Deploying and Configuring VMware Unified Access Gateway

Unified Access Gateway 2207

vmware by Broadcom

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

https://docs.vmware.com/

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

Contents

Deploying and Configuring VMware Unified Access Gateway 6

1 Preparing to Deploy VMware Unified Access Gateway 7

Unified Access Gateway as a Secure Gateway 7

Using Unified Access Gateway Instead of a Virtual Private Network 8

Unified Access Gateway System and Network Requirements 9

Firewall Rules for DMZ-Based Unified Access Gateway Appliances 13

System Requirements for Deploying VMware Tunnel with Unified Access Gateway 21

Port Requirements for VMware Tunnel Proxy 22

Port Requirements for VMware Per-App Tunnel 27

Network Interface Connection Requirements 33

Unified Access Gateway Load Balancing Topologies 33

Configure Avi Vantage for load balancing UAG (when used as web reverse proxy) 36

Unified Access Gateway High Availability 40

Configure High Availability Settings 42

Unified Access Gateway Configured with Horizon 43

VMware Tunnel (Per-App VPN) Connection with Basic Configuration 44

VMware Tunnel (Per-App VPN) Connections in Cascade Mode 45

Content Gateway Basic Configuration 46

Content Gateway with Relay and Endpoint Configuration 47

DMZ Design for Unified Access Gateway with Multiple Network Interface Cards 48

Upgrade with Zero Downtime 51

Deploying Unified Access Gateway Without Network Protocol Profile (NPP) 53

Join or Leave the Customer Experience Improvement Program 54

2 Deploying Unified Access Gateway Appliance 55

Using the OVF Template Wizard to Deploy Unified Access Gateway 56

Deploy Unified Access Gateway Using the OVF Template Wizard 56

Configuring Unified Access Gateway From the Admin Configuration Pages 66

Configure Unified Access Gateway System Settings 67

Configure Syslog Server Settings 75

Change Network Settings 77

Configure User Account Settings 78

Configure JSON Web Token Settings 84

Configure Outbound Proxy Settings 85

Configure Unified Access Gateway to Automatically Apply Authorized OS Updates 86

Update TLS Server Signed Certificates 88

3 Using PowerShell to Deploy Unified Access Gateway 90

System Requirements to Deploy Unified Access Gateway Using PowerShell 90

Using PowerShell to Deploy the Unified Access Gateway Appliance 91

PowerShell Parameters for Deploying Unified Access Gateway 99

4 Deployment Use Cases for Unified Access Gateway 104

Deployment with Horizon and Horizon Cloud with On-Premises Infrastructure 104

Unified Access Gateway Support for IPv4 and IPv6 Dual Mode for Horizon Infrastructure 109

Advanced Edge Service Settings 110

Configure Horizon Settings 112

Blast TCP and UDP External URL Configuration Options 124

Endpoint Compliance Checks for Horizon 124

Configure Workspace ONE Intelligence (Risk Analytics) as the Endpoint Compliance Check Provider for Horizon 125

Configure OPSWAT as the Endpoint Compliance Check Provider for Horizon 126

Time Interval for Delaying Compliance Check 134

Time Interval for Periodic Endpoint Compliance Checks 134

Deployment as Reverse Proxy 135

Configure Reverse Proxy With Workspace ONE Access 137

Configure Reverse Proxy With VMware Workspace ONE UEM API 141

Deployment for Single Sign-on Access to On-Premises Legacy Web Apps 143

Identity Bridging Deployment Scenarios 145

Configuring Identity Bridging Settings 148

Configuring Horizon for Unified Access Gateway and Third-Party Identity Provider Integration 162

Configure the Identity Provider with Unified Access Gateway Information 163

Upload Identity Provider's SAML Metadata to Unified Access Gateway 165

Configure Horizon Settings on Unified Access Gateway for SAML Integration 166

Workspace ONE UEM Components on Unified Access Gateway 168

VMware Tunnel on Unified Access Gateway 169

About TLS Port Sharing 181

Content Gateway on Unified Access Gateway 181

Secure Email Gateway on Unified Access Gateway 186

Additional Deployment Use Cases 189

Configure Workspace ONE Intelligence Connection Settings 190

Select the Workspace ONE Intelligence Data Setting 191

5 Configuring Unified Access Gateway Using TLS/SSL Certificates 193

Configuring TLS/SSL Certificates for Unified Access Gateway Appliances 193

Selecting the Correct Certificate Type 193

Convert Certificate Files to One-Line PEM Format 195

Change the Security Protocols and Cipher Suites Used for TLS or SSL Communication 197

6 Configuring Authentication in DMZ 199

Configuring Certificate or Smart Card Authentication on the Unified Access Gateway Appliance 199

Configure Certificate Authentication on Unified Access Gateway 200

Obtain the Certificate Authority Certificates 202

Configure RSA SecurID Authentication in Unified Access Gateway 203

Configuring RADIUS for Unified Access Gateway 204

Configure RADIUS Authentication 205

Generate Unified Access Gateway SAML Metadata 207

Creating a SAML Authenticator Used by Other Service Providers 207

Copy Service Provider SAML Metadata to Unified Access Gateway 208

7 Troubleshooting Unified Access Gateway Deployment 209

Monitoring Edge Service Session Statistics 210

Monitor Session Statistics API 211

Unified Access Gateway Session Flow For Horizon 214

Monitoring the SEG Health and Diagnostics 218

Monitoring the Health of Deployed Services 220

Troubleshooting Deployment Errors 221

Troubleshooting Errors: Identity Bridging 223

Troubleshooting Errors: Cert-to-Kerberos 225

Troubleshooting Endpoint Compliance 226

Troubleshooting Certificate Validation in the Admin UI 226

Troubleshooting Firewall and Connection Issues 227

Troubleshooting Root Login Issues 229

About the Grub2 Password 232

Collecting Logs from the Unified Access Gateway Appliance 232

Configure Log Level Settings in Unified Access Gateway 237

Syslog Formats and Events 238

Export Unified Access Gateway Settings 246

Import Unified Access Gateway Settings 247

Troubleshooting Errors: Content Gateway 247

Troubleshooting High Availability 248

Troubleshooting Security: Best Practices 249

User Sessions Impacted by Changes in Unified Access Gateway Admin UI Settings 250

Troubleshooting Unified Access Gateway Configuration for Horizon RSA SecurID Authentication 251

Configurable Boot Time Commands for First Boot and Every Boot 252

Deploying and Configuring VMware Unified Access Gateway

Deploying and Configuring VMware Unified Access Gateway provides information about designing VMware Horizon®, VMware Workspace ONE Access, 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.

Read the following topics next:

- 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.

For information about the Unified Access Gateway Lifecycle Support Policy, see https://kb.vmware.com/s/article/2147313.

Hypervisor Requirements

Unified Access Gateway supports the following virtualization platforms:

- VMware vSphere (ESXi with vCenter)
- Microsoft Azure
- Microsoft Hyper-V (Tunnel, Secure Email Gateway, and Content Gateway Edge Services only)
- Amazon AWS EC2
- Google Cloud GCE

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.

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, it is recommended 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

Important Unified Access Gateway is a VMware virtual appliance. Security and general patches are distributed by VMware as updated virtual appliance image files. Customization of a Unified Access Gateway appliance or upgrading individual components is not supported apart from increasing memory and the number of vCPUs which can be performed through vCenter Server **Edit** settings.

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

- Virtual appliance download size (depends on the Unified Access Gateway version)
- Thin-provisioned disk minimum requirement is 3.5 GB
- Thick-provisioned disk minimum requirement is 20 GB

Note In addition to the minimum disk requirements, vSphere can create other files such as a swap file on the ESXi datastore for each virtual machine. Disk space is also used for any virtual machine snapshots created with vCenter Server. An ESXi datastore also contains some other small files for each virtual machine.

If memory reservation is not configured, vSphere creates a per-virtual machine swap file (`.vswp`) of up to the virtual machine memory size. This swap space is for any unreserved virtual machine memory. For example, a 4 GB RAM Unified Access Gateway appliance with a vSphere thick-provisioned disk uses a 20 GB ESXi `.vmdk` file and the appliance can use a 4 GB ESXi swap file. This results in a total disk space requirement of 24 GB. Similarly, for a 16 GB RAM Unified Access Gateway appliance, the total disk space requirement can be 36 GB.

For more information about Swap Space and Memory Overcommitment, see *vSphere Resource Management* documentation.

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 16GB RAM
  - Extra Large - 8 core and 32GB RAM

  You can configure these settings using PowerShell. For information about PowerShell parameters, see Using PowerShell to Deploy the Unified Access Gateway Appliance.

  For more information about the Unified Access Gateway sizing recommendations, you can see VMware Configuration Maximums.

Browser Versions Supported

Supported browsers for launching the Admin UI are Chrome, Firefox, and Internet Explorer. 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.

Multicast DNS and `.local` hostnames

UAG (Unified Access Gateway) 3.7 and later versions support Multicast DNS in addition to the Unicast DNS. Multi-label names with the domain suffix `.local` are routed to all local interfaces which are capable of IP multicasting by using the Multicast DNS protocol.

Avoid defining `.local` in a Unicast DNS server because RFC6762 reserves this domain use for Multicast DNS. For example, if you use a hostname `hostname.example.local` in a configuration setting such as Proxy Destination URL on the UAG, then the hostname is not resolved with Unicast DNS because `.local` is reserved for Multicast DNS.

Alternatively, you can use one of the following methods in which the `.local` domain suffix is not required:

- Specify an IP address instead of a `.local` hostname.
- An additional alternative DNS A record can be added in the DNS server.

  In the earlier example of host name, `hostname.example.int` can be added to the same IP address as `hostname.example.local` and used in the UAG configuration.
- A local `hosts` file entry can be defined.

  In the earlier example, a local `hosts` entry can be defined for `hostname.example.local`.

  `hosts` file entries specify names and IP addresses and can be set by using the UAG Admin UI or through PowerShell `.ini` file settings.

  Important The `/etc/hosts` file on UAG must not be edited.

  On the UAG, local `hosts` file entries are searched before performing a DNS search. Such a search ensures that if the host name is present on the `hosts` file, then the `.local` names can be used and a DNS search is not required at all.

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. Unified Access Gateway services use DNS to resolve hostnames. The DNS server IP addresses are configurable. DNS requests are made on UDP port 53 and so it is important that an external firewall does not block these requests or replies.

Table 1-1. Port Requirements for the Secure Email Gateway

Port	Protocol	Source	Target/Destination	Description
443* or any port greater than 1024	HTTPS	Devices (from Internet and Wi-Fi)	Unified Access Gateway Secure Email Gateway endpoint	Secure Email Gateway listens on port 11443. When 443 or any other port is configured, Unified Access Gateway will internally route the SEG traffic to 11443.
443* or any port greater than 1024	HTTPS	Workspace ONE UEM Console	Unified Access Gateway Secure Email Gateway endpoint	Secure Email Gateway listens on port 11443. When 443 or any other port is configured, Unified Access Gateway will internally route the SEG traffic to 11443.
443* or any port greater than 1024	HTTPS	Email Notification Service (when enabled)	Unified Access Gateway Secure Email Gateway endpoint	Secure Email Gateway listens on port 11443. When 443 or any other port is configured, Unified Access Gateway will internally route the SEG traffic to 11443.
5701	TCP	Secure Email Gateway	Secure Email Gateway	Used for Hazelcast distributed cache.
41232	TLS/TCP	Secure Email Gateway	Secure Email Gateway	Used for Vertx cluster management.
44444	HTTPS	Secure Email Gateway	Secure Email Gateway	Used for Diagnostic and Administrative functionalities.
Any	HTTPS	Secure Email Gateway	Email Server	SEG connects to Email server's listener port, usually 443, to serve email traffic
Any	HTTPS	Secure Email Gateway	Workspace ONE UEM API server	SEG fetches the configuration and policy data from Workspace ONE. Port is usually 443.
88	TCP	Secure Email Gateway	KDC Server/AD Server	Used for fetching Kerberos authentication tokens when KCD authentication is enabled.

Note As the Secure Email Gateway (SEG) service runs as a non-root user in the Unified Access Gateway, the SEG cannot run on the system ports. Therefore, the custom ports must be greater than port 1024.

Table 1-2. Port Requirements for Horizon

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
3389	TCP	Unified Access Gateway	Desktops and RDS Hosts	Only required if the Horizon Clients use the RDP protocol.
9427	TCP	Unified Access Gateway	Desktops and RDS Hosts	MMR, CDR, and HTML5 features For example, Microsoft Teams Optimization, Browser Redirection, and others.

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 1-3. 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.

Table 1-3. Port Requirements for Web Reverse Proxy (continued)

Port	Protocol	Source	Target	Description
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 1-4. Port Requirements for Admin UI

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

Table 1-5. 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.
443* or any port > 1024	HTTPS	Unified Access Gateway Content Gateway Endpoint	Workspace ONE UEM API Server	
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 1-6. 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 UEMConsole		
443* or any port > 1024	HTTPS	Unified Access Gateway Content Gateway Relay	Workspace ONE UEM API Server	
443* or any port > 1024	HTTPS	Unified Access Gateway Content Gateway Endpoint	Workspace ONE UEM API Server	
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.
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 1-7. 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, UDP	Devices (from Internet and Wi-Fi)	VMware Tunnel Per-App tunnel	Run the following command after installation: `netstat -tlpn | grep [Port]`	1

Table 1-8. 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 UEMCloud 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
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 1-9. 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
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 1-10. 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. The VMware 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
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

The following points are valid for the VMware Tunnel requirements.

Note * - 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 1-11. 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
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 1-12. 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.
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**.

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

Source	Target or Destination	Protocol	Port	Verification	Notes
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 1-13. 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.

Table 1-13. Port Requirements for VMware Tunnel Proxy Relay-Endpoint Configuration (continued)

Source	Target or Destination	Protocol	Port	Verification	Notes
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 1-13. 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 1-13. 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 allow 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 1-14. 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 1-14. 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 1-15. 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.

Table 1-15. Port Requirements for VMware Per-App Tunnel Cascade Configuration (continued)

Source	Destination	Protocol	Port	Verification	Notes
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 1-15. 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

Table 1-15. Port Requirements for VMware Per-App Tunnel Cascade Configuration (continued)

Source	Destination	Protocol	Port	Verification	Notes
					UEM SaaS customers, the **REST API URL** is most commonly the **Console URL** 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 allow outbound communication, refer to the VMware Knowledge Base article that lists up-to-date IP ranges: 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

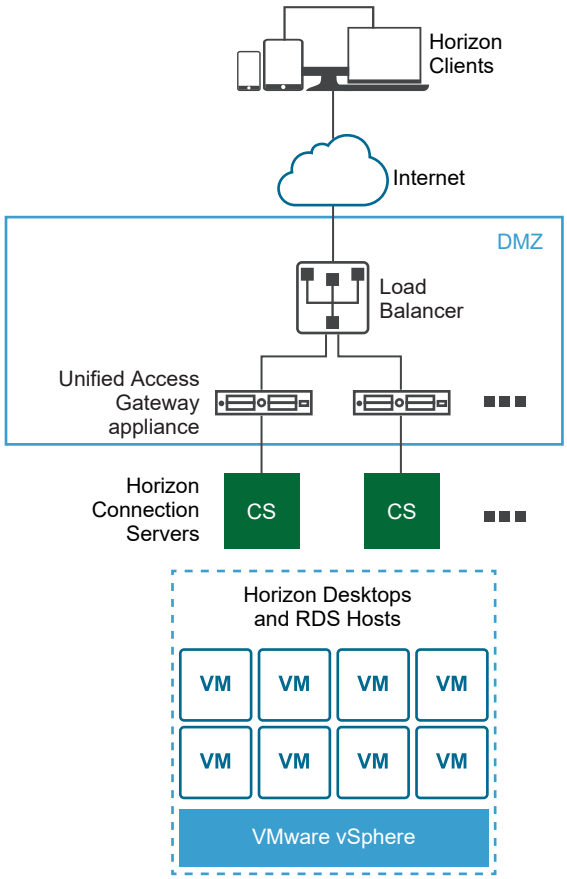
A Unified Access Gateway appliance in the DMZ can be configured to point to a server or a load balancer that fronts a group of servers. Unified Access Gateway appliances work with standard third-party load balancing solutions that are configured for HTTPS.

