is resolved by the relay server. This deployment model separates the publicly available server from the server that connects directly to internal resources, providing an added layer of security.

The relay server role includes communicating with the API and AWCM components and authenticating devices when requests are made to VMware Tunnel. In this deployment model, communication to API and AWCM from the relay server can be routed to the Outbound Proxy via endpoint server. The Per-App Tunnel service must communicate with API and AWCM directly. When a device makes a request to the VMware Tunnel, the relay server determines if the device is authorized to access the service. Once authenticated, the request is forwarded securely using HTTPS over a single port (the default port is 2010) to the VMware Tunnel endpoint server.

The role of the endpoint server is to connect to the internal DNS or IP requested by the device. The endpoint server does not communicate with the API or AWCM unless **Enable API and AWCM outbound calls via proxy** is set to **Enabled** in the VMware Tunnel settings in the Workspace ONE UEM console. The relay server performs health checks at a regular interval to ensure that the endpoint is active and available.

These components can be installed on shared or dedicated servers. Install VMware Tunnel on dedicated Linux servers to ensure that performance is not impacted by other applications running on the same server. For a relay-endpoint deployment, the proxy and Per-App Tunnel components are installed on the same relay server.

Figure 4-11. On-premises configuration for Relay-Endpoint deployments
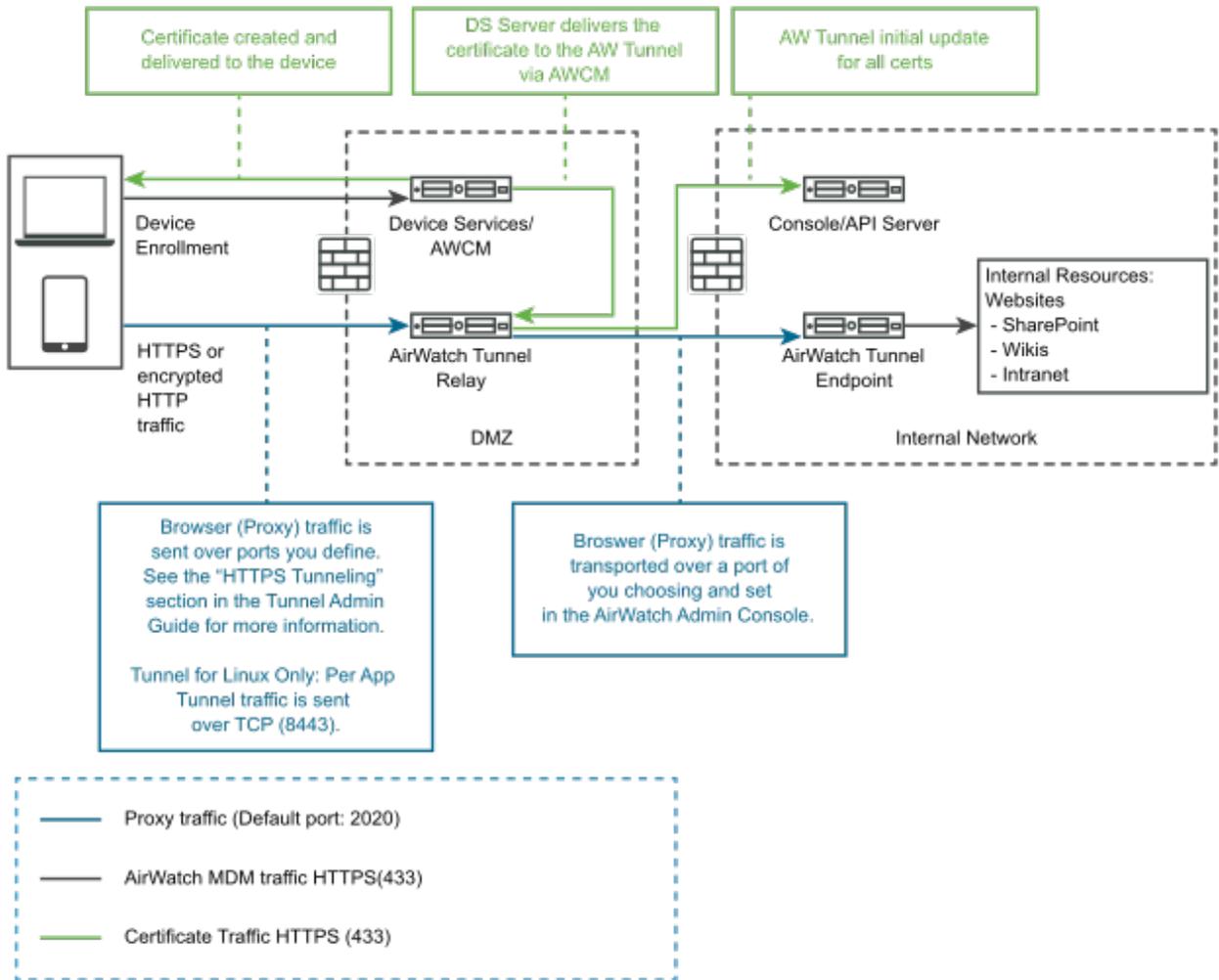
Figure 4-12. SaaS configuration for Relay-Endpoint deployments
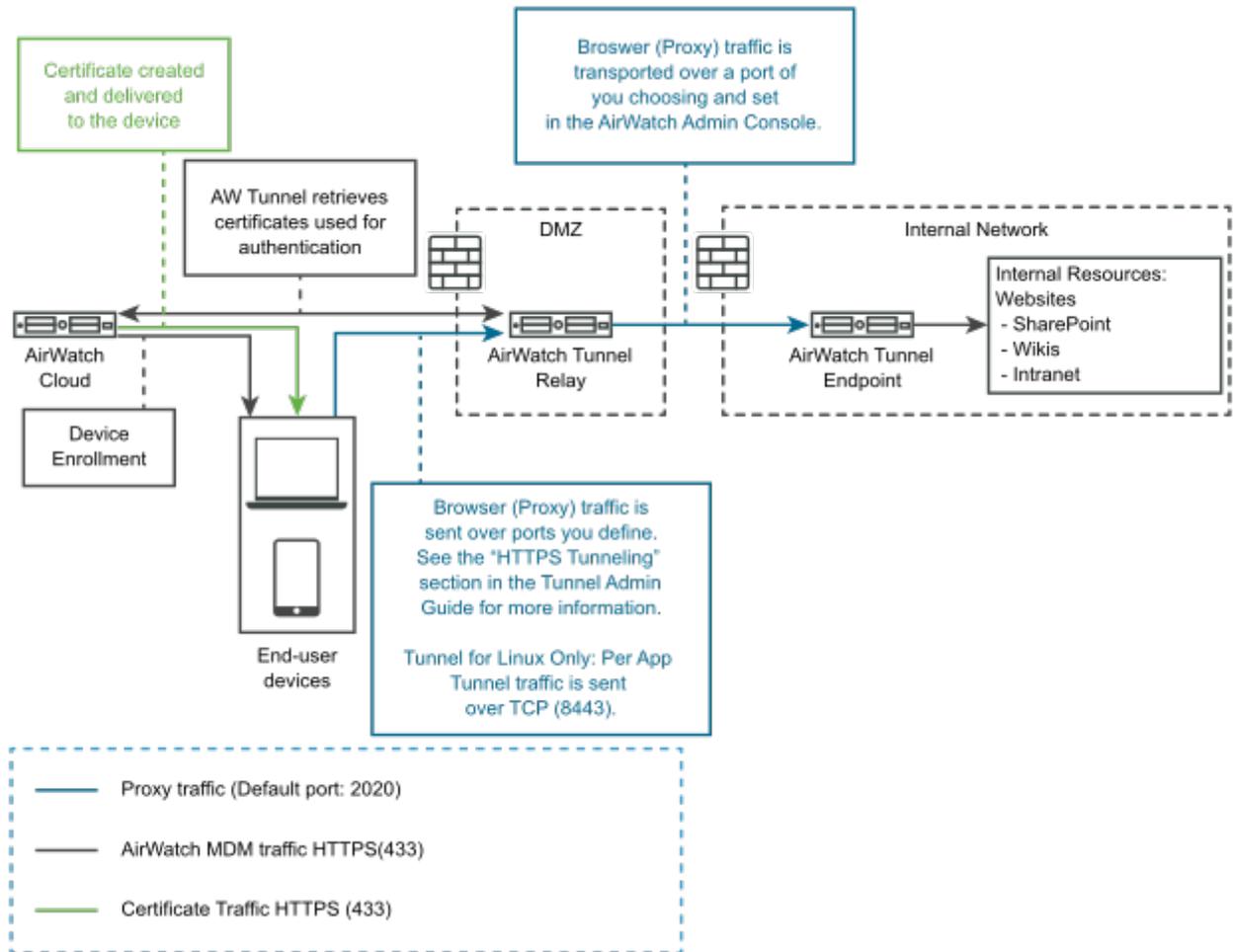
Configure VMware Tunnel Settings for Workspace ONE UEM

Tunnel proxy deployment secures the network traffic between an end user device and a website through the Workspace ONE Web mobile application.

Procedure

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

2   Navigate to **General Settings > Edge Service Settings** and 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 theWorkspace ONE UEM 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.

Option	Description
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 Workspace ONE UEM 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 Workspace ONE UEM console.
Host Entries	Enter the details to be added in `/etc/hosts` file. Each entry should include 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 example-alias`. Click the '+' sign to add multiple host entries.
	Important The host entries are saved only after you click **Save**.
Trusted Certificates	Select the trusted certificate files in PEM format, to be added to the trust store. By default, the alias name is the filename of the PEM certificate. Edit the alias text box to give a different name.

7   Click **Save**.

Deployment of VMware Tunnel for Workspace ONE UEM using PowerShell

You can use PowerShell to deploy the VMware Tunnel for Workspace ONE UEM.

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

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

About TLS Port Sharing

TLS port sharing is enabled by default on Unified Access Gateway whenever multiple edge services are configured to use TCP port 443. Supported edge services are VMware Tunnel (Per-App VPN), Content Gateway and Web reverse proxy.

Note If you want TCP port 443 to be shared, ensure that each configured edge service has a unique external hostname pointing to Unified Access Gateway.

Content Gateway on Unified Access Gateway

Content Gateway (CG) is a component of the Workspace ONE UEM Content Management solution that securely allows access to On-premise repository content on mobile devices.

Prerequisites

You must configure the Content Gateway node using the Workspace ONE UEM console before you can configure Content Gateway on Unified Access Gateway. After configuring the node, note down the *Content Gateway Configuration GUID*, which is automatically generated.

Note The acronym CG is also used to refer to Content Gateway.

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

Option	Description
Identifier	Indicates that this service is enabled.
API Server URL	The Workspace ONE UEM 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	User name to log into the API server.
	Note It is required that the admin account have, at a minimum, the permissions associated with the Content Gateway role
API Server Password	Password to log into the API server.
CG Hostname	Host name used to configure edge settings.

Option	Description
CG Configuration GUID	Workspace ONE UEM Content Gateway configuration ID. This ID is automatically generated when the Content Gateway is configured on the Workspace ONE UEM console. The Configuration GUID is displayed on the Content Gateway page on the UEM console under **Settings > Content > Content Gateway**.
Outbound Proxy Host	The host where the outbound proxy is installed. Unified Access Gateway makes a connection to API Server through an outbound proxy if configured.
Outbound Proxy Port	Port of the outbound proxy.
Outbound Proxy Username	User name to log into the outbound proxy.
Outbound Proxy Password	Password to log into the outbound proxy.
NTLM Authentication	Specify whether the outbound proxy requires NTLM authentication.
Trusted Certificates	Add a trusted certificate to this edge service. Click '+' to select a certificate in PEM format and add to the trust store. Click '-' to remove a certificate from the trust store. By default, the alias name is the filename of the PEM certificate. Edit the alias text box to give a different name.
Host Entries	Enter the details to be added in `/etc/hosts` file. Each entry should include 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`. Click '+' to add multiple host entries. **Important** The host entries are saved only after you click **Save**.

Note HTTP traffic is not allowed for Content Gateway on port 80 on Unified Access Gateway, because TCP port 80 is used by the edge Service Manager.

4   Click **Save**.

Content Gateway Configuration

Configure Content Gateway settings in the Workspace ONE UEM console to establish a node and pre-configure the settings that get bundled into the configuration file, eliminating the need to configure the settings manually post-installation on the server.

Configuration includes selecting the platform, configuration model, associated ports, and if necessary, uploading an SSL certificate.

From Workspace ONE UEM console version 9.6 onwards, Unified Access Gateway (UAG) is the recommended installation type when configuring a Content Gateway node. You can use this option to configure a new Content Gateway on Unified Access Gateway or to migrate your existing Content Gateway to Unified Access Gateway.

For more info about configuring Content Gateway on Unified Access Gateway, see Workspace ONE UEM Components on Unified Access Gateway in the UAG documentation. For information about migration, see Migrating Content Gateway to Unified Access Gateway documentation.

Procedure

1   Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Content Gateway** in the Organization Group of your choice.

2   Set **Enable the Content Gateway** to **Enabled**.

You might need to select **Override** to unlock Content Gateway settings.

3   Click **Add**.

4   Complete the fields that appear to configure a Content Gateway instance.

a   Configure the **Installation Type**.

Setting	Description
Installation Type	Select the Operating System for the Content Gateway server.

b   Configure the **Content Configuration** settings.

Setting	Description
Configuration Type	■ **Basic** – Endpoint configuration with no relay component. ■ **Relay** – Endpoint configuration with a relay component.
Name	Provide a unique name used to select this Content Gateway instance when attaching it to a Content Repository, Repository Template, or RFS Node.
Content Gateway Relay Address	If implementing a relay configuration, enter the URL used to access the Content Gateway Relay from the Internet.
Content Gateway Relay Port	If implementing a relay configuration, enter the relay server port.
Content Gateway Endpoint Address	Enter the host name of the Content Gateway endpoint. The Public SSL certificate bound on the configured port must be valid for this entry.
Content Gateway Endpoint Port	Enter the endpoint server port.

c   Configure the **Content SSL Certificate** settings.