Note Unified Access Gateway is certified to work with Avi Vantage load balancers when Unified Access Gateway is deployed as a web reverse proxy.

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.

Configure Avi Vantage for load balancing UAG (when used as web reverse proxy)

The information documented here helps you configure Avi Vantage, used as a load balancing solution, for Unified Access Gateway when deployed as web reverse proxy. The configuration involves a set of tasks that must be performed by using the Avi controller.

By using the Avi UI, you must create an IP group, create a custom health monitor profile, create a pool, install the SSL certificate required for VIP, and create a virtual service.

By using the VIP used in the virtual service, you can access the web reverse proxy.

Prerequisites

- Ensure that you have already deployed Unified Access Gateway as a web reverse proxy.

  Deployment as Reverse Proxy

- Ensure that Avi controller is deployed and you have access to the controller and Avi UI.

  For more information about Avi Vantage, see Avi documentation.

Procedure

1 Create an IP group

  Create an IP group which has a list of Unified Access Gateway servers that need to be used for load balancing.

2 Create a Custom Health Monitor Profile

  Create a health monitor profile for the Unified Access Gateway on Avi Vantage. The health monitor profile is used to monitor the health of the Unified Access Gateway.

3 Create Pools

  Pools contain the list of Unified Access Gateway servers and the health monitor profile for Unified Access Gateway. Pools are then added to VS (Virtual Service).

4 Install the SSL Certificate Required for VIP (virtual IP)

  The SSL connection is terminated at Avi virtual service. Therefore, the SSL certificate must be assigned to the virtual service. For this assignment to happen, it is necessary to install the SSL certificate at Avi Vantage.

5 Create a Virtual Service

  Create a virtual service with the Unified Access Gateway server's VIP. This is the VIP to which the client devices connect.

Create an IP group

Create an IP group which has a list of Unified Access Gateway servers that need to be used for load balancing.

Since the same Unified Access Gateway servers are used as pool members in two different pools, IP groups can be attached to the pool instead of directly attaching servers to the pool. Any configuration change to the pool members like addition or removal of servers needs to be done at the IP Group level.

Procedure

1 From the Avi Vantage UI, navigate to **Templates > Groups**.

2 Click **Create IP Group**.

3 Enter the **IP Group Name**.

4 In the **IP Information** section, enter the IP Address of Unified Access Gateway servers.

5 Click **Add**.

6 Click **Save**.

What to do next

Create a Custom Health Monitor Profile

Create a Custom Health Monitor Profile

Create a health monitor profile for the Unified Access Gateway on Avi Vantage. The health monitor profile is used to monitor the health of the Unified Access Gateway.

For more information about health monitor profile, see Avi documentation.

Procedure

1. From the Avi Vantage UI, navigate to **Templates > Profiles > Health Monitors**.
2. Click **Create**.
3. In the **New Health Monitor** window, enter the profile information for Unified Access Gateway.
   a. Enter the value of **Health Monitor Port** as `443`.
   b. Enter the value of **Client Request Data** as `GET /favicon.ico HTTP/1.1`.
   c. Select the **Response Code** as `2XX`.
   d. Enable **SSL Attributes**.
   e. Select the **SSL Profile** as `System-Standard`.
   f. Enter the value of **Maintenance Response Code** as `503`.
4. Click **Save**.

What to do next

Create Pools

Create Pools

Pools contain the list of Unified Access Gateway servers and the health monitor profile for Unified Access Gateway. Pools are then added to VS (Virtual Service).

A typical virtual service points to one pool.

Procedure

1. From the Avi Vantage UI, navigate to **Applications > Pools**.
2. Click **Create Pool**.
3. In the **Select Cloud** window, select the cloud which belongs to the VMware vCenter/vSphere ESX cloud infrastructure type.

   The cloud infrastructure type is configured as part of Avi Controller deployment.
4. Click **Next**.

5 In the **New Pool** window, enter the required information in addition to the following:

   a In the **Load Balance** field, choose `Consistent Hash` with `Source IP Address` as the hash key.

   b In the **Health Monitors** section, click **Add Active Monitor**.

   c Select the health monitor that was created previously for Unified Access Gateway.

6 Select **Enable SSL**.

7 Choose the **SSL profile** as `System-Standard`.

8 Click **Next**.

9 In the **Servers** tab, add the previously created IP Group of Unified Access Gateway servers.

10 Click **Next**.

11 Navigate to **Advanced** > **Review**.

12 Click **Save**.

What to do next

Install the SSL Certificate Required for VIP (virtual IP)

Install the SSL Certificate Required for VIP (virtual IP)

The SSL connection is terminated at Avi virtual service. Therefore, the SSL certificate must be assigned to the virtual service. For this assignment to happen, it is necessary to install the SSL certificate at Avi Vantage.

Note It is recommended to install a certificate signed by a valid certificate authority instead of using self-signed certificates.

For more information about installing the SSL certificate, see Avi documentation.

What to do next

Create a Virtual Service

Create a Virtual Service

Create a virtual service with the Unified Access Gateway server's VIP. This is the VIP to which the client devices connect.

Procedure

1 From the Avi Vantage UI, navigate to **Applications** > **Virtual Services**.

2 Click **Create Virtual Service** > **Advanced Setup**.

3 In the **Select Cloud** window, select the cloud which belongs to the VMware vCenter/vSphere ESX cloud infrastructure type.

   The cloud infrastructure type is configured as part of Avi Controller deployment.

4 In the **New Virtual Service** window, configure the virtual service.
   a Enter the virtual service name.
   b Enter the VIP address.
   c In **Services**, enter the port number as `443`.
   d For the port number `443`, select the **SSL** checkbox.

      SSL is enabled for port `443`.
   e Select the **Application Profile** as `System-Secure-HTTP`.
   f Select the **Pool** that was created previously for Unified Access Gateway.
   g Select the **SSL Profile** as `System-Standard`.
   h Select the SSL certificate that was installed previously.
5 Click **Next**.
6 Navigate to **Advanced** tab.
7 Click **Save**.

What to do next

Access web reverse proxy by using the VIP.

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), Secure Email Gateway 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.
- If HA is configured, ensure that VIP is accessed using FQDN on port 443.

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.

Note In a high availability configuration, when the Horizon Client sends requests, Unified Access Gateway might not receive the actual source IP address of the request. Unified Access Gateway sends the received source IP address to the Horizon Connection Server. To ensure that the Connection Server receives the actual source IP address, you must use a layer 7 load balancer which preserves the source IP address.

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, turn on the **Mode** toggle 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**.

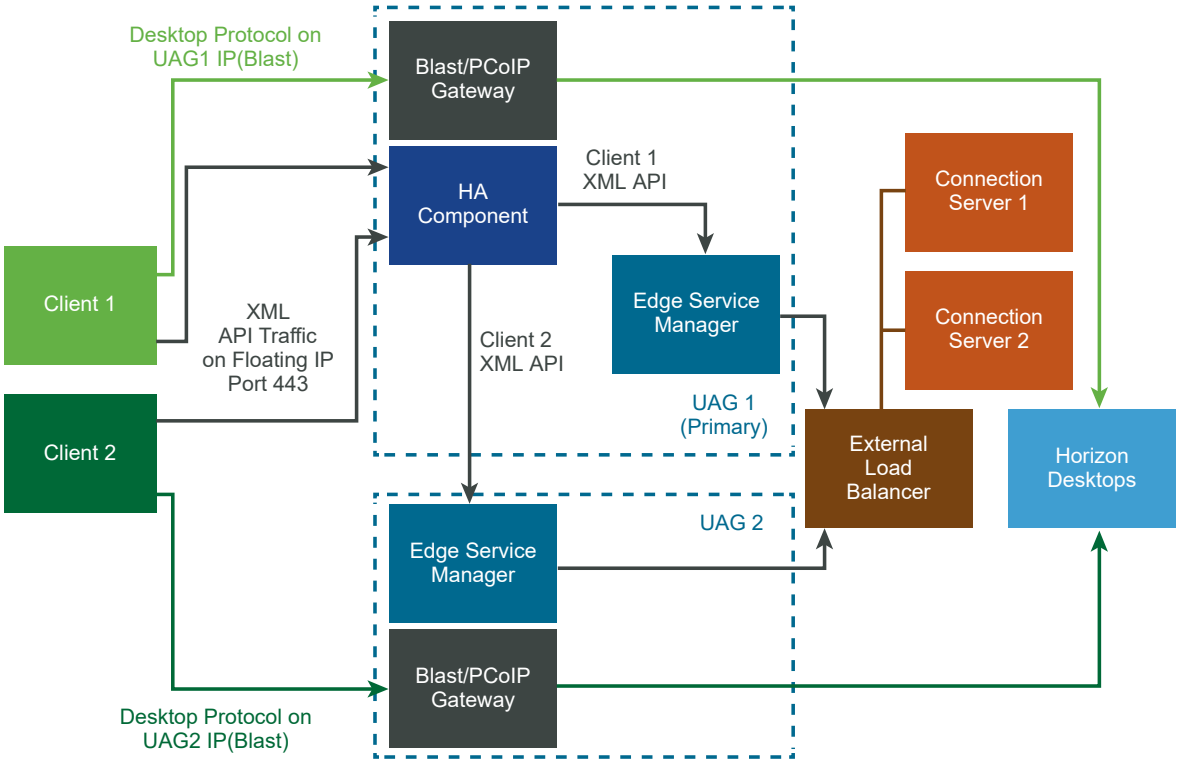
- The different states of **High Availability Settings** indicate the following:
- **Not Configured**: Indicates **High Availability settings** are not configured.
- **Processing**: Indicates **High Availability Settings** are being processed to take effect.
- **Primary**: Indicates that the node is elected as the primary 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



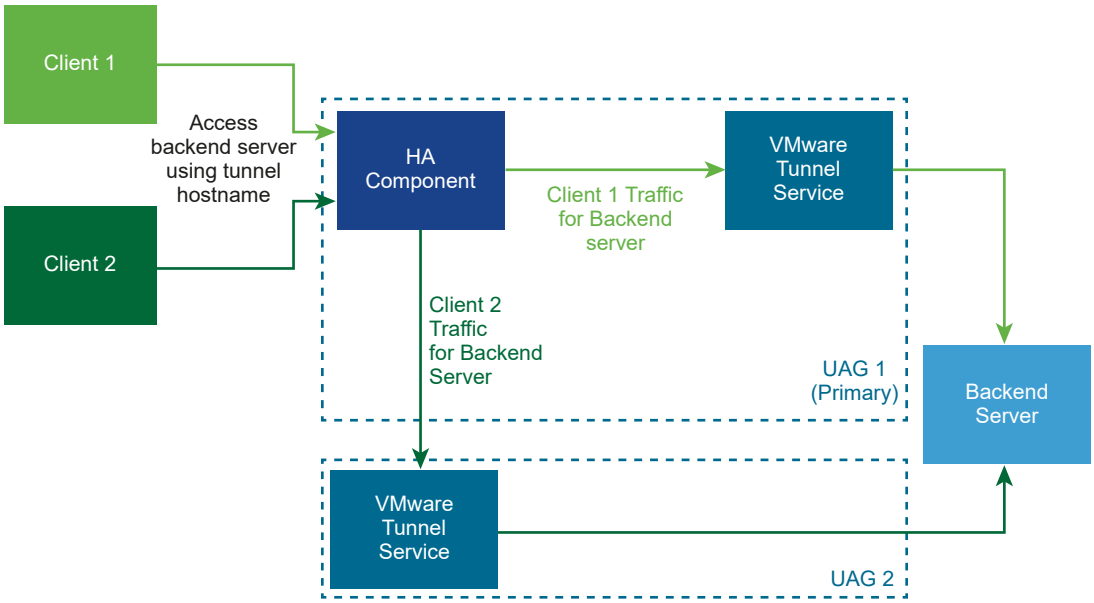
Mode and Affinity: The affinity is based on the source IP address. The first connection from the client is distributed using round robin mechanism. However subsequent connections from the same client are sent to the same Unified Access Gateway which handled the first connection.

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

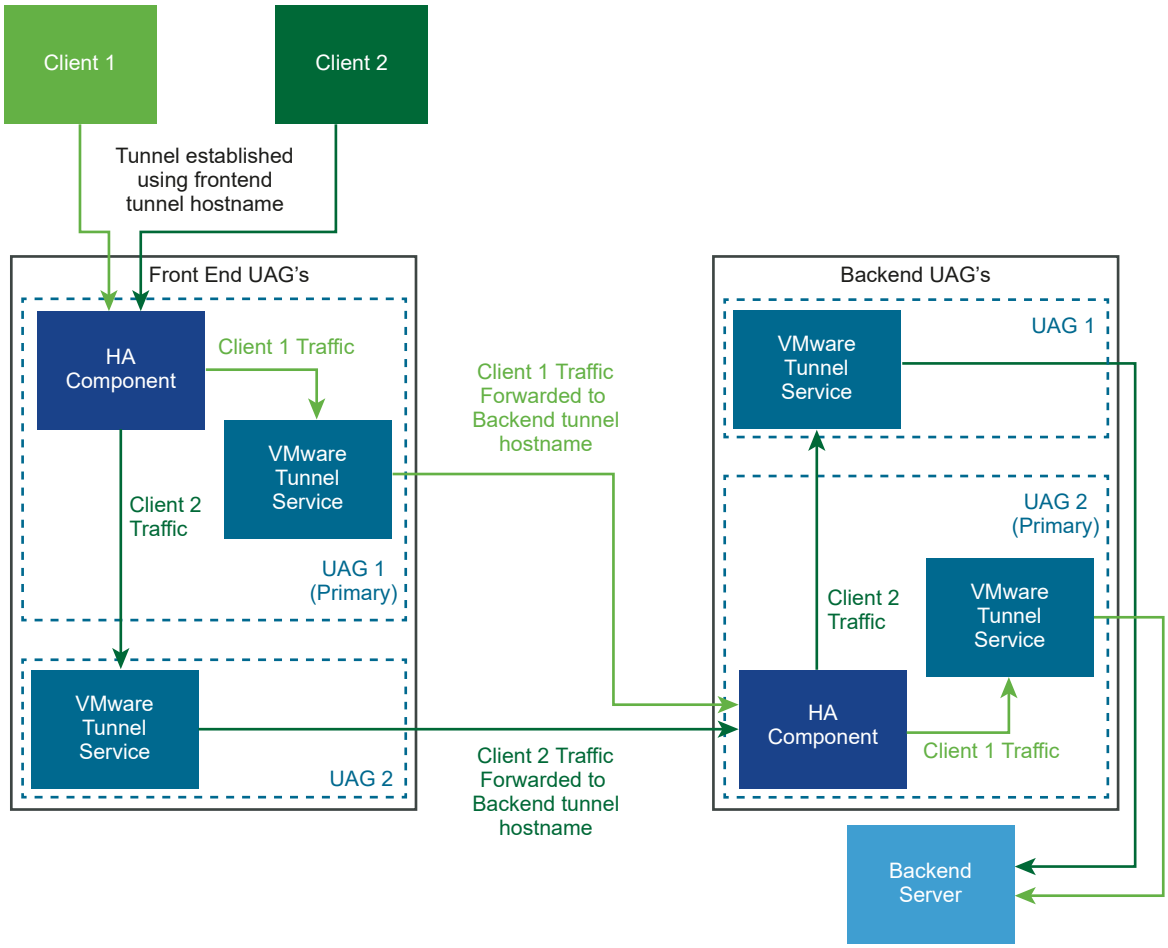
VMware Tunnel (Per-App VPN) is configured with cascade settings in the Workspace ONE UEM console.