Setting	Description
Public SSL Certificate (required for Linux requirements)	If necessary, upload a PKCS12 (.pfx) certificate file with a full chain for the Content Gateway Installer to bind to the port. The full chain includes a password, server certificate, intermediates, root certificate, and a private key. **Note** To ensure that your PFX file contains the entire certificate chain, you can run commands such as `certutil –dump myCertificate.pfx` or `openssl pkcs12 –in myCertificate.pfx –nokeys` using command line tools such as Certutil or OpenSSL. These commands display the complete certificate information. Requirements vary by platform and SSL configuration.
Ignore SSL Errors (not recommended)	If using a self-signed certificate, consider enabling this feature. If enabled, Content Gateway ignores certificate trust errors and certificate name mismatches.

ICAP Proxy configurations are not supported from Workspace ONE UEM console version 9.7. However, existing configurations can be edited. For information about configuring ICAP Proxy, see https://support.workspaceone.com/articles/115001675368.

5   Select **Add**.

6   Select **Save**.

What to do next

During configuration, you specify the platform and configuration model for Content Gateway. After configuring settings in the UEM Console, download the installer, configure additional nodes, or manage configured nodes.

Basic (Endpoint Only) Deployment Model for Content Gateway

The basic endpoint deployment model of VMware Content Gateway is a single instance of the product installed on a server with a publicly available DNS.

In the Basic deployment model, VMware Content Gateway is typically installed in the internal network behind a load balancer in the DMZ that forwards traffic on the configured ports to the VMware Content Gateway. VMware Content Gateway then connects directly to your internal content repositories. All deployment configurations support load balancing and reverse proxy.

The basic endpoint Content Gateway server communicates with the Devices Services. Device Services connects the end-user device to the correct Content Gateway.

If the basic endpoint is installed in the DMZ, the proper network changes must be made for the VMware Content Gateway to access various internal resources over the necessary ports. Installing this component behind a load balancer in the DMZ minimizes the number of network changes to implement the VMware Content Gateway. It provides a layer of security because the public DNS is not pointed directly to the server that hosts the VMware Content Gateway.
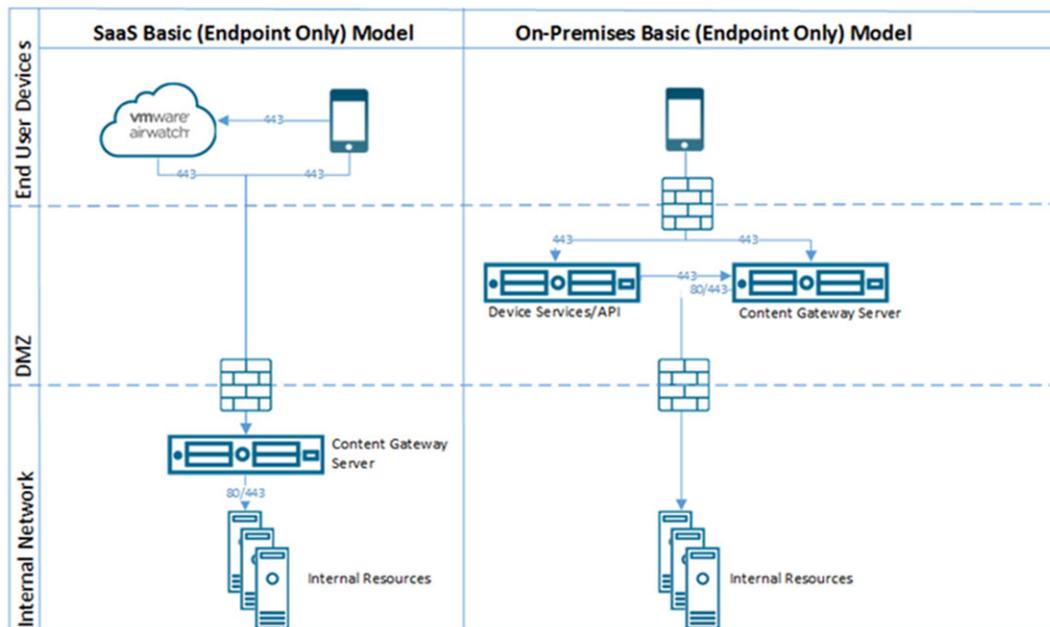
## Relay-Endpoint Deployment Model for Content Gateway

The relay-endpoint deployment model architecture includes two instances of the VMware Content Gateway with separate roles.

The VMware Content Gateway relay server resides in the DMZ and can be accessed from public DNS over the configured ports.

By default, 443 is the port for accessing the Content Gateway. The VMware Content Gateway endpoint server is installed in the internal network hosting internal resources. This server must have an internal DNS record that the relay server can resolve. This deployment model separates the publicly available server from the server that connects directly to internal resources, providing an added layer of security.

The role of the endpoint server is to connect to the internal repository or content requested by the device. The relay server performs health checks at a regular interval to ensure that the endpoint is active and available.

These components can be installed on shared or dedicated servers. To ensure that other applications running on the same server does not impact the performance, install VMware Content Gateway on dedicated servers.
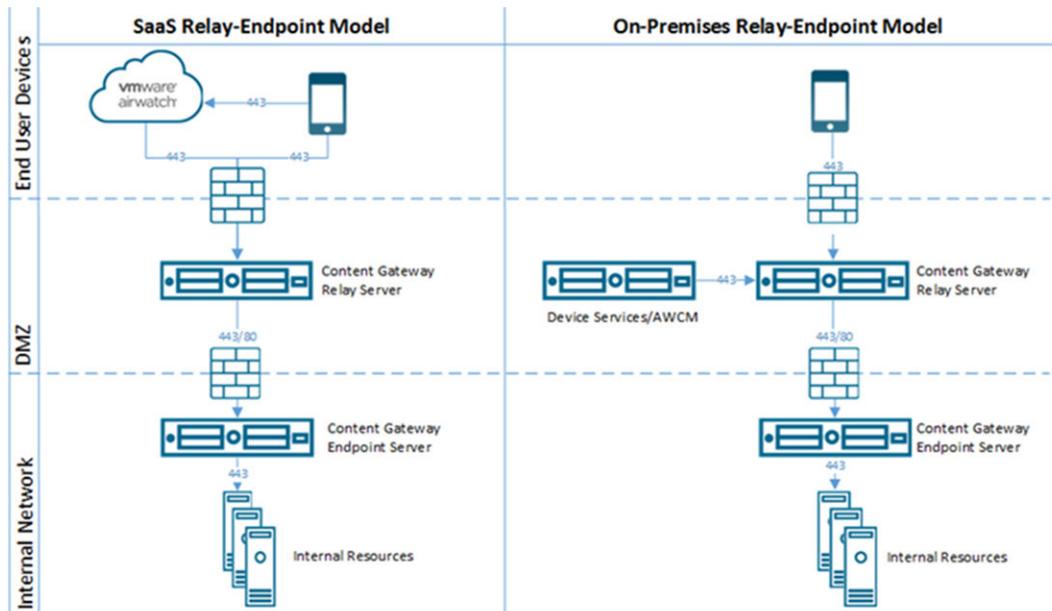
Secure Email Gateway on Unified Access Gateway

Secure Email Gateway is a component of Workspace ONE UEM that helps protect your mail infrastructure and enables Mobile Email Management (MEM) functionality.