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



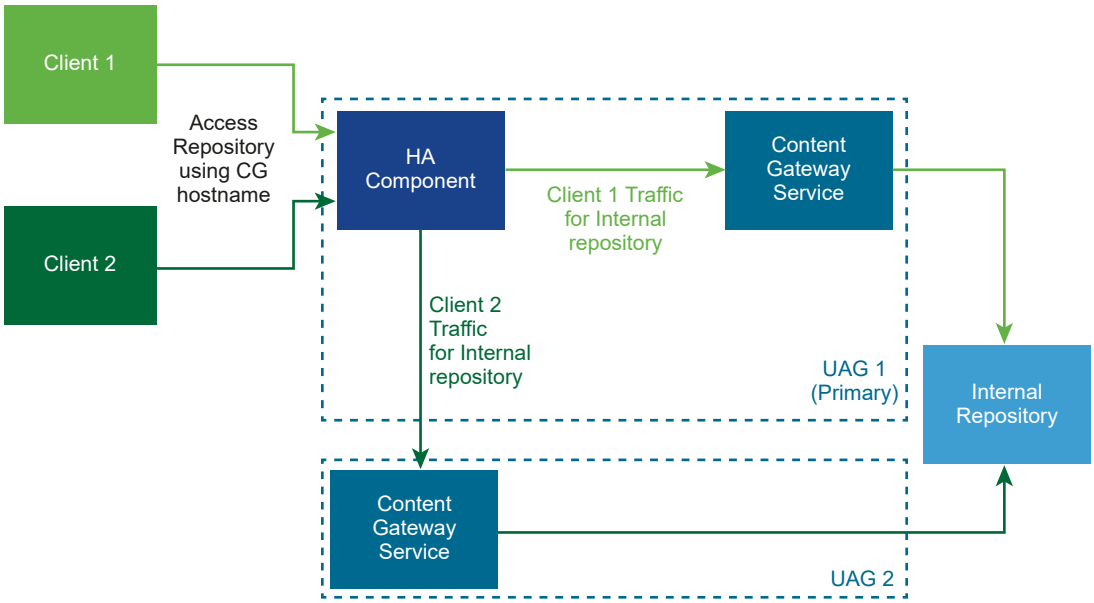
Mode and Affinity: Least connections algorithm is used for HA and load distribution. A new request is sent to the server with the fewest number of current connections to clients. Session affinity is not required as they are stateless connections.

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

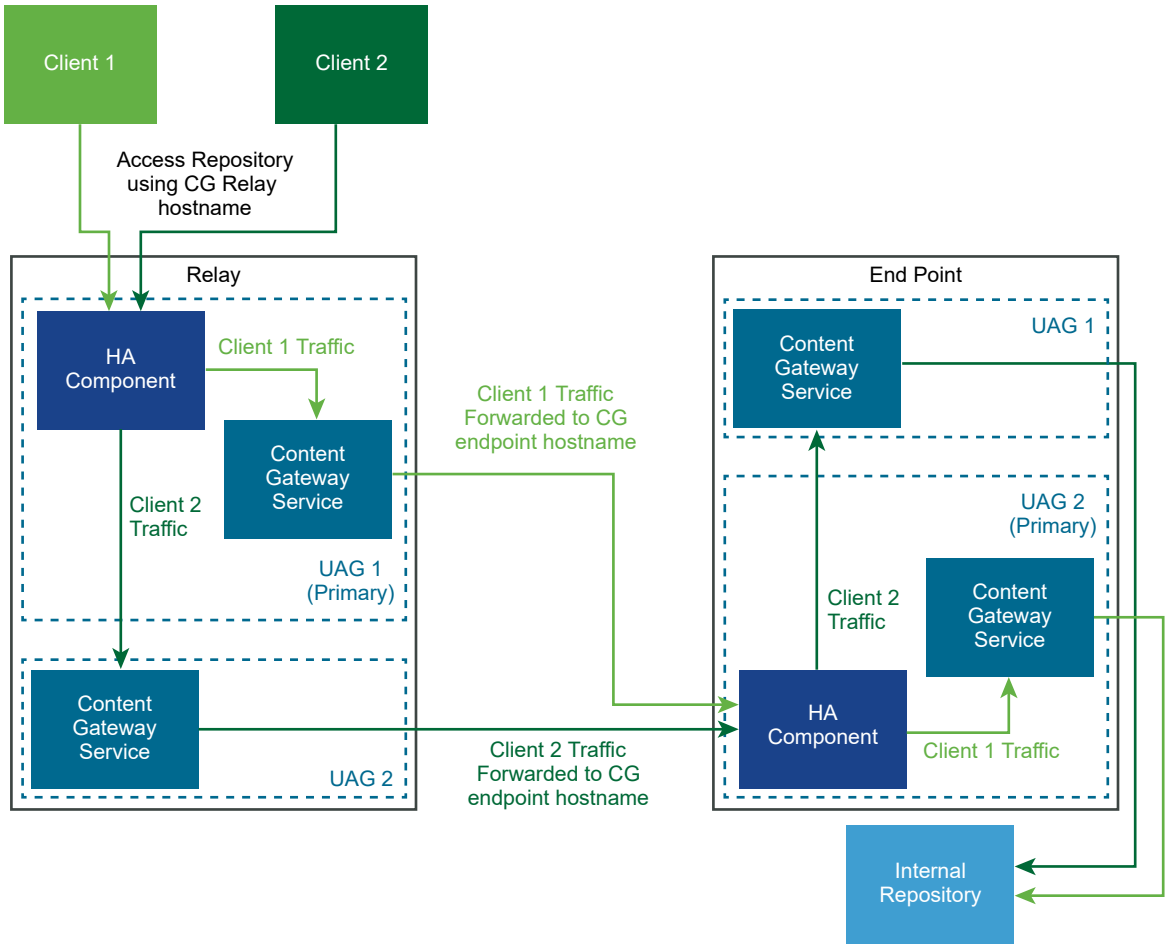
Content Gateway is configured with Relay and Endpoint configuration in the Workspace ONE UEM console.

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.

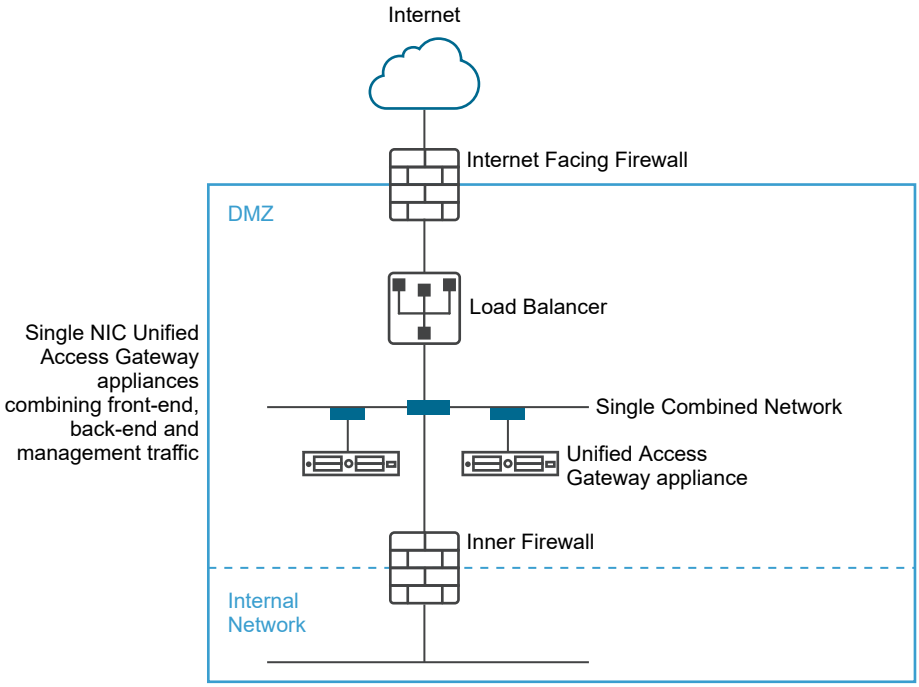
You can specify one, two, or three NICS settings which are specified as onenic, twonic or threenic.

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 (eth0) 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.

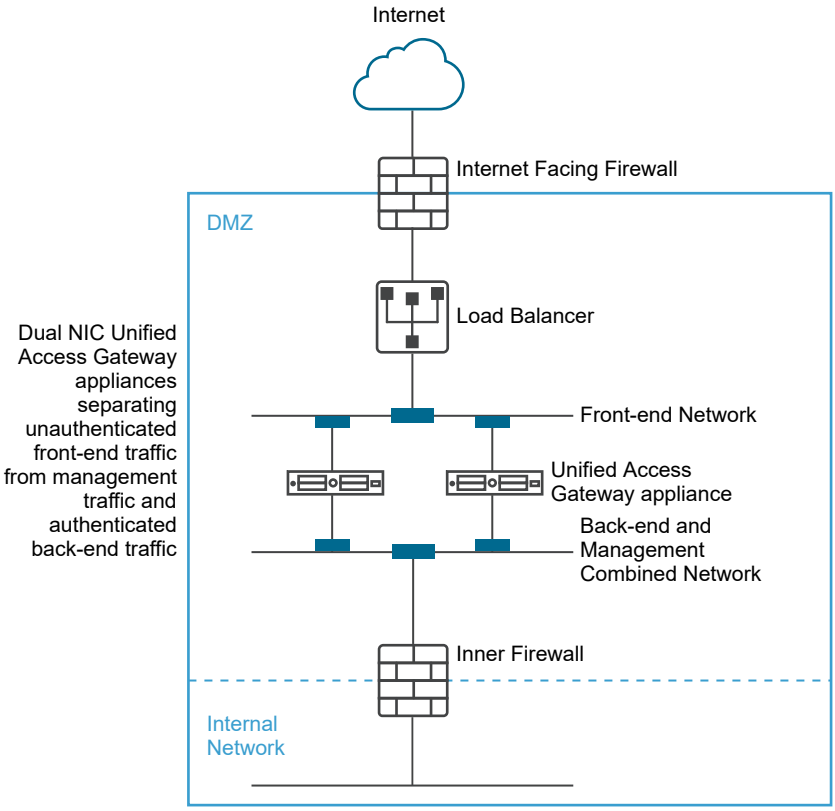
Figure 1-7. Unified Access Gateway Single NIC Option



Separating Unauthenticated User Traffic from Back-End and Management Traffic

An alternative option over the single NIC deployment (eth0) 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 (eth1).

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

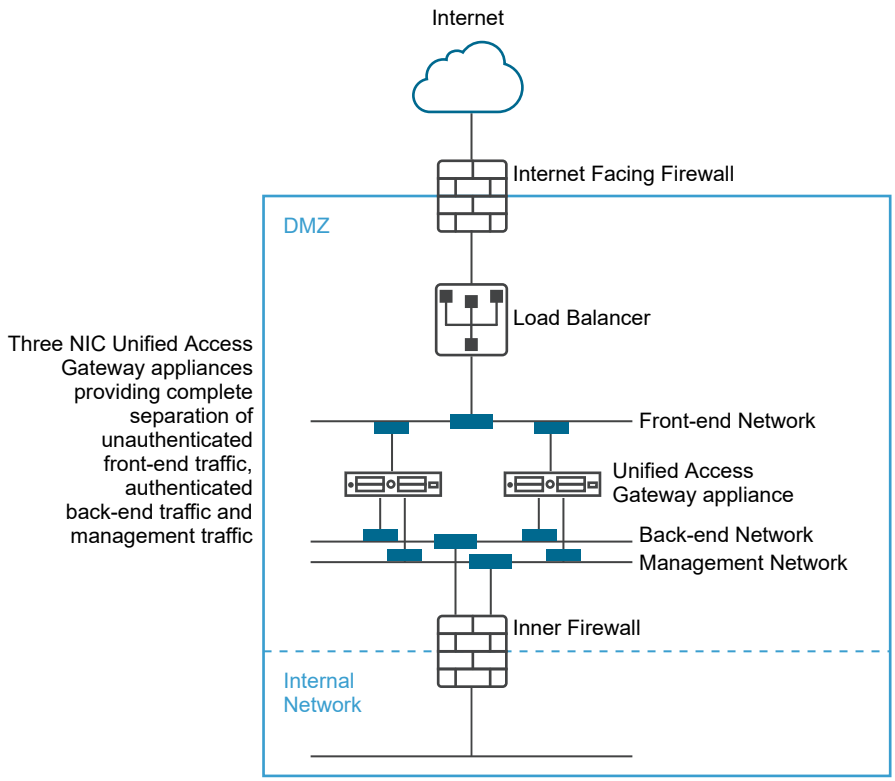
If a device on the unauthenticated front-end network, such as the load balancer, was compromised then reconfiguring that device to bypass Unified Access Gateway is not possible in this two NIC deployment. It combines layer 4 firewall rules with layer 7 Unified Access Gateway security. Similarly, if the 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** toggle is turned on, 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 toggle is turned off, or `HTTP/1.1 503`, if the Quiesce Mode toggle is tuned on.

  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. Turn on the **Quiesce Mode** toggle 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. In the **Advanced Settings** section, click the **System Configuration** gearbox icon.
2. Turn on the **Join CEIP** toggle.

   If you turn on this toggle, the Customer Experience Improvement Program dialog box appears with the check box selected to indicate that you are joining the program.
3. Review the information on the dialog and click **Close**.
4. Click **Save** on the System Configuration page to save your changes.

Deploying Unified Access Gateway Appliance

2

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

Two versions of the Unified Access Gateway OVA are available, standard version and a FIPS version.

The FIPS version of the OVA supports the following Edge services:

- Horizon (pass-through auth, certificate auth, and SAML auth)

  Note Certificate authentication includes both smart card authentication and device certificate authentication.

- VMware Per-App Tunnel
- Secure Email Gateway

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. FIPS mode cannot be changed after Unified Access Gateway is deployed.

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.

Read the following topics next:

- Using the OVF Template Wizard to Deploy Unified Access Gateway
- Configuring Unified Access Gateway From the Admin Configuration Pages
- Update TLS 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.

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, Large, and Extra 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 16GB RAM
  - Extra Large - 8 core and 32GB RAM

  You can configure these settings using PowerShell. For information about PowerShell parameters, see Using PowerShell to Deploy the Unified Access Gateway Appliance.

  For more information about the Unified Access Gateway sizing recommendations, you can see VMware Configuration Maximums.

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-unified-access-gateway-YY.MM.0.0-xxxxxxx_OVF10.ova`), where *YY.MM* is the version number and *xxxxxxx* is the build number.
- If there is 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 an OVF template** page, click **URL** and enter a URL to download and install the OVF template from the internet or click **Local file** to browse to the `.ova` file that you downloaded. 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.

Table 2-1. OVF Deployment Options

Option	Description
Select a name and folder	
Name and Location	Enter a name for the Unified Access Gateway virtual appliance in the **Virtual machine name** field. The name must be unique within the inventory folder. Names are case-sensitive. **Select a location for the virtual machine** from the list.
Select a compute resource	
Host / Cluster	Select the host or cluster on which you want to run the virtual appliance. Result: Compatibility and validation checks are done to verify if the compute resource can support the OVF.
Review details Verify the OVF deployment details.	
Configuration	

Table 2-1. OVF Deployment Options (continued)

Option	Description
Select a 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 16GB RAM ■ **Extra Large** - 8 core and 32GB RAM
Select storage	
Select virtual disk format	For evaluation and testing environments, select the Thin Provision format. For production environments, select one of the Thick Provision formats. Thick Provision Eager Zeroed is a type of thick virtual disk format that supports clustering features such as fault tolerance but takes much longer to create than other types of virtual disks.
VM storage policy	Datastore default or any other configured storage policy. For more information, see *Virtual Machine Storage Policies* in the *VMware vSphere Documentation* at VMware Docs.
Select networks	

Table 2-1. OVF Deployment Options (continued)

Option	Description
	If you are using a vSphere Web Client, the Select 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. 1 If you are using more than one NIC, on the **ManagementNetwork** row, select the destination network, and then 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. 2 If you have a third NIC, select the third row and complete the settings. If you are using only two NICs, for **BackendNetwork** row, select the same network that you used for **ManagementNetwork**. 3 Select the **Internet** row and 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. Click **NEXT**. **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. DNS Server and default gateway settings are global and not associated with any specific NIC.
Customize template	

Table 2-1. OVF Deployment Options (continued)

Option	Description
Networking 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. **Note** ■ The values are case-sensitive. ■ While deploying Unified Access Gateway using the vSphere Client HTML5 in vSphere 6.7 or earlier, only NIC1 (eth0) is available for configuration. Multiple NICs are available for configuration when using the vSphere client HTML5 in vSphere 7.0. ■ **IPMode for NIC1 (eth0):** 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 (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.

Table 2-1. OVF Deployment Options (continued)

Option	Description
	■ **NIC 1 (eth0) IPv6 address**. Enter the IPv6 address for the NIC if you entered STATICV6 for the NIC mode. ■ **DNS server addresses**. Enter space-separated IPv4 or IPv6 addresses of the domain name servers for the 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 ■ **DNS Search Domain**. Enter space-separated DNS Search list. ■ **NIC 1 (eth0) IPv4 Netmask**. Enter the IPv4 netmask for the NIC. ■ **NIC 1 (eth0) IPv6 Prefix**. Enter the IPv6 prefix for the NIC. ■ **NIC1 (eth0) Custom Configuration**. Enter the custom configuration value for the NIC in the format, `SectionName^Parameter=Value`. An example of a custom configuration entry is `DHCP^UseDNS=false`. This value, when used, disables the usage of DNS IP addresses provided by the DHCP server. Using the same format, you can add multiple such systemd.network configuration entries separated by semi-colons. ■ **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. ■ **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.
Unified Gateay Appliance name	Enter the host name of the appliance for identification. If you do not enter any name, the system automatically generates the name.
Join CEIP	Select **Join the VMware Customer Experience Improvement Program** to join CEIP or deselect the option to leave CEIP.
Password Options	
OS Login Username	Enter the username to access the local console of Unified Access Gateway. When configured, a new sudo privileged user with given username is created and root login is disabled. Only a-z, 0-9, underscrore (_) and hyphen (-) are allowed and the maximum length is 32. **Note** Leave this field blank to use root user.

Table 2-1. OVF Deployment Options (continued)

Option	Description
Password for OS login	Enter the password for OS login. This password applies to either root or the custom user as configured in **OS Login Username** field.
Password Expiration in days for the OS user	Enter the Password expiration policy for the OS user. If set to zero password never expires. The default value is 365 days.
Password policy minimum length	Enter the minimum length of the password. The default value is 6.
Password policy for minimum character classes	Enter password policy for minimum number (1,2,3,4) of classes of character type (uppercase, lowercase, digit, others).
Password policy for maximum failed attempts	Enter the maximum failed attempts allowed. The default value is 3.
Password policy for unlock time in seconds on maximum failed attempts	Enter the time in seconds to unlock the password when you have reached maximum failed attempts. The default value is 900.
Session idle timeout for OS user in seconds	Enter the session idle timeout for OS user. The range is 30 -3600 seconds. Session expiry is disabled if this is set to zero (0). The default value is 300.
Maximum limit on concurrent login sessions for sudo user	Enter the maximum limit on cuncurrent login sessions for sudo user. If sudo user is not configured, this setting is ignored. The default value is 10 and minimum configurable is 1. There is no maximum limit.
Password for the admin user, which enables REST API access	
Admin password policy for minimum length	Enter the minimum length of the admin password. The default value is 6.
Admin password policy for maximum failed attempts	Enter the maximum failed attempts allowed. The default value is 3.
Admin password policy for unlock time in seconds on maximum failed attempts	Enter the time in seconds to unlock the admin password when you have reached maximum failed attempts. The default value is 900.
Admin session idle timeout for OS user in seconds	Enter the session idle timeout for the admin.The default value is 10 and the maximum is 1440 minutes.
Maximum concurrent sessions for admin console users	Enter the maximum limit on cuncurrent login sessions for the admin. The default value is 5 and maximum value is 50. When maximum session count exceeds for a user, least recently used session will be expired.
Compliance	

Table 2-1. OVF Deployment Options (continued)

Option	Description
Enable DISA STIG compliance	Sets the OS configuration to comply with the current Photon OS 3.0 DISA STIG Readiness Guidelines. Select this check box to automatically configure password complexity and other STIG requirements. **Note** This setting should be used with the FIPS version when DISA STIG OS compliance is required.
System Properties	
Enable SSH	Option to enable SSH for accessing Unified Access Gateway virtual machine.
Allow SSH root login using password	Option to access Unified Access Gateway virtual machine by using an SSH root login and password. By default, the value of this option is `true`.
Allow SSH login using key pair	Option to access Unified Access Gateway virtual machine by using an SSH root login and public-private key pairs. By default, this value is `false`. The Unified Access Gateway Admin UI has a field, **SSH Public Keys**, where an administrator can upload public keys to allow the configured or the root user access to Unified Access Gateway when using the public-private key pair option. For this field to be available on the Admin UI, the value of this option and **Enable SSH** must be `true` at the time of deployment itself. If either of these options are not `true`, the **SSH Public Keys** field is not available on the Admin UI. **SSH Public Keys** field is an advanced system setting in the Admin UI. See Configure Unified Access Gateway System Settings.
Login Shell Banner Text	Option to customize the banner text displayed when logging into Unified Access Gateway using SSH or the vSphere Client's Web Console. This option can be configured only at the time of deployment. If you do not configure this option, the default text is displayed: *VMware EUC Unified Access Gateway*. Only ASCII characters are supported in the customized text. For multi-line banner texts, `\n` must be used as the line seperator. **Note** When Unified Access Gateway is deployed using the OVF template and the login banner text is configured, at the first launch of Unified Access Gateway, the vSphere Client's Web Console displays the default banner text and the customized banner text is ignored. On subsequent launches, the customized banner text is displayed.

Table 2-1. OVF Deployment Options (continued)

Option	Description
SSH Interface	Configure the network interface on which SSH login is enabled. By default, SSH is enabled on all the interfaces. The supported values are `eth0`, `eth1`, and `eth2` based on the configuration.
SSH Port	Configure the port on which SSH is enabled. The default value is `22`.
Commands to Run During First boot	Enter semi-colon separated list of commands in plain-text or base64 encoded format to run during first boot up of Unified Access Gateway. Maximum size is 8kB. For more information, see Configurable Boot Time Commands for First Boot and Every Boot.
Commands to Run During Every Boot	Enter semi-colon separated list of commands in plain-text or base64 encoded format to run during every boot up of Unified Access Gateway. Maximum size is 8kB. For more information, see Configurable Boot Time Commands for First Boot and Every Boot.
SecureRandom Source	Allows you to configure the secure random bit generator source used by Java processes for cryptographic functions. This option can be configured only at the time of deployment. Supported values are: `/dev/random` and `/dev/urandom`. By default, `/dev/random` is used in the non-FIPS mode and `/dev/urandom` is used in the FIPS mode.

5 On the **Ready to complete** page, review the information 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 start. A log of these messages is also available in the file `/var/log/boot.msg`.

6 Power on the virtual machine.

7 When the appliance is powered on, 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://<mycoUnifiedGatewayAppliance>.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 if the virtual machine has the IP address displayed during the installation of the OVA. If the IP address is not configured, use the VAMI command mentioned in the UI to reconfigure the NICs. Run the command as "`cd /opt/vmware/share/vami`" then the command "`./vami_config_net`".

Configuring Unified Access Gateway From the Admin Configuration Pages

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

Note 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, and X.509 Certificate
- 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.

- Monitor the sessions of each edge service on Unified Access Gateway.
- Download Unified Access Gateway log files.
- Export Unified Access Gateway settings to retrieve the configuration settings.
- Set the log level settings.

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 Addresses of the DNS servers

    Note A maximum of two DNS server IP addresses can be specified.

    Unified Access Gateway uses the platform default fallback public DNS addresses only when no DNS server addresses are provided to Unified Access Gateway either as part of the configuration settings or through DHCP.
  - 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 Unified Access Gateway appliance name. **Note** The appliance name can consist of a text string up to 24 characters which includes alphabets (A-Z), digits (0-9), minus sign `(-)`, and period `(.)`. However, the appliance name cannot have spaces.
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_GB`** for British English

TLS Server Cipher Suites	Enter a comma-separated, list of cipher suites, which are cryptographic algorithms used to encrypt inbound TLS connections to Unified Access Gateway
	This option is used with few other options such as TLS versions, named groups, signature schemes, and so on that are used in enabling various security protocols.
	The TLS Server Cipher suites supported in FIPS mode are as follows:
	■ Default enabled cipher suites:
	  ■ `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
	  ■ `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`
	■ Cipher suites that are supported and can be manually configured:
	  ■ `TLS_RSA_WITH_AES_256_CBC_SHA256`
	  ■ `TLS_RSA_WITH_AES_128_CBC_SHA256`
	  ■ `TLS_RSA_WITH_AES_256_CBC_SHA`
	  ■ `TLS_RSA_WITH_AES_128_CBC_SHA`
	The default TLS Server Cipher suites supported in non-FIPS mode are as follows:
	■ `TLS_AES_128_GCM_SHA256`
	■ `TLS_AES_256_GCM_SHA384`
	■ `TLS_CHACHA20_POLY1305_SHA256`
	■ `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`
	■ `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
	■ `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256`
	■ `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384`
	This option can be configured during PowerShell deployment by adding the `cipherSuites` parameter in the `ini` file. See Using PowerShell to Deploy the Unified Access Gateway Appliance.

Option	Default Value and Description
TLS Client Cipher Suites	Enter a comma-separated, list of cipher suites, which are cryptographic algorithms used to encrypt outbound TLS connections to Unified Access Gateway This option is used with few other options such as TLS versions, named groups, signature schemes, and so on that are used in enabling various security protocols. The following cipher suites are supported in FIPS mode: ■ `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384` ■ `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256` ■ `TLS_DHE_RSA_WITH_AES_128_CBC_SHA256` ■ `TLS_DHE_RSA_WITH_AES_256_CBC_SHA256` ■ `TLS_DHE_RSA_WITH_AES_256_GCM_SHA384` ■ `TLS_DHE_RSA_WITH_AES_128_GCM_SHA256` ■ `TLS_RSA_WITH_AES_256_CBC_SHA256` ■ `TLS_RSA_WITH_AES_128_CBC_SHA256` ■ `TLS_RSA_WITH_AES_256_CBC_SHA` ■ `TLS_RSA_WITH_AES_128_CBC_SHA` In the non-FIPS mode, by default, all cipher suites that are supported by the SSL library (Java/Open SSL) can be used. This option can be configured during PowerShell deployment by adding the `outboundCipherSuites` parameter in the `ini` file. See Using PowerShell to Deploy the Unified Access Gateway Appliance.
SSL Provider	Select the SSL Provider implementation used for handling TLS connections. To configure `TLS Named Groups` and `TLS Signature Schemes`, the value of this option must be `JDK`. By default, the value of this option is `OPENSSL`. **Note** When the value of this option is `JDK`, OCSP-based certificate revocation check is not supported. However, CRL-based certificate revocation check is supported. Any changes to this option results in Unified Access Gateway services getting restarted. Ongoing Unified Access Gateway sessions are not retained during the restart. This option can be configured during PowerShell deployment by adding the `sslProvider` parameter in the `ini` file. See Using PowerShell to Deploy the Unified Access Gateway Appliance.
TLS Named Groups	Allows the administrator to configure the desired named groups (elliptic curves) from a list of supported named groups used for key exchange during SSL handshake. This option allows comma-separated values. Some of the supported named groups are as follows: `secp256r1, secp384r1, secp521r1`. To configure this option, ensure that the `SSL Provider` option is set to `JDK`. Else, the `TLS Named Groups` option is disabled. Any changes to this option results in Unified Access Gateway services getting restarted. Ongoing Unified Access Gateway sessions are not retained during the restart. This option can be configured during PowerShell deployment by adding the `tlsNamedGroups` parameter in the `ini` file. See Using PowerShell to Deploy the Unified Access Gateway Appliance.

Option	Default Value and Description
TLS Signature Schemes	Allows the administrator to configure the supported TLS signature algorithms used for key validation during SSL handshake. This option allows comma-separated values. For example: some of the supported signature schemes are as follows: `rsa_pkcs1_sha`, `rsa_pkcs1_sha256`, `rsa_pkcs1_sha384`, `rsa_pss_rsae_sha256`, and `rsa_pss_rsae_sha384`. To configure this option, ensure that the `SSL Provider` option is set to `JDK`. Else, the `TLS Signature Schemes` option is disabled. Any changes to this option results in Unified Access Gateway services getting restarted. Ongoing Unified Access Gateway sessions are not retained during the restart. This option can be configured during PowerShell deployment by adding the `tlsSignatureSchemes` parameter in the `ini` file. See Using PowerShell to Deploy the Unified Access Gateway Appliance.
Enable TLS 1.0	By default, this toggle is turned off. Turn on this toggle to enable TLS 1.0 security protocol.
Enable TLS 1.1	By default, this toggle is turned off. Turn on this toggle to enable TLS 1.1 security protocol.
Enable TLS 1.2	By default, this toggle is turned on. The TLS 1.2 security protocol is enabled.
Enable TLS 1.3	By default, this toggle is turned on. The TLS 1.3 security protocol is enabled.
Allowed Host Headers	Enter the IP address or the host name as the host header values. This setting is applicable for the Unified Access Gateway deployment with Horizon and Web Reverse Proxy use cases. For Unified Access Gateway deployments with Horizon, you might be required to provide multiple host headers. This depends on whether N+1 Virtual IP (VIP) is used and the Blast Secure Gateway (BSG) and VMware Tunnel are enabled and configured to use port 443 externally. The Horizon clients send the IP address in the host header for the blast connection request. If the BSG is configured to use port 443, then the allowed host headers must contain the external IP address of the BSG hostname configured in the blast external URL for the specific UAG. If the host header values are not specified then any host header value sent by the client is accepted by default.
CA Certificate	This option is enabled when a Syslog server is added. Select a valid Syslog Certificate Authority certificate.
Health Check URL	Enter a URL that the load balancer connects to and checks the health of Unified Access Gateway.
HTTP Health Monitor	By default, this toggle is turned off. The default configuration redirects HTTP health check URL requests to HTTPS. When you turn on this toggle, Unified Access Gateway responds to the health check request even on HTTP.
Cookies to be Cached	The set of cookies that Unified Access Gateway caches. The default is none.

Option	Default Value and Description
Session Timeout	Default value is **36000000** milliseconds. **Note** The value of `Session Timeout` on the Unified Access Gateway must be the same as the value of the `Forcibly disconnect users` setting on the Horizon Connection Server. The `Forcibly disconnect users` setting is one of the General Global Settings in the Horizon console. For more information about this setting, see *Configuring Settings for Client Sessions* in the *VMware Horizon Administration* documentation at VMware Docs.
Quiesce Mode	Turn on this toggle to pause the Unified Access Gateway appliance to achieve a consistent state to perform maintenance tasks
Monitor Interval	Default value is **60**.
Password Age	Number of days the password is valid for the user in the ADMIN role. The default value is `90` days. Maximum value that can be configured is `999` days. For password to never expire, specify the value of this field as `0`.
Monitoring Users Password Age	Number of days the password is valid for the users in the MONITORING role. The default value is `90` days. The maximum value that can be configured is `999` days. For the password to never expire, specify the value of this field as `0`.
Request Timeout	Indicates the maximum time Unified Access Gateway waits for a request to be received. The default value is `3000`. This timeout must be specified in milliseconds.
Body Receive Timeout	Indicates the maximum time Unified Access Gateway waits for a request body to be received. The default is `5000`. This timeout must be specified in milliseconds.
Maximum Connections per Session	Maximum number of TCP connections allowed per TLS session. The default value is `16`. For no limit on the allowed number of TCP connections, set the value of this field to `0`. **Note** Field value of `8` or lower causes errors in the Horizon Client .
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	The maximum wait time in milliseconds before which authentication must happen. The default is 300000. If 0 is specified, it indicates no time limit for authentication.
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.