Prerequisites

You must configure the Secure Email Gateway using the Workspace ONE UEM console before you can configure Secure Email Gateway on Unified Access Gateway. After configuring the node, note down the Secure Email Gateway Configuration GUID, which is automatically generated. For more information, see Secure Email Gateway documentation.

Note The acronym SEG is also used to refer to Secure Email Gateway.

Note Secure Email Gateway is supported by all the Unified Endpoint Management (UEM) versions.

Procedure

1 Navigate to **General Settings > Edge Service Settings > Secure Email Gateway Settings** and click the gearbox icon.

2 Select **YES** to enable Secure Email Gateway settings.

3 Configure the following settings.

Option	Default Value and Description
API Server URL	The Workspace ONE UEM 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 Secure Email Gateway configuration from API server.
API Server Username	User name to log into the API server. **Note** It is required that the admin account have, at a minimum, the permissions associated with the Secure Email Gateway role.
API Server Password	Password to log into the API server.
Secure Email Gateway Server Hostname	Host name used to configure edge settings.
MEM Configuration GUID	Workspace ONE UEM Mobile Email Management configuration ID. This ID is automatically generated when the Mobile Email Management is configured on the Workspace ONE UEM console. The Configuration GUID is displayed on the Mobile Email Management configuration page on the UEM console.
Outbound Proxy Host	The host where the outbound proxy is installed. Unified Access Gateway makes a connection to API Server through an outbound proxy if configured.
Outbound Proxy Port	Port of the outbound proxy.
Outbound Proxy Username	User name to log into the outbound proxy.
Outbound Proxy Password	Password to log into the outbound proxy.
Trusted Certificates	Add a trusted certificate to this edge service. Click '+' to select a certificate in PEM format and add to the trust store. Click '-' to remove a certificate from the trust store. By default, the alias name is the filename of the PEM certificate. Edit the alias text box to give a different name.
Host Entries	Enter the details to be added in /etc/hosts file. Each entry should include 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. Click '+' to add multiple host entries. **Note** The host entries are saved only after you click **Save**.

4 Click **Save**.

Changing logging levels for Secure Email Gateway on Unified Access Gateway

You can change the log levels for Secure Email Gateway in Unified Access Gateway.

Prerequisites

Enable SSH on the Linux virtual machine, if not already enabled.

Procedure

1   Connect to Unified Access Gateway Secure Email Gateway machine using Secure Shell.

2   Edit the log configuration file for SEG using the command.

```
vi /opt/vmware/docker/seg/container/config/logback.xml
```

3   Look for an appropriate logger for which you want to change the logging level. For example, `logger name="com.airwatch" groupKey="app.logger" level="error"`

4   Change the value of attribute `level` from `error` to any levels such as `warn,Info, Debug.`

5   Save the file.

Results

The logging level change reflects in the logs.

Enable EWS Proxy on SEG

SEG provides authorization and compliance for Exchange Web Services (EWS) traffic used by VMware Email Notification Service (ENS).

The following procedure describes the steps to enable EWS proxy on Secure Email Gateway.

Procedure

1   Connect to Unified Access Gateway Secure Email Gateway machine using Secure Shell.

2   Edit the properties file with the following command

```
vi /opt/vmware/docker/seg/container/config/override/application-override.properties
```

3   Add the entry in `application-override.properties` file.

```
enable.boxer.ens.ews.proxy=true
```

4   Save the file.

5   Save the SEG configuration on Unified Access Gateway Admin UI again.

Additional Deployment Use Cases

You can deploy Unified Access Gateway with multiple edge services on the same appliance, such as with Horizon and Web Reverse Proxy and Unified Access Gateway with VMware Tunnel, Content Gateway, and Web Reverse Proxy.

Considerations for Deploying Unified Access Gateway with Multiple Services

Note the following important considerations before you deploy the edge services together.

- Understand and meet the networking requirements - See Firewall Rules for DMZ-Based Unified Access Gateway Appliances.

- Follow sizing guidelines - See the sizing options section in the Deploy Unified Access Gateway Using the OVF Template Wizard topic.

- Horizon Connection Server does not work with an enabled web reverse proxy when there is an overlap in the proxy pattern. Therefore, if both Horizon and a web reverse proxy instance are configured and enabled with proxy patterns on the same Unified Access Gateway instance, remove the proxy pattern '/' from Horizon settings and retain the pattern in the web reverse proxy to prevent the overlap. Retaining the '/' proxy pattern in the web reverse proxy instance ensures that when a user clicks the URL of Unified Access Gateway, the correct web reverse proxy page is displayed. If only Horizon settings are configured, the above change is not required.

- When deploying Unified Access Gateway with the combined services of VMware Tunnel, Content Gateway, and Web Reverse Proxy, if you use the same port 443 for all the services, every service should have a unique external hostname. See About TLS Port Sharing.

- The different edge services can be configured independently using the Admin UI and you can import any previous settings if you want. When deploying with PowerShell, the INI file makes the deployment production-ready.

- If Horizon Blast and VMware Tunnel are enabled on the same Unified Access Gateway appliance, then VMware Tunnel must be configured to use a different port number other than 443 or 8443. If you want to use port 443 or 8443 for VMware Tunnel, you must deploy the Horizon Blast service on a separate Unified Access Gateway appliance.

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.

This chapter includes the following topics:

- Configuring TLS/SSL Certificates for Unified Access Gateway Appliances

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.

Results

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

You can update the default self-signed certificate with a CA-signed certificate. See Update SSL Server Signed Certificates. For smart card certificates, see Configuring Certificate or Smart Card Authentication on the Unified Access Gateway Appliance.

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.

Results

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 Only one of the two factor user authentication methods can be specified for an Edge Service. This can be Certificate/Smart Card authentication, RADIUS authentication, or RSA Adaptive Authentication.

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

This chapter includes the following topics:

- Configuring Certificate or Smart Card Authentication on the Unified Access Gateway Appliance
- Configure RSA SecurID Authentication in Unified Access Gateway
- Configuring RADIUS for Unified Access Gateway
- Configuring RSA Adaptive Authentication in Unified Access Gateway
- Generate Unified Access Gateway SAML Metadata

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 Horizon 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 certificate revocation lists (CRLs) and with the Online Certificate Status Protocol (OCSP) is supported. A CRL is a list of revoked certificates published by the CA that issued the certificates. OCSP is a certificate validation protocol that is used to get the revocation status of a certificate.

You can configure both CRL and OCSP in the certificate authentication adapter configuration. When you configure both types of certificate revocation checking and the **Use CRL** in case of **OCSP failure check box** is enabled, OCSP is checked first and if OCSP fails, revocation checking falls back to CRL.

Note Revocation checking does not fall back to OCSP if CRL fails.

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 file location of the CRL and the URL of the OCSP server.

- ▪ (Optional) OCSP Response Signing certificate file location.

- ▪ Consent form content, if a consent form displays before authentication.