Option	Default Value and Description
Max Allowed System CPU	Indicates the maximum allowed average system CPU usage in one minute. When the configured CPU limit is exceeded, new sessions are not allowed and the client receives an HTTP 503 error to indicate that the Unified Access Gateway appliance is temporarily overloaded. Additionally, the exceeded limit also allows a load balancer to mark the Unified Access Gateway appliance down so that new requests can be directed to other Unified Access Gateway appliances. Value is in percentage. Default value is `100%`.
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	Turn on this toggle to enable SNMP service. Simple Network Management Protocol collects system statistics, memory, disk space usage statistics, and Tunnel edge service MIB information by Unified Access Gateway. The list of available Management Information Base (MIB), ■ UCD-SNMP-MIB::systemStats ■ UCD-SNMP-MIB::memory ■ UCD-SNMP-MIB::dskTable ■ VMWARE-TUNNEL-SERVER-MIB::vmwTunnelServerMIB
SNMP Version	Select the desired SNMP version. **Note** If you have deployed Unified Access Gateway through PowerShell, enabled SNMP, but not configured SNMPv3 settings either through PowerShell or the Unified Access Gateway Admin UI, then by default SNMPv1 and SNMPV2c versions are used. For configuring the SNMPv3 settings in the Admin UI, see Configure SNMPv3 Using the Unified Access Gateway Admin UI. For configuring SNMPv3 settings through PowerShell deployment, certain SNMPv3 settings must be added to the `INI` file. See Using PowerShell to Deploy the Unified Access Gateway Appliance.
Admin Disclaimer Text	Enter the disclaimer text based on your organization's user agreement policy. For an administrator to successfully log into the Unified Access Gateway Admin UI, the administrator must accept the agreement policy. The disclaimer text can be configured either through PowerShell deployment or by using the Unified Access Gateway Admin UI. For more information about the PowerShell setting in the `INI` file, see Using PowerShell to Deploy the Unified Access Gateway Appliance. While using the Unified Access Gateway Admin UI to configure this text box, the administrator must first log into the Admin UI and then configure the disclaimer text. On subsequent administrator logins, the text is displayed for the administrator to accept before accessing the login page.
DNS	Enter Domain Name System addresses that are added to `/run/systemd/resolve/resolv.conf` configuration file. It must contain a valid DNS search address. Click '+' to add a new DNS address.

Option	Default Value and Description
DNS Search	Enter Domain Name System search that is added to `/run/systemd/resolve/resolv.conf` configuration file. It must contain a valid DNS search address. Click '+' to add a new DNS search entry.
Time Sync With Host	Turn on this toggle to synchronize the time on the Unified Access Gateway appliance with the time of the ESXi host. By default, this toggle is turned off. This option uses VMware Tools for time synchronization and is supported only when Unified Access Gateway is deployed on the ESXi host. If you choose this option for time synchronization, then the `NTP Servers` and `FallBack NTP Servers` options are disabled. This option can be configured through PowerShell by adding the `hostClockSyncEnabled` parameter in the `INI` file. See Using PowerShell to Deploy the Unified Access Gateway Appliance.
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. If you choose this option for time synchronization, then the `Time Sync With Host` is disabled.
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. If you choose this option for time synchronization, then the `Time Sync With Host` is disabled.
Extended Server Certificate Validation	Turn on this toggle to ensure that Unified Access Gateway performs extended validation on the received SSL server certificate for outbound TLS connections to the backend servers. The extended checks include validating the expiry of the certificate, mismatch in the hostname, certificate revocation status, and extended key usage values. By default, this option is disabled. This option can be configured through PowerShell by adding the `extendedServerCertValidationEnabled` parameter in the `ini` file. See Using PowerShell to Deploy the Unified Access Gateway Appliance.
SSH Public Keys	Upload public keys to enable root user access to Unified Access Gateway virtual machine when using the public-private key pair option. Administrators can upload multiple, unique public keys to Unified Access Gateway. This field is visible on the Admin UI only when the following SSH options are set to `true` during deployment: **Enable SSH** and **Allow SSH root login using key pair**. For information about these options, see Deploy Unified Access Gateway Using the OVF Template Wizard.

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.

Configure SNMPv3 Using the Unified Access Gateway Admin UI

You can configure SNMPv3 in the Unified Access Gateway Admin UI. SNMPv3 has enhanced security features such as authentication and privacy. Unified Access Gateway continues to support SNMPv1 and SNMPv2c, which are the default versions. You can also configure SNMPv3 through PowerShell deployment by adding certain SNMPv3-related settings in the `INI` file.

If you have deployed Unified Access Gateway through PowerShell, enabled SNMP, but not configured SNMPv3 settings, then by default SNMPv1 and SNMPV2c versions are used.

You can also configure SNMPv3 settings using PowerShell. For more information about these parameters, see Using PowerShell to Deploy the Unified Access Gateway Appliance.

Procedure

1. In the Admin UI's **Configure Manually** section, click **Select**.
2. In the **Advanced Settings** section, click the **System Configuration** gearbox icon.
3. Turn on the **Enable SNMP** toggle to enable the SNMP service.

   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.
4. Select the **SNMP Version** as `SNMPv3`.
5. Enter the **SNMPv3 USM User** name.
6. Enter the **SNMP Engine ID**.

   This value is unique for each Unified Access Gateway appliance.

   The maximum length of the engine ID is limited to 27 characters.
7. Select the **SNMPv3 Security Level**.

8 Depending on the security level selected in the previous step, perform the following actions:

Security Level	Actions
`No Auth, No Priv` **(No Authentication, No Privacy)**	Click **Save**. No further actions are necessary.
`Auth, No Priv` **(Authentication, No Privacy)**	a Select the **SNMPv3 Auth Algorithm**. b Enter the **SNMPv3 Auth Password**. Password must be at least 8 characters long. c **Confirm Auth Password** entered in the previous step. d Click **Save**.
`Auth, Priv` **(Authentication, Privacy)**	a Select the **SNMPv3 Auth Algorithm**. The supported values are as follows: `MD5`, `SHA`, `SHA-224`, `SHA-256`, `SHA-384`, and `SHA-512`. b Enter the **SNMPv3 Auth Password**. Password must be at least 8 characters long. c Confirm the **Auth Password** entered in the previous step. d Select the **SNMPv3 Privacy Algorithm**. The supported values are `DES` and `AES`. e Select the **SNMPv3 Privacy Password**. Password must be at least 8 characters long. f **Confirm Privacy Password** entered in the previous step. g Click **Save**.

Configure Syslog Server Settings

The Syslog server logs the events that occur on the Unified Access Gateway (UAG) appliance.

Configure the Syslog server settings by providing details such as Category, Protocol, Syslog URL, Syslog Client Certificate, and so on. You can configure multiple syslog servers with different protocols.

Procedure

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

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

3 In the Syslog Server Settings window, enter the following details.

Option	Description
Add Syslog Entry	Click **Add Syslog Entry** to add new syslog server details to the table.
Category	Select the syslog category from the drop-down menu. The options are: ■ All Events: All events including audit, edge services, admin, and so on are logged to the Syslog server. ■ Audit Events Only: Only audit events are logged to the Syslog server.

Option	Description

Protocol	Select the Syslog server type from the drop-down menu.
	The options are:
	■ UDP: Syslog messages are sent over the network in plain text over UDP. It is mandatory to add the Syslog URL.
	■ TCP: Syslog messages are streamed over TCP. It is mandatory to add the Syslog URL.
	■ TLS: TLS encryption is added between two syslog servers to keep the messages secured. Enter the following details.
	  ■ **Host**: Add the syslog server host name.
	  ■ (Optional) **Port**: Add a new syslog server port. The default port number is `514`.
	  ■ (Optional) **Accepted Peer**: Add a new syslog accepted peer. It can be an IP address or a name. Examples:
	  ■ `1.2.3.4`
	  ■ `server.example.com`
	  ■ **CA Certificate**: Select a valid syslog CA certificate if you have configured syslog servers.
	■ MQTT: Syslog messages are streamed over MQTT. Enter the following details.
	  ■ **URL**: Add a new URL or host name or IP address.
	  ■ **Topic**: Add a string that MQTT recipient uses to filter messages for each connected client.

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 or combination of host name and IP address with optional port number. The default port number is `514`. Example URLs: ■ `server1.example.com` ■ `101.20.30.40` ■ `1.2.3.4:515` By default Content Gateway and Secure Email Gateway edge services events are logged. To log events on syslog server for Tunnel Gateway edge service configured on Unified Access Gateway, an administrator has to configure the Syslog on Workspaceone UEM console with the information. `Syslog Hostname=localhost and Port=514` Click **Add** to add the server details. The added details appear in a table on the Syslog Server Settings window but not saved to the back-end until you click **Save**.
Syslog Client Certificate	Select a valid Syslog client certificate in the PEM format. **Note** The client certificate and key, when configured is applied to all the servers configured in the TLS mode.

Option	Description
Syslog Client Certificate Key	Select a valid Syslog client certificate key in the PEM format. **Note** When Unified Access Gateway is deployed using PowerShell, if an invalid or expired certificate or key is provided, the admin UI instance will not be available.
Syslog Include System Messages	Turn on this toggle to enable system services such as haproxy, cron, ssh, kernel, and system to send system messages to the syslog server. By default, the toggle is turned off. Alternately, this feature can also be configured through the PowerShell deployment. For more information about the setting in the `INI` file, see Using PowerShell to Deploy the Unified Access Gateway Appliance.

4 Click **Save**.

If you want to change the added Sylsog servers' settings, click the gearbox icon corresponding to the servers listed in the table. A window appears with the server details. After making the changes, click **OK** to update the details and then click **Save** to save the details to the back-end.

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 are logged in as an admin with ROLE_ADMIN role.
- 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. Each route is in the form ipv4-network-address/bits ipv4-gateway-address. For example, 20.2.0.0/16 10.2.0.1. **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 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.

Password Expiry

Superuser and low-privileged administrators can view the time period left for password expiry. On the **Account Settings** page, the **Password expires in (days)** field provides the countdown in number of days until the date on which the password expires. This field helps users remain aware of the password expiry date and take appropriate action such as reset their password.

Note Password expiry time period is rounded off to the immediate lowest whole number.

For example, if the number of days left for the password to expire is 1 day 23 hours, the value is displayed as 1 day.

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, download logs, and export configurations.

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 **Username** for the user.
   b. (Optional) Turn on the **Enabled** toggle if you want to enable the user immediately after adding the user.
   c. (Optional) By default, the **Pre-expire Password** toggle is turned on. If you do not want to be prompted to change the password upon first logon, turn off the **Pre-expire Password** toggle.
   d. 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 ! @ # $ % * ( ) characters.
   e. 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.

Configure SAML Authentication for Admin UI

You can configure the SAML authentication method to authenticate the users with administrator access to the admin UI. This delegates authentication and authorization to an external SAML 2.0 identity provider (IdP) with Unified Access Gateway admin acting as the SAML Service Provider (SP). When a user accesses Unified Access Gateway admin UI with `https://<<uag-fqdn>>:9443/admin` they are redirected to the external IdP where they are prompted to enter

their credentials. If they are authenticated correctly and authorized, they are redirected back to UAG and automatically logged on.

A SAML application must be created on the IdP specifically for Unified Access Gateway admin. SAML metadata exported from this IdP application is used to configure the SAML trust on Unified Access Gateway. This is a fully federated SAML integration so there is no need to separately add admin users to Unified Access Gateway.

The IdP SAML application can be assigned to specific users or user groups to grant admin access, and the authorized administrator's username is received in the signed SAML assertion NameID field. If the IdP encrypts SAML assertions, then the public SSL certificate from Unified Access Gateway is used to configure this encryption on the IdP.

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 **SAML Login Configuration** and then complete the settings

   a To enable the Enable SAML Authentication setting, toggle the button to **Yes**.

   b Select the Identity provider from the drop-down menu.

Note

- The identity provider is available for selection in the drop-down menu if you have previously uploaded the identity provider metadata file.
- Use the following settings for the SAML configuration on the identity provider's admin console.

Option	Description
Single sign on URL	Enter the assertion consumer service URL as `https://<<uag-fqdn>>:9443/login/saml2/sso/admin`
Audience URI (SP Entity ID)	Enter the audience URL as `https://<<uag-fqdn>>:9443/admin`
SP Issuer	If required, enter the SP issuer as `https://<<uag-fqdn>>:9443/admin`

For information about configuring the identity provider and uploading the identity provider metadata file to UAG, see Configure the Identity Provider with Unified Access Gateway Information and Upload Identity Provider's SAML Metadata to Unified Access Gateway.

4 Click **Save**.

The authentication changes are applied, and the admin user automatically logs out of the admin UI. On the next login, Unified Access Gateway redirects the admin's login request to the identity provider, and on successful authentication, the identity provider provides access to the admin.

Note To revert the admin configuration settings and restore the default password authentication, use the `adminrest` command. For more information, see Recover the Admin using the adminreset Command.

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. Turn on or turn off the **Enable** toggle depending on whether you want to enable or disable the user.

      Note By default, the **Pre-expire Password** toggle is turned on. When the **Pre-expire Password** toggle is turned on, you are prompted to change the password upon first logon.

   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 ! @ # $ % * ( ) characters.
5. Click **Save**.

Reset the Admin Password using the Unified Access Gateway Console

If the admin user password 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.

For more information on root password see, Troubleshooting Root Login Issues.

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
```

Note If non-root administrator is configured for Unified Access Gateway OS login, run the command with sudo. For example, `sudo 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 ! @ # $ % * ( ) characters.

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: ********
```

The admin password must be at least 8 characters long, contains at least one uppercase and one lowercase letter, one digit, and one special character, which includes ! @ # $ % * ( ) characters.

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 recently set. User is 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.

Recover the Admin using the adminreset Command

Use this command to reset the admin access settings to defaults and restart the admin service. This command allows you to recover the Unified Access Gateway admin portal when the portal cannot be accessed due to misconfiguration of settings like TLS ciphers, admin SAML Authentication.

This command resets the following admin access settings to defaults.

- TLS settings - ciphers, protocol, signature schemes, and named groups.
- TLS Certificate - admin TLS certificate is replaced with a new self-signed certificate.
- SAML login for the admin - if this setting is configured, deactivates the admin SAML login and reverts to password login.

Procedure

1. Log in to Unified Access Gateway console with configured user (usually root).
2. Enter the following command to reset the admin access settings.

   ```
   adminreset
   ```

   Note If a non-root administrator is configured for Unified Access Gateway OS login, run the command with sudo. For example, `sudo adminreset`.

3. Enter `y` to confirm.

   Note Alternatively, use the `resetadmin -f` command to forcefully reset all admin access settings, without prompting for confirmation.

Results

The admin reset is completed successfully.

Note You can set the admin password using `adminpwd` command. See Reset the Admin Password using the Unified Access Gateway Console.

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

Unified Access Gateway supports the JSON Web Token (JWT) validation. You can configure the JSON web token settings to validate a SAML artifact issued by Workspace ONE Access during single sign-on to Horizon and to support the Horizon protocol redirect feature when the Unified Access Gateway is used with Horizon Universal Broker.

The Workspace ONE Access issues a JWT wrapped Horizon SAML artifact when the **Wrap Artifact in JWT** check box is enabled in the Workspace ONE Access Horizon configuration. This allows the Unified Access Gateway appliance to block authentication attempts unless a trusted JWT is supplied with the SAML artifact authentication attempt.

In both the use cases, you must specify the JWT settings to permit the Unified Access Gateway to trust the issuer of the JWT tokens received.

Use a dynamic public key URL for the JWT settings so that the Unified Access Gateway automatically maintains the latest public keys for this trust. You must only use static public keys if the Unified Access Gateway cannot access the dynamic public key URL.

The following procedure describes the JSON web token settings configuration:

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:

Option	Default and Description
Name	A name to identify this setting for validation.
Issuer	The JWT issuer values as specified in the issuer claim in the incoming token to be validated. By default, the value of this field is set to the **Name** field. **Note** **Issuer** is configured only for the Universal Broker protocol redirect use case.

Option	Default and Description
Dynamic Public key URL	Enter the URL for dynamically fetching the public key. A public key can either be a single public key or a JSON Web Key Set (JWKS) format. With the JWKS format, multiple JSON Web Key (JWK) format public keys can be obtained for validating the JWT. Each JWK has a unique identifier (kid) and this identifier is present in the JWT provided to UAG. Using this identifier, UAG identifies the public key to be used.
Public key URL thumbprints	Enter the list of public key URL 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.
Trusted Certificates	■ To select a certificate in the PEM format and add to the trust store, click **+**. ■ To remove a certificate from the trust store, click **-**. ■ To provide a different name, edit the alias text box. By default, the alias name is the filename of the PEM certificate.
Public key refresh interval	The time interval in seconds at which the public key is fetched from the URL periodically.
Static Public Keys	**Note** If a dynamic public key URL is not available, set a static public key. Click **+** to select and add a public key to use for JWT validation. The file must be in `PEM` format.

5 Click **Save**.

Results

The details of the parameters are listed under JWT Settings.

Configure Outbound Proxy Settings

For outbound connections to go through a web proxy server from the Unified Access Gateway to the desired host over the Internet, you must configure the **Outbound Proxy Settings** in the Unified Access Gateway Admin UI.

Unified Access Gateway does not support proxy server authentication.

In this release of Unified Access Gateway, the **Outbound Proxy Settings** are supported for the following outbound connections:

- OPSWAT and the file server (used when the on-demand agent executable file is uploaded to Unified Access Gateway by using the **URL Reference** upload type). When outgoing traffic from Unified Access Gateway is for an OPSWAT host, then such a connection must first go through the web proxy server.
- Workspace ONE Intelligence API calls (to fetch Workspace ONE Intelligence Risk Score or to post data to Workspace ONE Intelligence).

- Packages repository when appliance package updates are configured.
- Fetching JWT public key from a configured remote URL.
- Fetching CRL/OCSP information during extended validation of backend server certificates.
- Sending telemetry data to VMware when CEIP flag is enabled.

The following procedure describes the **Outbound Proxy Settings** configuration:

Procedure

1 Log in to the Admin UI and in the **Configure Manually** section, click **Select**.

2 Go to **Advanced Settings > Outbound Proxy Settings** and click the gear box icon.

3 In the **Outbound Proxy Settings** window, click **Add**.

4 Enter the following information:

Option	Default and Description
Name	Multiple proxy settings can be added in the Admin UI. This text box acts as a unique identifier for every proxy setting. **Note** This text box is mandatory and cannot be updated.
Proxy Server URL	Outbound connections from Unified Access Gateway go through the proxy server, which is mentioned in this text box and then to the desired host over the Internet. Value of this text box must either be a hostname or an IP address prefixed with either HTTP or HTTPS.
Proxy Included Host	Outbound connections for the host mentioned in this text box must go through a proxy server from the Unified Access Gateway to the host over the Internet. Value of this text box must either be a hostname or an IP address. For example, if OPSWAT or the file server is the host, the corresponding hostname must be configured in this text box.
Trusted Certificates	■ To select a certificate in the PEM format and add to the trust store, click **+**. ■ To remove a certificate from the trust store, click **-**. ■ To provide a different name, edit the alias text box. By default, the alias name is the filename of the PEM certificate.

5 Click **Save**.

Configure Unified Access Gateway to Automatically Apply Authorized OS Updates

Occasionally, VMware might authorize the update of one or more OS packages to rectify a critical vulnerability that affects a specific version of Unified Access Gateway and for which no viable workaround is available.

You can configure the Unified Access Gateway to automatically fetch and apply any available authorized Photon OS package to the Unified Access Gateway version which has been deployed in your environment. These updates are then fetched and applied automatically when the appliance is next booted.

In earlier versions, such critical updates were performed manually using the `tdnf` command based on the guidance provided by VMware Global Support Services.

In the **Appliance Updates Settings** section, you can select the frequency of applying updates such as on next reboot or every reboot of the Unified Access Gateway appliance.

Note Updates are applied to the Unified Access Gateway appliance only during the boot cycles after configuring the desired updates scheme on this page.

Procedure

1 Log in to the Admin UI and in the **Configure Manually** section, click **Select**.

2 Go to **Advanced Settings > Appliance Updates Settings** and click the gear box icon.

3 In the **Appliance Updates Settings** window, enter the following information:

Configuration Setting	Action
Apply Updates Scheme	Select the frequency at which the Photon OS and Unified Access Gateway updates can be fetched and applied to Unified Access Gateway. By default, the updates scheme is `Don't apply updates`. **Important** If you select the `Apply updates on next boot` scheme, then after the updates are applied at the next immediate reboot of Unified Access Gateway, the scheme is automatically set back to the default value.
OS Updates URL	Enter the location of the repository from which the Photon OS packages are fetched and applied to the Unified Access Gateway appliance. By default, the value of this text box is `https://packages.vmware.com/photon`. You can either use the default value or provide a URL to your custom repository by mirroring the default VMware repository. The files in a mirrored repository must not be changed. The value of this text box must be an absolute URL, which can either be an IP address or hostname prefixed with `https`. **Note** If you provide your custom URL for OS updates, the settings get applied after a maximum of one minute.

Configuration Setting	Action
Appliance Updates URL	Enter the location of the repository from which the Unified Access Gateway authorized OS packages list is fetched and applied to the Unified Access Gateway appliance. By default, the value of this text box is `https://packages.vmware.com/uag`. You can either use the default value or provide a URL to your custom repository by mirroring the default VMware repository. These files in a mirrored repository must not be changed. The value of this text box must be an absolute URL, which can either be an IP address or hostname prefixed with `https`. **Note** If you provide your custom URL for appliance updates, the settings get applied after a maximum of one minute.
Trusted Certificates	**Note** Normally, it is not necessary to specify the trusted certificates because https://packages.vmware.com uses a trusted certificate. This setting is only required if you are connecting to a local repository that does not use a certificate issued by a trusted CA. ■ To select a certificate in PEM format and add to the trust store, click **+** . ■ To provide a different name, edit the alias text box. By default, the alias name is the filename of the PEM certificate. ■ To remove a certificate from the trust store, click **-**.

4 Click **Save**.

Results

After the updates are applied, the Unified Access Gateway appliance gets rebooted and a `package-updates.log` file is generated. This log file is available in the `UAG-log-archive.zip`. You can use the `package-updates.log` file for checking the status of the update and troubleshooting purpose.

For information about accessing `UAG-log-archive.zip` from the Admin UI, see Collecting Logs from the Unified Access Gateway Appliance.

Update TLS Server Signed Certificates

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

By default, Unified Access Gateway uses a self-signed TLS server certificate. For production environments, VMware strongly recommends that you replace the default self-signed certificate with a trusted CA signed certificate for your environment.

Note the following considerations when you upload a certificate:

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

- When you upload a CA-signed certificate on the admin interface, the TLS 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.

  Note With PowerShell deployment of Unified Access Gateway the TLS server certificate can be specified. It is not necessary to replace it manually.

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 **Configure Manually** section of the Unified Access Gateway admin UI, click **Select**.
2. In the **Advanced Settings** section, click the **TLS 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.

Using PowerShell to Deploy Unified Access Gateway

3

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

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

Read the following topics next:

- System Requirements to Deploy Unified Access Gateway Using PowerShell
- Using PowerShell to Deploy the Unified Access Gateway Appliance
- PowerShell Parameters for Deploying Unified Access Gateway

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.

- PowerShell script runs on Windows 8.1 or later machines or Windows Server 2008 R2 or later.
- VMware vSphere ESXi host with a vCenter Server.
- 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/.
- Microsoft Hyper-V

  Note For more information see, VMware Workspace ONE UEM documentation.
- Microsoft Azure

  Note For more information see, Unified Access Gateway PowerShell Deployment to Microsoft Azure.

- Amazon AWS EC2

  Note For more information see, Unified Access Gateway PowerShell Deployment to Amazon Web Services.

You must select the vSphere data store and the network to use.

Using PowerShell to Deploy the Unified Access Gateway Appliance

PowerShell scripts prepare your 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. 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.

You can include the parameters in the INI file for creating low-priviledged admin users with monitoring roles. Creating superuser admin user is not supported. You can configure the password policies for the root user and admin user before deploying the Unified Access Gateway instance.

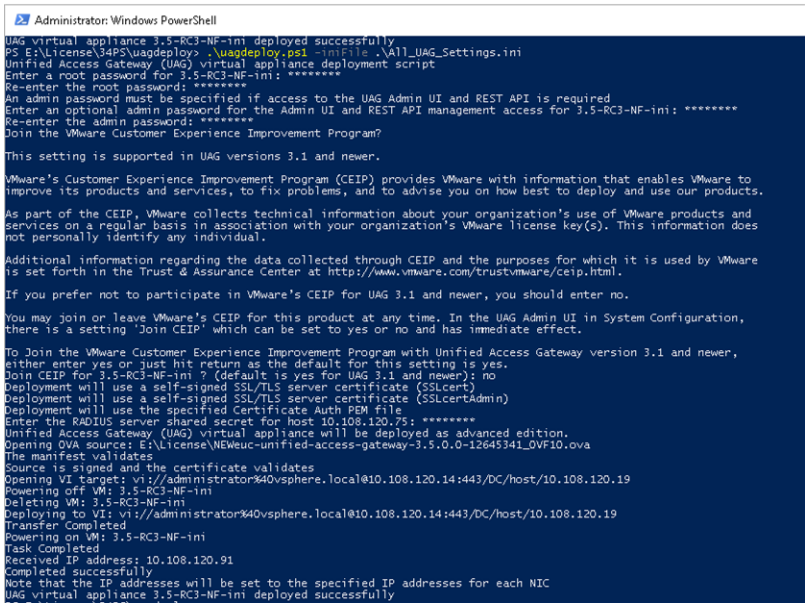
For more information about the parameters, you can see the section in which the equivalent admin UI parameter is used. For example: some of the deployment parameters are described in PowerShell Parameters for Deploying Unified Access Gateway and Deploy Unified Access Gateway Using the OVF Template Wizard, for information about parameters used in system configuration, syslog server settings, network settings, and so on, see Configuring Unified Access Gateway From the Admin Configuration Pages, and for information about parameters used in edge services and other use cases of Unified Access Gateway such as Workspace ONE Intelligence and Identify Bridging, see Chapter 4 Deployment Use Cases for Unified Access Gateway.

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 the VMware Download page for Unified Access Gateway.

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 *UAG1*. The configuration file is named *uag1.ini*. This file contains all the configuration settings for UAG1. You can use the sample `INI` files in the `uagdeploy.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.
- To convert the private key from PKCS8 to PKCS1, thats is, from the BEGIN PRIVATE KEY format to BEGIN RSA PRIVATE KEY format, run the following openssl command:

  ```
  openssl rsa -in key.pem -out keyrsa.pem
  ```

  To convert PKCS#12 format file with either a .p12 or .pfx file extension and to ensure the key is an RSA key, run the following commands:

  ```
  openssl pkcs12 -in cert.pfx -nokeys -out cert.pem
  ```

  ```
  openssl pkcs12 -in cert.pfx -nodes -nocerts -out key.pem
  ```

  ```
  openssl rsa -in key.pem -check -out keyrsa.pem
  ```

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=
deploymentOption=threenic
eth0CustomConfig=DHCP^UseDNS=false
eth1CustomConfig=DHCP^UseDNS=false
eth2CustomConfig=DHCP^UseDNS=false
authenticationTimeout=300000
fipsEnabled=false
sysLogType=TCP
uagName=UAG1
locale=en_US
ipModeforNIC3=DHCPV4_DHCPV6
tls12Enabled=true
```

```
ipMode=DHCPV4_DHCPV6
requestTimeoutMsec=10000
ipModeforNIC2=DHCPV4_DHCPV6
tls11Enabled=false
clientConnectionIdleTimeout=180
tls10Enabled=false
adminCertRolledBack=false
cookiesToBeCached=none
healthCheckUrl=/favicon.ico
quiesceMode=false
syslogUrl=10.108.120.108:514
syslogSystemMessagesEnabled=false
isCiphersSetByUser=false
tlsPortSharingEnabled=true
ceipEnabled=true
bodyReceiveTimeoutMsec=15000
monitorInterval=60
cipherSuites=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TL
S_ECDHE_RSA_WITH_AES_128_CBC_SHA256
, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
outboundCipherSuites=
adminPasswordExpirationDays=90
monitoringUsersPasswordExpirationDays=90
rootSessionIdleTimeoutSeconds=300
rootPasswordExpirationDays=365
passwordPolicyMinLen=6
passwordPolicyMinClass=1
passwordPolicyUnlockTime=900
passwordPolicyFailedLockout=3
adminPasswordPolicyFailedLockoutCount=3
adminPasswordPolicyMinLen=8
adminPasswordPolicyUnlockTime=5
adminSessionIdleTimeoutMinutes=10
httpConnectionTimeout=120
isTLS11SetByUser=false
sessionTimeout=36000000
ssl30Enabled=false
snmpEnabled= TRUE | FALSE
ntpServers=ipOrHostname1 ipOrHostname2
fallBackNtpServers=ipOrHostname1 ipOrHostname2
sshEnabled=
sshPasswordAccessEnabled=
sshKeyAccessEnabled=
sshPublicKey1=
adminDisclaimerText=
sshLoginBannerText=VMware EUC Unified Access Gateway
secureRandomSource=
hostClockSyncEnabled=false
extendedServerCertValidationEnabled=false
sslprovider=
tlsNamedGroups=
tlsSignatureSchemes=
osLoginUsername=
adminMaxConcurrentSessions=5
osMaxLoginLimit=10
```

```
dsComplianceOS=false
sshPort=22
sshInterface=eth0

[WorkspaceOneIntelligenceSettings1]
encodedCredentialsFile=
name=TEST1
trustedCert1=
urlThumbprints=bed22939bf8546d15de2136f4c33f48f31d44e71

[WorkspaceOneIntelligenceSettings2]
encodedCredentialsFile=
name=RISK_SCORE

[SnmpSettings]
version= v3
usmUser= SAM_SNMP_V3
securityLevel=
authAlgorithm=
authPassword=
privacyAlgorithm=
privacyPassword=
engineID=uag1.example.com

[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]
endpointComplianceCheckProvider=Workspace_ONE_Intelligence_Risk_Score
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
complianceCheckOnAuthentication=true
proxyDestinationUrlThumbprints=
proxyDestinationPreLoginMessageEnabled=true

[Airwatch]
tunnelGatewayEnabled=true
tunnelProxyEnabled=true
pacFilePath=
```

```
pacFileURL=
credentialFilePath=
apiServerUsername=domain\apiusername
apiServerPassword=*****
proxyDestinationUrl=https://null
ntlmAuthentication=false
healthCheckUrl=/favicon.ico
organizationGroupCode=
apiServerUrl=https://null
airwatchOutboundProxy=false
outboundProxyHost=1.2.3.4
outboundProxyPort=3128
outboundProxyUsername=proxyuser
outboundProxyPassword=****
reinitializeGatewayProcess=false
airwatchServerHostname=tunnel.acme.com
trustedCert1=c:\temp\CA-Cert-A.pem
hostEntry1=1.3.5.7 backend.acme.com

[AirwatchSecureEmailGateway]
airwatchOutboundProxy=false
memConfigurationId=abc123
apiServerUsername=domain\apiusername
healthCheckUrl=/favicon.ico
apiServerUrl=https://null
outboundProxyHost=1.2.3.4
outboundProxyPort=3128
outboundProxyUsername=proxyuser
outboundProxyPassword=****
reinitializeGatewayProcess=false
airwatchServerHostname=serverNameForSNI
apiServerPassword=****
trustedCert1=c:\temp\CA-Cert-A.pem
pfxCerts=C:\Users\admin\My Certs\mycacerts.pfx
hostEntry1=1.3.5.7 exchange.acme.com

[AirWatchContentGateway]
cgConfigId=abc123
apiServerUrl=https://null
apiServerUsername=domain\apiusername
apiServerPassword=*****
outboundProxyHost=
outboundProxyPort=
outboundProxyUsername=proxyuser
outboundProxyPassword=*****
airwatchOutboundProxy=false
hostEntry1=192.168.1.1 cgbackend.acme.com
trustedCert1=c:\temp\CA-Cert-A.pem
ntlmAuthentication=false
reinitializeGatewayProcess=false
airwatchServerHostname=cg.acme.com

[SSLCert]
pemPrivKey=
pemCerts=
```

```
pfxCerts=
pfxCertAlias=

[SSLCertAdmin]
pemPrivKey=
pemCerts=
pfxCerts=
pfxCertAlias=

[WorkspaceONEIntelligenceRiskScoreEndpointComplianceCheckSettings]
allowLow=true
allowMedium=true
allowHigh=true
complianceCheckInterval=5
allowOthers=false
name=Workspace_ONE_Intelligence_Risk_Score
workspaceOneIntelligenceSettingsName=RISK_SCORE