Procedure

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

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

3 Click the gearbox in the X.509 Certificate line.

4 Configure the X.509 Certificate form.

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

Option	Description
Enable X.509 Certificate	Change NO to **YES** to enable certificate authentication.
*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.
Enable Cert Revocation	Change NO to **YES** to enable certificate revocation checking. Revocation checking prevents users who have revoked user certificates from authenticating.
Use CRL from Certificates	Select the check box to use the certificate revocation list (CRL) published by the CA that issued the certificates to validate the status of a certificate, revoked or not revoked.
CRL Location	Enter the server file path or the local file path from which to retrieve the CRL
Enable OCSP Revocation	Select the check box to use the Online Certificate Status Protocol (OCSP) certificate validation protocol to get the revocation status of a certificate.
Use CRL in case of OCSP Failure	If you configure both CRL and OCSP, you can select this box to fall back to using CRL if OCSP checking is not available.
Send OCSP Nonce	Select this check box if you want the unique identifier of the OCSP request to be sent in the response.
OCSP URL	If you enabled OCSP revocation, enter the OCSP server address for revocation checking.
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*.

Option	Action
*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 as *@somedomain.com*. Is used to send additional content such as domain name to the RADIUS server or the RSA SecurID server. For example, if a user logs in as *user1*, then *user1@somedomain.com* is sent to the server.

Configuring RADIUS for Unified Access Gateway

You can configure Unified Access Gateway so that users are required to use strong RADIUS two-factor authentication. You configure the RADIUS server information on the Unified Access Gateway appliance.

RADIUS support offers a wide range of third-party two-factor authentication options. To use RADIUS authentication on Unified Access Gateway, you must have a configured RADIUS server that is accessible on the network from Unified Access Gateway.

When users log in and RADIUS authentication is enabled, users enter their RADIUS authentication user name and passcode in the login dialog box. If the RADIUS server issues a RADIUS Access-Challenge, Unified Access Gateway displays a second dialog box to the user prompting for the challenge response text input, such as a code communicated to the user through a SMS text or other out-of-band mechanism. Support for a RADIUS passcode entry and challenge response entry is limited to text-based input only. Entry of the correct challenge response text completes the authentication.

If the RADIUS server requires the user to enter their Active Directory password as the RADIUS passcode, then for Horizon use the administrator can enable the Horizon Windows single sign-on feature on Unified Access Gateway so that when RADIUS authentication is complete, the user will not get a subsequent prompt to reenter the same Active Directory domain password.

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
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.

Option	Action
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 as *@somedomain.com*. Is used to send additional content such as domain name to the RADIUS server or the RSA SecurID server. For example, if a user logs in as *user1*, then *user1@somedomain.com* is sent to the server.
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 basic MS-CHAPv2 validation	Change NO to **YES** to enable basic MS-CHAPv2 validation. If this option is set to **YES**, then the additional validation of response from the RADIUS server is skipped. By default, full validation will be performed.
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.
Search Attribute	Enter the account attribute that contains the username.

Option	Description
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 Horizon 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**.

Results

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 Edge Service Session Statistics

- Monitoring the Health of Deployed Services

- Troubleshooting Deployment Errors

- Troubleshooting Errors: Identity Bridging

- Troubleshooting Errors: Cert-to-Kerberos

- Troubleshooting Endpoint Compliance

- Troubleshooting Certificate Validation in the Admin UI

- Troubleshooting Firewall and Connection Issues

- Troubleshooting Root Login Issues

- Collecting Logs from the Unified Access Gateway Appliance

- Export Unified Access Gateway Settings

- Import Unified Access Gateway Settings

- Troubleshooting Errors: Content Gateway

- Troubleshooting High Availability

- Troubleshooting Security: Best Practices

Monitoring Edge Service Session Statistics

Unified Access Gateway provides information on active sessions of each edge service. You can quickly see that services you deployed are configured, up and running successfully from the admin UI for each Edge Service.

Procedure

1   Navigate to **Support Settings** > **Edge Service Session Statistics**.

2   In the **Support Settings** section, click the **Edge Service Session Statistics** gearbox icon.

Figure 7-1. Edge Service Session Statistics

- **Edge Service** lists the specific edge service for which the session statistics are displayed.

- **Total Sessions** indicate the sum of active and inactive sessions.

- **Active Sessions (Logged in Sessions)** indicate the number of ongoing authenticated sessions.

- **Inactive Sessions** indicate the number of unauthenticated sessions.

- **Failed Login Attempts** indicate the number of failed login attempts.

- **Session High Water Mark** indicate the maximum number of concurrent sessions at a given point in time.

- **PCoIP Sessions** indicate the number of sessions established with PCoIP.

- **BLAST Sessions** indicate the number of sessions established with Blast.

- **Tunnel Sessions** indicate the number of sessions established with Horizon Tunnel.

Table 7-1. Example of Edge Service Session Statistics

Edge Service	Total Sessions	Active (Logged In) Sessions	Inactive Sessions	Failed Login Attempts	Session High Water Mark	PCoIP Sessions	BLAST Sessions	Tunnel Sessions
Horizon	11	0	11	8	11	0	0	0
Reverse Proxy (jira)	10	0	10	10	10	-	-	-
Reverse Proxy (sp_blr)	11	0	11	11	11	-	-	-
Reverse Proxy (sp_https_ saml)	4	0	4	0	5	-	-	-

Table 7-1. Example of Edge Service Session Statistics (continued)

Edge Service	Total Sessions	Active (Logged In) Sessions	Inactive Sessions	Failed Login Attempts	Session High Water Mark	PCoIP Sessions	BLAST Sessions	Tunnel Sessions
Reverse Proxy (sp_multi_domain)	8	0	8	8	8	-	-	-
VMware Tunnel	1	1	0	0	1	-	-	-
Total	45	1	44	37		-	-	-

Monitor Session Statistics API

The parameters listed here describe the session statistics captured at the last monitoring interval.

URL call: `https://<UAGIP>:9443/rest/v1/monitor/stats`

Table 7-2. Horizon View

Attribute	Description
`totalSessions`	Indicates the sum of active and inactive sessions. Admin UI: **Total Sessions**.
`highWaterMarkOfSessions`	Indicates the maximum number of concurrent sessions at a given point in time. Admin UI: **Session High Water Mark**.
`authenticatedSessions`	Indicates the number of ongoing authenticated sessions (logged in sessions). Admin UI: **Active (Logged In) Sessions**.
`unauthenticatedSessions`	Indicates the number of unauthenticated sessions. Admin UI: **Inactive Sessions**.
`failedLoginAttempts`	Indicates the number of failed login attempts. Admin UI: **Failed Login Attempts**
`userCount`	Indicates the number of unique users currently authenticated.
BLAST	
`sessions`	Indicates the number of active BLAST sessions.
`maxSessions`	Indicates the number of authorized BLAST sessions.
PCoIP	
`sessions`	Indicates the number of active PCoIP sessions created during the start of a desktop or an application.
`maxSessions`	Indicates the maximum number of concurrent PCoIP sessions at a given point in time.
VMware Tunnel	

Table 7-2. Horizon View (continued)

Attribute	Description
sessions	Indicates the number of active VMware Tunnel sessions created on authentication through View Client.
maxSessions	Indicates the maximum number of concurrent VMware Tunnel sessions at a given point in time.