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

[JWTSettings2]
publicKey1=
publicKey2=
name=JWT_2

[AdminUser1]
name=monitoringUser1
enabled=true

[AdminUser2]
name=monitoringUser2
enabled=true

[OutboundProxySettings1]
proxyUrl=
name=
proxyType=HTTP
includedHosts1=
includedHosts2=
trustedCert1=

[OutboundProxySettings2]
proxyUrl=
name=
proxyType=HTTP
includedHosts1=
includedHosts2=
trustedCert1=

[adminSAMLSettings]
enable=true
```

```
entityId=https://www.entityid.com

[OPSWATEndpointComplianceCheckSettings]
allowInCompliance=
allowEndpointUnknown=
complianceCheckFastInterval=
complianceCheckInitialDelay=
complianceCheckInterval=
allowNotInCompliance=
allowOutOfLicenseUsage=
allowAssessmentPending=
allowOthers=
hostName=
name=
clientSecret=
clientKey=

[PackageUpdates]
packageUpdatesScheme=OFF|ON_NEXT_BOOT|ON_EVERY_BOOT
packageUpdatesOSURL=
packageUpdatesURL=
trustedCert1=
```

Note

- The `[adminSAMLSettings]` included in the INI file is for configuring the SAML authentication method used to authenticate the users with administrator access to the admin UI. Here, `entityId` refers to the external metadata provider entity id.
- Passwords for the low-privileged admin users with monitoring roles are provided as parameter to the PowerShell script. If the password is not provided, then the user is prompted to enter the password. Provide the parameter as `newAdminUserPwd` and the parameter value similar to `monitoringUser1:P@ssw0rd1;monitoringUser2:P@ssw0rd2`. The `enabled` parameter in the INI file is optional and defaults to true if the parameter is unavailable.

5 To make sure that the script execution is not restricted., type the PowerShell `set-executionpolicy` command.

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

You only need to do this once to remove the restriction.

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.

PowerShell Parameters for Deploying Unified Access Gateway

Unified Access Gateway can be deployed either by using the vSphere Web Client or PowerShell scripts. In either method, you must configure some parameters for the deployment. The information provided here helps you understand some of the configuration parameters that are used during the PowerShell deployment.

Configuration Parameter	Description
`osLoginUsername`	This setting is present in the [General] section of the `.ini` file. Enter a customized username of the high privilege user during Unified Access Gateway deployment. Maximum length of the username is `32` characters and can be a combination of `a-z`, `0-9`, underscore _ and, hyphen -. When this user is configured, the root login is deactivated.
osMaxLoginLimit	This setting is present in the [General] section of the `.ini` file. Allows you to configure the limit on concurrent logins of Unified Access Gateway local console using high privileged non-root user. The default value is `10`. **Note** This configuration is effective only when non-root user (osLoginUsername) is configured for Unified Access Gateway local console login. There is no limit on the concurrent logins of root user.
`sshEnabled`	This setting is present in the [General] section of the `.ini` file. When set to `true`, this parameter automatically enables SSH access on the deployed appliance. When sent to `false`, SSH is not enabled. **Note** VMware does not generally recommend enabling SSH on Unified Access Gateway except in certain specific situations and where access can be restricted. If root console access is required for Amazon AWS EC2 deployments, SSH can be enabled. For more information on Amazon AWS EC2, see *Unified Access Gateway PowerShell Deployment to Amazon Web Services* at VMware Docs. Enabling SSH access on Unified Access Gateway deployments for vSphere, Hyper-V, or Microsoft Azure is not generally required as console access with those platforms can be used. 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.
`sshPort`	This setting is present in the [General] section of the `.ini` file. Configure the port on which SSH is enabled. The default value is `22`.

Configuration Parameter	Description
sshInterface	This setting is present in the [General] section of the .ini file. Configure the network interface on which SSH login is enabled. By default, SSH is enabled on all the interfaces. The supported values are eth0, eth1, and eth2 based on the configuration.
syslogType	Enables syslog configuration.
Custom configuration setting	The custom configuration values that must be added to the systemd.network files can be provided in the following format: SectionName^Parameter=Value. An example of a custom configuration entry is DHCP^UseDNS=false. This value, when used, disables the usage of DNS IP addresses provided by the DHCP server. Using the same format, you can add multiple such systemd.network configuration entries separated by semi-colons. Example of custom configuration values for the eth (0,1, and 2) is included in the General section of the sample .ini file.
rootSessionIdleTimeoutSeconds	Duration (in seconds) for which the Unified Access Gateway console session has been idle. After this timeout, the console logs out automatically. Default value of this parameter when logging into Unified Access Gateway using SSH on Microsoft Azure is 180 seconds, and 300 seconds for other platforms. For Serial console session, the default value is 900 seconds. The maximum value of this parameter is 3600 seconds.
rootPasswordExpirationDays	Password expiration policy for the root users. The default password expiration time is 365 days. To prevent password expiry, the expiration time can be set to 0.
passwordPolicyMinLen	Minimum length of the root user password. The default value of this parameter is 6. The maximum value of this parameter is 64.
passwordPolicyMinClass	Minimum number of classes of character types that can be used to configure the root password complexity. The classes of character types are as follows: uppercase, lowercase, digits, and others. The default value is 1. This parameter can be configured with the following values: 1, 2, 3, and 4. If the parameter has the default value, then you can use characters from all the four classes. If the parameter value is 1, then you can use characters from any one of the classes.

Configuration Parameter	Description
passwordPolicyFailedLockout	Number of failed login attempts allowed for the root user to access the Unified Access Gateway console. The default value is 3.
passwordPolicyUnlockTime	Duration for which the Unified Access Gateway console is locked out after the configured number of failed login attempts by the root user. After the lockout, the Unified Access Gateway console is unlocked and the root user can access the console. The default value is 900 seconds.
adminpasswordPolicyMinLen	Minimum length of the admin user password. The default value of this parameter is 8. The maximum value of this parameter is 64.
adminpasswordPolicyFailedLockoutCount	Number of failed login attempts allowed for the admin user to access the Unified Access Gateway admin UI. The default value is 3.
adminpasswordPolicyUnlockTime	Duration (in minutes) for which the Unified Access Gateway admin UI is locked out after the configured number of failed login attempts by the admin user. After the lockout, the Unified Access Gateway admin UI is unlocked and the admin user can access the UI. The default value is 5 minutes.
adminSessionIdleTimeoutMinutes	Duration (in minutes) for which the Unified Access Gateway admin UI session has been idle. After this timeout, the admin UI logs out automatically. The default value is 10 minutes. The maximum value is 1440 minutes. If the parameter value is 0, the session does not expire even though in idle state.
adminMaxConcurrentSessions	This setting is present in the [General] section of the .ini file. Allows you to configure limit on concurrent admin sessions. The default value is 5. The supported range is 1-50. When this value is set to 1, no concurrent sessions are allowed. If you want to create a new session when the number of concurrent sessions already hit the limit, the system will invalidate the least recently used session.

Configuration Parameter	Description
`sshLoginBannerText`	Option to customize the banner text displayed when logging into Unified Access Gateway using SSH or the vSphere Client's Web Console. This option can be configured only at the time of deployment. If you do not configure this parameter, the default text displayed is *VMware EUC Unified Access Gateway*. Only ASCII characters are supported in the customized text. For multi-line banner texts, `\n` must be used as the line separator.
`secureRandomSource`	Allows you to configure the secure random bit generator source used by Java processes for cryptographic functions. This option can be configured only at the time of deployment. Supported values are: `/dev/random` and `/dev/urandom`. By default, `/dev/random` is used in the non-FIPS mode and `/dev/urandom` is used in the FIPS mode.
`dsComplianceOS`	This setting is present in the [General] section of the `.ini` file. Default value is `false`. When set to `true`, this Boolean flag sets the OS configuration to comply with the current Photon OS 3.0 DISA STIG Readiness Guide. The password complexity and other STIG requirements are automatically configured. **Note** This setting must be used with the FIPS version when DISA STIG OS compliance is required.

Deployment Use Cases for Unified Access Gateway

4

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

You can deploy Unified Access Gateway with Horizon, Horizon Cloud with On-Premises Infrastructure, Workspace ONE Access, and Workspace ONE UEM.

Read the following topics next:

- 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
- Configuring Horizon for Unified Access Gateway and Third-Party Identity Provider Integration
- Workspace ONE UEM Components on Unified Access Gateway
- Additional Deployment Use Cases
- Configure Workspace ONE Intelligence Connection Settings
- Select the Workspace ONE Intelligence Data Setting

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

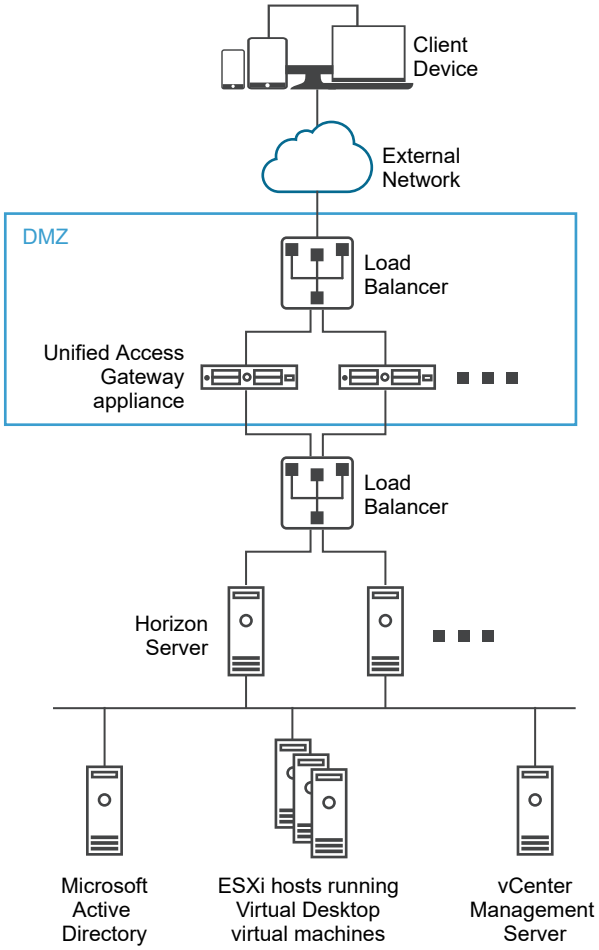
Unified Access Gateway provides secure remote access to On-Premises virtual desktops and applications in a customer data center. This operates with an On-Premises deployment of Horizon or Horizon Air for unified management.

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. See Unified Access Gateway 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.

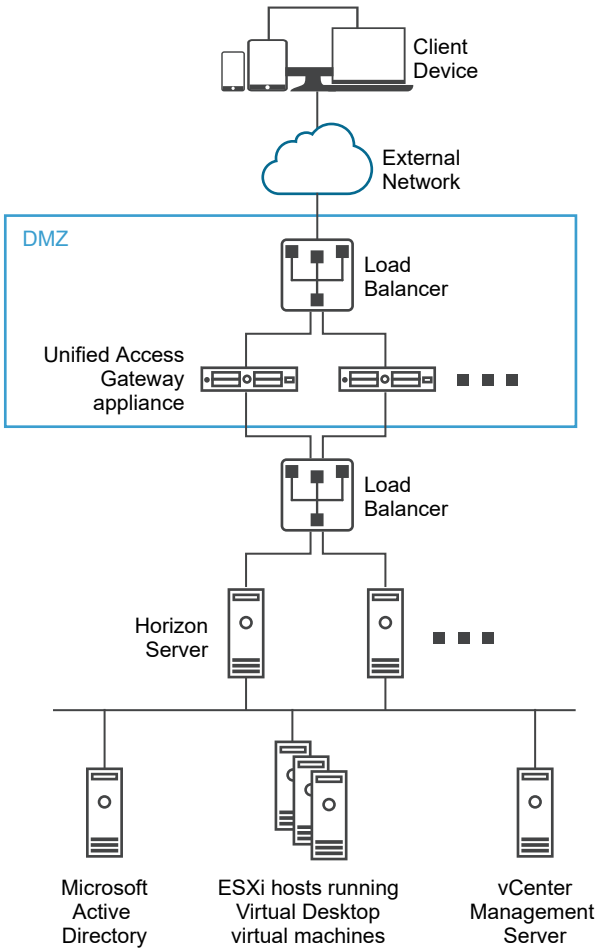
It is recommended that users deploying Horizon 7 use Unified Access Gateway appliance instead of Horizon security server.

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.

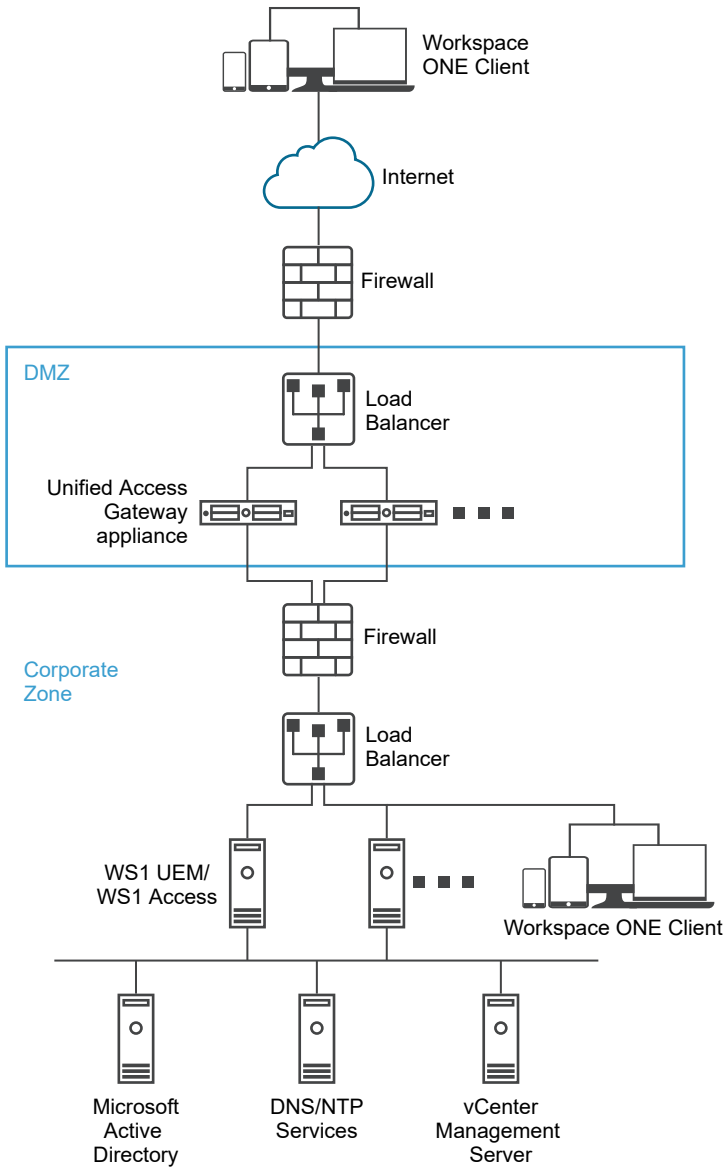
- Secure deployment. Unified Access Gateway is implemented as a hardened, locked-down, preconfigured Linux-based virtual machine.
- Scalable. You can connect Unified Access Gateway to an individual Horizon Connection Server, or you can connect it through a load balancer in front of multiple Horizon Connection 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.

Unified Access Gateway Support for IPv4 and IPv6 Dual Mode for Horizon Infrastructure

You can use Unified Access Gateway to act as a bridge for Horizon Clients to connect to a back-end Horizon Connection Server or agent environment. In this scenario, Horizon Client and the Horizon Connection Server can be configured with different IP modes: IPv4 or IPv6 and conversely.

The Horizon back-end environment might consist of Connection Servers, agent desktops, or other server-side infrastructure.

IP Mode Combinations for Horizon Infrastructure

Horizon Client and Horizon Connection Server can have the following IP modes in the Horizon infrastructure:

Horizon Client	Horizon Connection Server	Supported
IPv4	IPv4	Yes
IPv6	IPv4	Yes
IPv6	IPv6	Yes
IPv4	IPv6	Yes

Note When Horizon Client and Horizon Connection Server are configured with different IP modes (IPv4 or IPv6 and conversely), the **Connection Server IP mode**, a setting in the Unified Access Gateway Admin UI, can have one of the following values: same IP mode as the Horizon Connection Server or mixed mode `(IPv4+IPv6)`.

For example: Horizon Client is configured with IPv4 and Horizon Connection Server is configured with IPv6, then the **Connection Server IP mode** can have either `IPv6` or `IPv4+IPv6` (mixed mode) values.

For more information about the **Connection Server IP mode** setting, see Configure Horizon Settings.

When the IP mode is bridged (IPv4 to IPv6 or IPv6 to IPv4), Unified Access Gateway does not support the following: Horizon Tunnel, PCoIP, or Blast UDP.

Note The Blast External URL must be configured to use TCP port 443 or 8443.

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 Workspace ONE Access. 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 Workspace ONE Access 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.

Note The pattern can also be used to exclude certain URLs. For example, to allow all URLs through but block /admin you can use the following expression. `^/(?!admin(.*))(.*)`

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 Workspace ONE Access 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 Workspace ONE Access 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 Workspace ONE Access to prevent the overlap.

Retaining the '/' proxy pattern in the web reverse proxy instance (Workspace ONE Access) ensures that when a user clicks the URL of Unified Access Gateway, the Workspace ONE Access 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 Workspace ONE Access 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 Workspace ONE Access 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, turn on the **Enable Horizon** toggle to enable Horizon settings.

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	**Note** You must specify a thumbprint only if the connection server SSL server certificate is not issued by a trusted CA. For example, a self-signed certificate or a certificate issued by an internal CA. Enter the list of Horizon server thumbprints in hexadecimal digits format. A thumbprint is of the format `[alg=]xx:xx...` where `alg` can be sha1 (default value), sha256, sha384, and sha512 or md5 and the `xx` are hexadecimal digits. Hash algorithm must meet the requirements specified for the minimum hash size. If multiple thumbprints are added, then it should be comma separated. The separator can be a space, colon (:), or no separator. For example, sha1=C3 89 A2 19 DC 7A 48 2B 85 1C 81 EC 5E 8F 6A 3C 33 F2 95 C3, sha256=ad:5c:f1:48:47:94:7e:80:82:73:13:6c:83:52:b:e:78:ed:ff:50:23:56:a8:42:8a:d9:30:fc:3a:33:d6:c6:db, sha512=2221B24DC78018A8FAFF81B7AD348722390793DE8C0E5E5AA1D622BCC951D4DA5DBB1C76C79A258A7AFBD1727447151C90E1733E7E83A7D1D46ADF1A31C78496. Certificate thumbprints can be configured for certificate validation for the server certificate returned in communication between Unified Access Gateway and Horizon Connection Server. This option can be configured during PowerShell deployment by adding the `proxyDestinationUrlThumbprints` parameter in the [Horizon] section in the `ini` file. See Using PowerShell to Deploy the Unified Access Gateway Appliance.
Enable PCOIP	Turn on this toggle to specify whether the PCoIP Secure Gateway is enabled.
Disable PCOIP Legacy Certificate	Turn on this toggle to use the uploaded SSL server certificate instead of Legacy certificate. Legacy PCoIP clients will not work if this toggle is turned on.
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	Turn on this toggle to use the Blast Secure Gateway.
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.

Option	Description