Table 7-3. Web Reverse Proxy

Attribute	Description
totalSessions	Indicates the sum of active and inactive sessions. Admin UI: **Total Sessions**.
highWaterMarkOfSessions	Indicates the maximum number of concurrent sessions at a given point in time. Admin UI: **Session High Water Mark**.
authenticatedSessions	Indicates the number of ongoing authenticated sessions (logged in sessions). Admin UI: **Active (Logged In) Sessions**.
unauthenticatedSessions	Indicates the number of unauthenticated sessions. Admin UI: **Inactive Sessions**.
failedLoginAttempts	Indicates the number of failed login attempts. Admin UI: **Failed Login Attempts**.
userCount	Indicates the number of unique users currently authenticated.
backendStatus	
status	Indicates if the back-end application is reachable. (Running, Not Reachable)
reason	Indicates and explains the status with reason. (Reachable, Error details)
kcdStatus	
status	Indicates if the kcd server is reachable. (Running, Not Reachable)
reason	Indicates and explains the status with reason. (Reachable, Error details)

Table 7-4. VMware Tunnel

| Attribute	Description
identifier	Indicates that the VMware Tunnel service is enabled.
status	Status of the VMware Tunnel service (vpnd service.
reason	Indicates and explains the status with reason for the VMware Tunnel service. Up or Down labels denote the service status. For example, it is reachable when the service is up and running, the VMware Tunnel server is not reachable when the service is down.
totalSessions	Indicates the number of active VMware Tunnel sessions created on authentication through the VMware Tunnel client.
connections	Indicates the number of active outbound connections from the VMware Tunnel Server.
upTime	Indicates the active (running) time of the VMware Tunnel service.
apiConnectivity	VMware Tunnel Server to the API connectivity. For example, True or False.

Table 7-4. VMware Tunnel (continued)

Attribute	Description
awcmConnectivity	VMware Tunnel Server to the AWCM connectivity. For example, True or False.
cascadeMode	Provides cascade information. For example, Off for Basic mode and front-end or back-end for a cascade setup.

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 7-2. Health Check
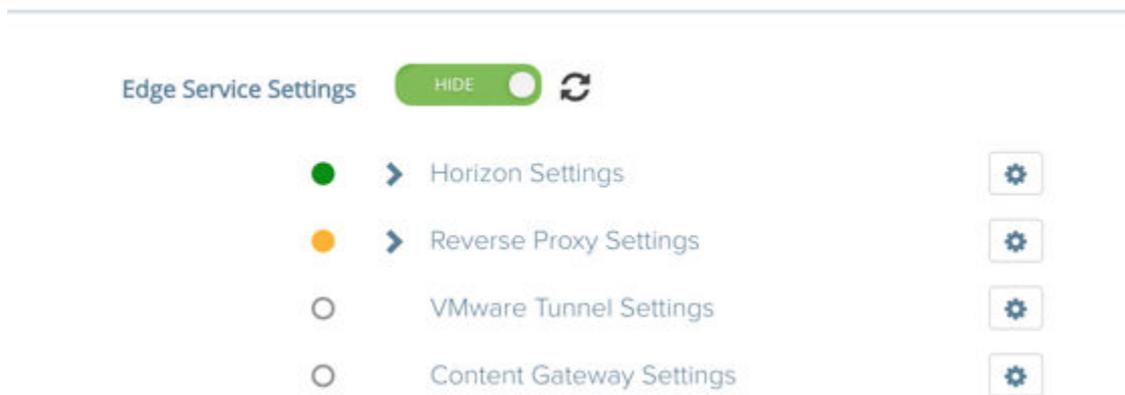
A circle displays before the service. The color coding is as follows.

- Blank circle - The setting is not configured.

- A red circle - service is down.

- An amber circle - The service is partially running.

- A green circle - 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 various 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 .\uagdeploy.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 netInternet, netManagementNetwork, and netBackendNetwork.

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.

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 Server 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 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. It is recommended that you use a different browser to deploy the Unified Access Gateway ova.

Unable to Deploy the Unified Access Gateway ova Using VMware vSphere HTML4/5 Web Client

You might run into errors such as `Invalid value specified for property`. This problem is not related to the Unified Access Gateway ova. It is recommended that you use the vSphere FLEX client instead to deploy the ova.

Unable to Deploy the Unified Access Gateway ova Using VMware vSphere 6.7 HTML5 Web Client

You may find that there are missing fields on the **Deployment Properties** page in the VMware vSphere 6.7 HTML5 Web Client. This problem is not related to the Unified Access Gateway ova. It is recommended that you use the vSphere FLEX client instead to deploy the ova.

Cannot Launch XenApp from Chrome From VMware Identity Manager

After deploying Unified Access Gateway as a web reverse proxy from VMware Identity Manager, you may not be able to launch XenApp from the Chrome Browser.

Follow the steps below to resolve this issue.

1　Use the following REST API to disable the feature flag `orgUseNonNPAPIForCitrixLaunch` from VMware Identity Manager service.

```
PUT https://fqdn/SAAS/jersey/manager/api/tenants/settings?tenantId=tenantname
{ "items":[ {"name":"orgUseNonNPAPIForCitrixLaunch","value": "false"} ] }
with the following two headers:
Content-Type application/vnd.vmware.horizon.manager.tenants.tenant.config.list+json
Authorization HZN value_of_HZN_cookie_for_admin_user
```

2　Wait for 24 hours for the change to take effect or restart the VMware Identity Manager service.

- To restart the service on Linux, log in to the virtual appliance and run the following command: `service horizon-workspace restart`.

- To restart the service on Windows, run the following script: `install_dir\usr\local\horizon\scripts\horizonService.bat restart` .

Troubleshooting Errors: Identity Bridging

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

Monitoring the health of KDC server and backend application server.

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

Figure 7-3. Health Check - Reverse Proxy Settings
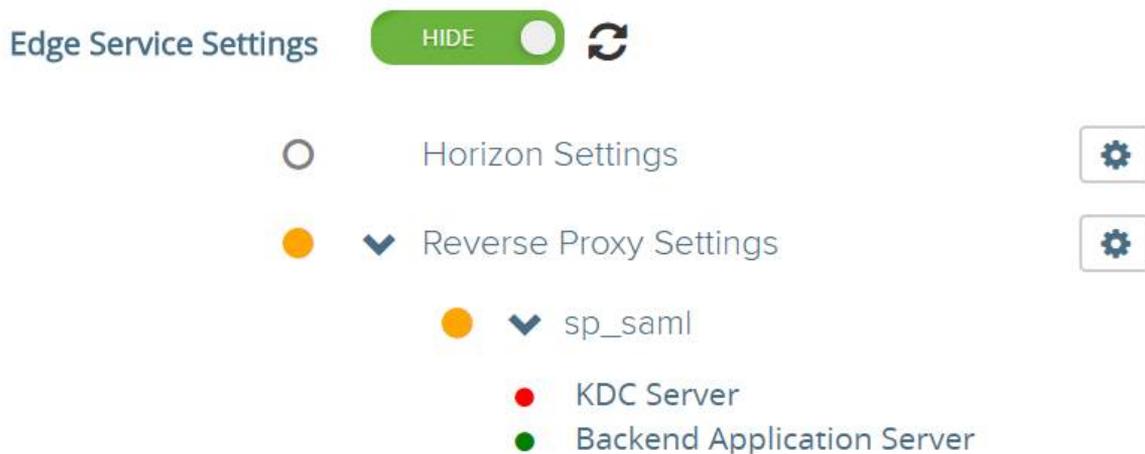
A circle displays before the service. The color coding is as follows.

- Red Circle: If the status is Red, it could mean one of the following.

  - Connectivity issues between Unified Access Gateway and Active Directory

  - Port blocking issues between Unified Access Gateway and Active Directory.

    Note   Ensure that both TCP and UDP port 88 is opened in the Active Directory machine.

  - Principal name and password credentials might be incorrect in the uploaded keytab file.

- Green Circle: If the status is Green, it means that the Unified Access Gateway is able to log in to the Active Directory with the credentials provided in keytab file.

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 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 Errors: 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 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 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.

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, all target certs are invalid. May be missing an intermediate/root certificates.	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.

Error	Issue
Not able to build cert chain path, CertificateExpiredException: certificate expired on *20171206054737GMT+00:00*. See log for more details.	The certificate has expired.
Error message "Unexpected data detected in stream" while uploading the certificate in PEM format.	Missing empty line or additional attributes between leaf and intermediate in chain certificate. Adding an empty line between leaf and intermediate certificate would resolve the issue.

Figure 7-4. Example

Troubleshooting Firewall and Connection Issues

You can monitor, test, and troubleshoot network problems such as firewall and connection issues from your Unified Access Gateway instance with various tools and commands such as `tcpdump` and `curl`.

Install and Run `tcpdump`

`tcpdump` is a command-line tool that you can use to analyze TCP packets for troubleshooting and testing purposes.

If you have not installed `tcpdump` on your Unified Access Gateway instance, run the following command from the command-line to install `tcpdump`:

`/etc/vmware/gss-support/install.sh`

The following examples show `tcpdump` usage:

- Run the following commands to monitor traffic over specific ports.

    Note If you specify port 8443, ensure that UDP 8443 is not blocked by an outer firewall.

    a tcpdump -i eth0 -n -v udp port 8443

    b tcpdump -i eth0 -n -v tcp port 8443

    c tcpdump -i any -n -v port 22443

- Run the following commands to trace the packets that are coming to and from the RADIUS server to Unified Access Gateway:

    ```
    nslookup <radius-server-hostname>
    tracepath <radius-server-hostname>
    tcpdump -i any -n -v port 1812
    ```

■ Run the following commands to trace the packets that are coming to and from the RSA SecurID server to Unified Access Gateway.

```
nslookup <rsa-auth-server-hostname>
tracepath <rsa-auth-server-hostname>
```

Using the `curl` command

You can also use the `curl` command to retrieve information about network connections.

■ Run the following command to test the connection to a back end connection server or a web server:

`curl -v -k https://<hostname-or-ip-address>:443/`

You can view the back end server connection issues in the `esmanager.log` file:

```
07/14 07:29:03,882[nioEventLoopGroup-7-1]ERROR
view.ViewEdgeService[onFailure: 165][]: Failed to resolve hostname
address in proxyDestinationUrl:xref:mbxxx-cs.xyz.in
```

■ You cannot test connections to back end virtual desktops such as PCoIP 4172 and Blast 22443 using `tcpdump` as the desktops do not listen on these port numbers until a session is ready. See the logs to look at possible connection failures on these ports.

  ■ Run the following command for Horizon Framework Channel TCP connection:

  `curl -v telnet://<virtualdesktop-ip-address>:32111`

  ■ Run the following command for Horizon MMR/CDR TCP connection:

  `curl -v telnet://<virtualdesktop-ip-address>:9427`

  ■ Run the following command to test port connectivity from Unified Access Gateway to the virtual desktop. Ensure that the session to the virtual desktop is active before running this command.

  `curl -v telnet://<virtualdesktop-ip-address>:22443`

PowerShell Commands

Run the following commands from the PowerShell command-line to monitor connectivity for specific ports:

1 `Test-NetConnection <uag-hostname-or-ip-address> -port 443`

2 `Test-NetConnection <uag-hostname-or-ip-address> -port 8443`

3 `Test-NetConnection <uag-hostname-or-ip-address> -port 4172`

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 file.

- 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 Photon OS splash screen appears, press e to enter GNU GRUB edit menu

3 In the GNU GRUB edit menu, go to the end of the line that starts with `linux`, add a space and
type `/boot/$photon_linux root=$rootpartition rw init=/bin/bash`. After adding these values,
GNU GRUB edit menu should look exactly like this:

Note For a FIPS appliance, the line should be `linux /boot/$photon_linux root=$rootpartition`
`rw init=/bin/bash fips=1`

4 Press the F10 key and at the bash command prompt enter **passwd** to change the password.

```
passwd
```

```
New password:
```

```
Retype new password:
```

```
passwd: password updated successfully
```
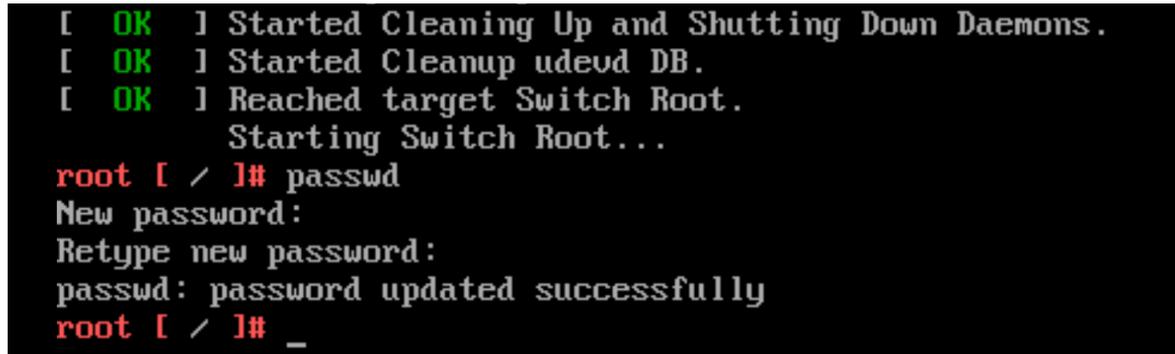
```
[  OK  ] Started Cleaning Up and Shutting Down Daemons.
[  OK  ] Started Cleanup udevd DB.
[  OK  ] Reached target Switch Root.
         Starting Switch Root...
root [ / ]# passwd
New password:
Retype new password:
passwd: password updated successfully
root [ / ]# _
```

5 Reboot the appliance `reboot -f`

- 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 `UAG-log-archive.zip` file from the Support Settings section 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 7-5. 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 7-6. Files That Contain System Information to Aid in Troubleshooting

File Name	Description	Linux Command (if applicable)
`rpm-version.log`	Version of the Unified Access Gateway appliance.	
`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 -anop`
`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, uagstats.json`	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`
`iptables.log`	IP tables for IPv4.	`iptables-save`
`ip6tables.log`	IP tables for IPv6.	`ip6tables-save`
`w.log`	Information about uptime, the users currently on the machine, and their processes.	`w`
`systemctl.log`	List of services currently running on the appliance	`systemctl`

Table 7-6. Files That Contain System Information to Aid in Troubleshooting (continued)

File Name	Description	Linux Command (if applicable)
`resolv.conf`	For connecting local clients directly to all the known DNS servers	
`hastats.csv`	Contains stats per node and total stats information for each back end type (Edge Service Manager, VMware Tunnel, Content Gateway)	

Table 7-7. Log Files for Unified Access Gateway

File Name	Description	Linux Command (if applicable)
`supervisord.log`	Supervisor (manager for the Edge Service manager, admin and a AuthBroker) log.	
`esmanager-x.log,` `esmanager-std-out.log`	Edge service manager log(s), showing back end processes performed on the appliance.	
`audit.log`	Audit log for all admin user operations.	
`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.	
`activeSessions.csv`	List of active Horizon or WRP sessions.	
`haproxy.conf`	Contains HA proxy configuration parameters for TLS port sharing.	
`vami.log`	Contains log messages from running `vami` commands to set network interfaces during deployment.	
`content-gateway.log,` `content-gateway-wrapper.log,` `0.content-gateway-YYYY-mm.dd.log.zip`	Contains log messages from 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.	
`tunnel-snap.tar.gz`	Tarball containing VMware Tunnel server and proxy logs.	
`aw-appliance-agent.log`	Appliance agent (for starting up Workspace ONE UEM services) logs.	

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

File Name	Description	Linux Command (if applicable)
config.yml	Contains Content Gateway configuration and log level details.	
smb.conf	Contains SMB client configuration.	
smb-connector.conf	Contain SMB protocol and log level details.	

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.

Import Unified Access Gateway Settings

Unified Access Gateway admin UI provides an option to export configuration settings in JSON format. After exporting the configuration settings in JSON format, you can use the exported JSON file to configure a newly deployed version of Unified Access Gateway appliance.

Procedure

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

2 Click JSON to export the Unified Access Gateway settings in the JSON format.

The file is saved by default in your Downloads folder

3 Delete the old Unified Access Gateway appliance or put it in Quiesce mode to delete it later.

4 Deploy the new version of Unified Access Gateway appliance

5 Import the JSON file you exported earlier.

Troubleshooting Errors: Content Gateway

You might experience difficulty when you configure Content Gateway in your environment. You can use the procedure to diagnose and fix the problem.

Issue with Sync, Download, and Upload for users using shares hosted on NetApp servers.

To manually change the configuration file, follow the steps:

1   Log in to the vSphere Client

2   Open the Unified Access Gateway console where Content Gateway is configured.

3   Navigate to `/opt/airwatch/content-gateway/conf`

4   Edit the `config.yml` file

5   Modify the flag value for parameter `aw.fileshare.jcifs.active` to `true`. The default value is `false`.

6   Restart the content-gateway service with the command

```
$ service content-gateway restart
```

Troubleshooting High Availability

You might experience difficulty when you configure High Availability in your environment. You can use a variety of procedures for diagnosing and fixing these problems.

1   Log in to Unified Access Gateway console.

2   Run `ip addr` command to check if the configured virtual IP address is assigned to eth0 interface.

3   Ensure virtual IP address is assigned within the same subnet as eth0 interface. Ensure it is reachable from the client machine. If there are connectivity issues then it could be due to virtual IP address not being unique and already assigned to a physical or virtual machine.

4   In the `haproxy.conf` file in log bundle, configuration related to the current cluster is available. For example,

```
server uag1 127.0.0.1:XXXX .....
server uag2 <IP of machine 2>:XXXX ....
server uag3 <IP of machine 3>:XXXX ....
```

The back-end configuration is based on the settings configured on Unified Access Gateway

- `lb_esmanageris` for Horizon and Web reverse proxy use cases.

- `lb_cg_server` is for Content Gateway use cases.

- `lb_tunnel_server` is for Tunnel use cases.

5   In the `haproxy.conf` file in log bundle, you can find details about the client connection source, corresponding connection sent, and the Unified Access Gateway server that handles the connections. For example,

```
2018—11—27T07:21:09+00:00 ipv6—localhost haproxy[15909]:
            incoming:::ffff:<IP of Client:xxxx> backend:lb_esmanager
            connecting—server:uag2/<IP of uag2> connecting—through:<IP of master
            node:xxxx> wait—time:1 connect—time:0 total—incoming:1 total—outgoing:1
            total—to—server:1
```

6   To view the statistics, see Collecting Logs from the Unified Access Gateway Appliance.

Table 7-8. Example of a CSV File

Column Name	Description
scur	Indicates the current number of concurrent connections handled by this server.
smax	High watermark of concurrent connections handled by this server during current uptime.
stot	Indicates the total number of connections handled by this server during current uptime.
bin	Indicates the total number of bytes sent to this server.
bout	Indicates the total number of bytes received from this server.
status	Indicates the status of the server. For example, if it is up or down. This is based on the last health check performed on this server.

7   Multiple master node election issues can be seen in the following cases,

- Different group ID or virtual IP address configured on the nodes that are intended to form the cluster.

- Virtual IP address and eth0 in different subnet.

- Multiple NICS on Unified Access Gateway configured within the same subnet.

Troubleshooting Security: Best Practices

When the service detects a load-balancing device in your web-servers, this additional information about your network is a vulnerability. You can use a variety of procedures for diagnosing and fixing these problems.

Different techniques are used to detect the presence of a load-balancing device, including HTTP header analysis and analysis of IP Time-To-Live (TTL) values, IP Identification (ID) values, and TCP Initial Sequence Numbers (ISN). The exact number of Web servers behind a load balancer is difficult to determine, so the number reported might not be accurate.

Furthermore, Netscape Enterprise Server Version 3.6 is known to display an erroneous `"Date:"` field in the HTTP header when the server receives multiple requests. This makes it difficult for the service to determine if there is a load-balancing device present by analyzing the HTTP headers.

Additionally, the result given by the analysis of IP ID and TCP ISN values may vary due to different network conditions when the scan was performed. By exploiting this vulnerability, an intruder could use this information in conjunction with other pieces of information to craft sophisticated attacks against your network.

Note If the Web servers behind the load balancer are not identical, the scan results for the HTTP vulnerabilities may vary from one scan to another.

- Unified Access Gateway is an appliance that is normally installed in a demilitarized zone (DMZ). The steps below help you protect Unified Access Gateway from vulnerability scanners from detecting this issue.

  - To prevent the detection of the presence of a load-balancing device based on HTTP header analysis, you should use Network-Time-Protocol (NTP) to synchronize the clocks on all of your hosts (at least those in the DMZ).

  - To prevent detection by analyzing IP TTL values, IP ID values, and TCP ISN values, you may use hosts with a TCP/IP implementation that generates randomized numbers for these values. However, most operating systems available today do not come with such a TCP/IP implementation.