Connection Server IP mode	Indicates the IP mode of a Horizon Connection Server. This field can have the following values: `IPv4`, `IPv6`, and `IPv4+IPv6`. Default is `IPv4`. ■ If all NICs in the Unified Access Gateway appliance are in IPv4 mode (no IPv6 mode), then this field can have one of the following values: `IPv4` or `IPv4+IPv6` (mixed mode). ■ If all NICs in the Unified Access Gateway appliance are in IPv6 mode (no IPv4 mode), then this field can have one of the following values: `IPv6` or `IPv4+IPv6` (mixed mode).
Client Encryption Mode	Indicates the mode of encryption for communications between Horizon Client, Unified Access Gateway, and Horizon Connection Server. The values for this option are `DISABLED`, `ALLOWED`, and `REQUIRED`. The default value is `ALLOWED`. ■ `DISABLED` - `Client Encryption Mode` option is disabled. When disabled, the existing behavior continues. In Unified Access Gateway versions earlier than 2111, non-encrypted communication is allowed between Horizon Client, Unified Access Gateway, and Horizon Connection Server. ■ `ALLOWED` - With Horizon Client 2111 or later, Unified Access Gateway allows only encrypted communication with Horizon Client and Horizon Connection Server. With earlier versions of Horizon Client, non-encrypted communication is allowed. This behavior is similar to when the feature is disabled. ■ `REQUIRED` - Only encrypted communication is allowed between the three components. **Note** If an earlier version of Horizon Client is used in this encrypted mode, then the non-encrypted communication fails and the end user is unable to launch the Horizon desktops and applications.
Re-Write Origin Header	If an incoming request to Unified Access Gateway has the `Origin` header and the **Re-Write Origin Header** toggle is turned on, Unified Access Gateway rewrites the `Origin` header with the **Connection Server URL**. The **Re-Write Origin Header** toggle works alongside the `checkOrigin` CORS property of the Horizon Connection Server. When this field is enabled, the Horizon administrator can bypass the need to specify Unified Access Gateway IP addresses in the `locked.properties` file. For information about Origin Checking, see *Horizon Security* documentation.

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

Option	Description
Auth Methods	The default is to use pass-through authentication of the user name and password. The following authentication methods are supported: `Passthrough`, `SAML`, `SAML and Passthrough`, `SAML and Unauthenticated`, `SecurID`, `SecurID and Unauthenticated`, `X.509 Certificate`, `X.509 Certificate and Passthrough`, `Device X.509 Certificate and Passthrough`, `RADIUS`, `RADIUS and Unauthenticated`, and `X.509 Certificate or RADIUS`. **Important** If you have chosen any of the `Unauthenticated` methods as the auth method, ensure that you configure the **Login Deceleration Level** in the Horizon Connection Server to `Low`. This configuration is necessary to avoid long delay in login time for endpoints while accessing the remote desktop or application. For more information about how to configure **Login Deceleration Level**, see the *Horizon Administration* documentation at VMware Docs.
Enable Windows SSO	This toggle can be used when **Auth Methods** is set to RADIUS and when the RADIUS passcode is the same as the Windows domain password. Turn on this toggle to use the RADIUS username and passcode for the Windows domain login credentials to avoid the need to prompt the user again. If Horizon is setup on a multi domain environment, if the user name provided does not contain a domain name, then the domain will not be sent to CS. If NameID suffix is configured and if the user name provided does not contain a domain name, then the configure NameID suffix value will be appended to the username. For example, if a user provided jdoe as the username and NameIDSuffix is set to `@north.int`, the Username sent is `jdoe@north.int`. If NameID suffix is configured and if username provided is in UPN format, NameID suffix will be ignored. For example, if a user provided `jdoe@north.int`, NameIDSuffix - `@south.int`, the Username is `jdoe@north.int` If the username provided is in the format `<DomainName\username>`, for example, `NORTH\jdoe`, Unified Access Gateway sends the username and domain name separately to CS.
RADIUS Class Attributes	This field 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.
Disclaimer Text	The Horizon disclaimer message that is displayed to the user and accepted by the user in cases where **Auth Method** is configured.
Smart Card Hint Prompt	Turn on this toggle to enable password hint for certificate authentication.
Health Check URI Path	The URI path for the connection server that Unified Access Gateway connects to, for health status monitoring.

Option	Description
Enable UDP Server	Connections are established through the UDP Tunnel server if there is a poor network. When the Horizon Client sends requests through the UDP, Unified Access Gateway receives the source IP address of these requests as `127.0.0.1`. Unified Access Gateway sends the same source IP address to the Horizon Connection Server. To ensure that the Connection Server receives the actual source IP address of the request, you must disable this option (**Enable UDP Server**) in the Unified Access Gateway admin UI.
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.
Blast Allowed Host Header Values	Enter an IP address or a host name By specifying a host header value, BSG (Blast Secure Gateway) allows only those requests that contain the specified host header value. A list of comma-separated values in the `host[:port]` format can be specified. The value can be an IP address, host name, or an FQDN name. The host header in the incoming Blast TCP port 8443 connection request to Blast Secure Gateway must match one of the values provided in the field. To allow a request that has no host name or IP address in the host header, use `_empty_`. If no value is specified, then any host header sent by the Horizon Client is accepted.
Enable Tunnel	If the Horizon secure tunnel is used, turn on this toggle. 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.

Option	Description
Endpoint Compliance Check Provider	Select the endpoint compliance check provider. Default is `None`. **Note** Only when the compliance check provider settings are configured in the admin UI, you can see the options available for selection. For more information about the endpoint compliance check providers and their configuration, see Endpoint Compliance Checks for Horizon.
Compliance Check on Authentication	Option to disable or enable the endpoint compliance check at user authentication. Compliance is always checked when a user starts a desktop or application session. When this option is enabled, compliance is also checked after the user authenticates successfully. If this option is enabled and the compliance check fails at authentication time, then the user session does not continue. If the option is disabled, Unified Access Gateway only checks compliance when a user starts a desktop or application session. This option is available only when an endpoint compliance check provider is selected. By default, this option is enabled. **Attention** If you have configured the **Compliance Check Initial Delay** option on the **Endpoint Compliance Check Provider Settings** page, **Compliance Check on Authentication** is automatically disabled. Unified Access Gateway does not check compliance on authentication. For more information about the time interval and the behavior of Unified Access Gateway when this time interval is configured, see Time Interval for Delaying Compliance Check. This option is also present as a parameter in the [Horizon] section in the `.ini` file and can be configured during deployment using PowerShell. For the parameter name, see Using PowerShell to Deploy the Unified Access Gateway Appliance.
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(.*))`. **Note** The pattern can also be used to exclude certain URLs. For example, to allow all URLs through but block /admin you can use the following expression.`^/(?!admin(.*))(.*)`
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.
Enable Proxy Pattern Canonical Match	Turn on this toggle to enable Horizon canonical match. Unified Access Gateway performs the equivalent of `C RealPath()` to normalize the URL converting character sequences such as `%2E` and removing the `..` sequences to create an absolute path. Proxy pattern check is then applied on absolute path. By default, this toggle is turned on for Horizon edge services. **Note** By default, this toggle is turned off for Web Reverse Proxy services.

Option	Description
Logout on Certificate Removal	**Note** This option is available when any of the smart card authentication methods is selected as an **Auth Method**. If this toggle is turned on and the smart card is removed, the end user is forced to log out from an Unified Access Gateway session.
User name label for RADIUS	Enter text to customize the user name label in the Horizon client. For example, `Domain Username` RADIUS authentication method must be enabled. To enable RADIUS, see Configure RADIUS Authentication. The default label name is `Username`. Maximum length of label name is 20 characters.
Passcode label for RADIUS	Enter a name to customize the passcode label in the Horizon client. For example, `Password` RADIUS authentication method must be enabled. To enable RADIUS, see Configure RADIUS Authentication. The default label name is `Passcode`. Maximum length of label name is 20 characters.
Match Windows User Name	Turn on this toggle to match RSA SecurID and Windows user name. When turned on,*securID-auth* is set to true and the *securID* and Windows user name matching is enforced. If Horizon is setup on a multi domain environment, if the user name provided does not contain a domain name, then the domain will not be sent to CS. If NameID suffix is configured and if the user name provided does not contain a domain name, then the configure NameID suffix value will be appended to the username. For example, if a user provided `jdoe` as the username and NameIDSuffix is set to `@north.int`, Username sent would be `jdoe@north.int`. If NameID suffix is configured and if username provided is in UPN format, NameID suffix will be ignored. For example, if a user provided `jdoe@north.int`, NameIDSuffix - `@south.int`, Username would be `jdoe@north.int` If the username provided is in the format `<DomainName\username>`, for example, `NORTH\jdoe`, Unified Access Gateway sends the username and domain name separately to CS. **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.

Option	Description
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`. **Important** The location must be set to `Internal` when any of the following auth methods are selected: `SAML and Unauthenticated`, `SecurID and Unauthenticated`, or `RADIUS and Unauthenticated`.
Show Connection Server Pre-login message	Turn on this toggle to show to the user any connection server pre-login message configured on the connection server during XML-API primary protocol flows. By default, this toggle is turned on for Horizon edge services. When this toggle is turned off, the user does not see the pre-login message configured on connection server.
Trusted Certificates	■ To select a certificate in PEM format and add to the trust store, click **+**. ■ To provide a different name, edit the alias text box. By default, the alias name is the filename of the PEM certificate. ■ To remove a certificate from the trust store, click **-**.
Response Security Headers	To add a header, click **+**. Enter the name of the security header. Enter the value. To remove a header, click **-**. 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 Port Redirect Mappings	For information about how UAG supports the HTTP Host Redirect capability and certain considerations required for using this capability, see Unified Access Gateway Support for HTTP Host Redirect. **Note** Source Host and Redirect Host support optional port, separated by colon. The default port number is `443`. ■ **Source Host:Port** Enter the host name of the source (host header value). ■ **Redirect Host:Port** Enter the host name of the individual Unified Access Gateway appliance whose affinity must be maintained with the Horizon Client.
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**.

Option	Description
SAML Audiences	Ensure that either SAML or SAML and Passthrough authentication method is chosen. Enter the audience URL. **Note** If the text box is left empty, audiences are not restricted. To understand how Unified Access Gateway supports SAML Audiences, see SAML Audiences.
SAML Unauthenticated Username Attribute	Enter the custom attribute name **Note** This field is available only when the value of **Auth Methods** is `SAML and Unauthenticated`. When Unified Access Gateway validates the SAML assertion, if the attribute name specified in this field is present in the assertion, then Unified Access Gateway provides unauthenticated access to the user name configured for the attribute in the Identity Provider. For more information about the `SAML and Unauthenticated` method, see Authentication Methods for Unified Access Gateway and Third-Party Identity Provider Integration.
Default Unauthenticated Username	Enter the default user name that must be used for unauthenticated access This field is available in the Admin UI when one of the following **Auth Methods** is selected: `SAML and Unauthenticated`, `SecurID and Unauthenticated`, and `RADIUS and Unauthenticated`. **Note** For `SAML and Unauthenticated` authentication method, the default user name for unauthenticated access is used only when the **SAML Unauthenticated Username Attribute** field is empty or the attribute name specified in this field is missing in the SAML assertion.
Disable HTML Access	If this toggle is turned on, web access to Horizon is disabled. See Configure OPSWAT as the Endpoint Compliance Check Provider 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.

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

Unified Access Gateway Support for HTTP Host Redirect

The HTTP Host Redirect capability can be used to simplify Horizon load balancing affinity requirements in certain multi VIP environments. To use the HTTP Host Redirect capability, UAG administrators must configure the **Host Redirect Mappings** text box in Horizon Settings.

When an HTTP request reaches UAG with a load balancer's host name, UAG responds with a HTTP 307 redirect and replaces the load balancer's host name with the UAG's own configured host name. For subsequent requests, the Horizon client directly reconnects with the UAG. This ensures that the subsequent requests are not routed through the load balancer. The redirect capability avoids issues with affinity control on load balancers where the requests could get routed to the incorrect UAG.

For example, consider an environment with a load balancer and two UAG appliances, UAG1 and UAG2. If a request reaches UAG1 with the load balancer's host name as `load-balancer.example.com`, UAG1 responds with a `HTTP 307` redirect and replaces the load balancer's host name with the UAG's own configured host name, `uag1.example.com`. For subsequent requests, Horizon client directly reconnects with UAG1.

Considerations while using HTTP Host Redirect

You need to be aware of the following considerations while using the HTTP Host Redirect capability:

- `N + 1` Virtual IP address is required, where

  `N` - number of UAG appliances deployed in the environment

  `1` - VIP of the load balancer

- Load balancers that operate at Layer 7 cannot be used.

To configure the settings in Horizon, see Configure Horizon Settings

SAML Audiences

SAML Audiences is a feature supported by UAG (Unified Access Gateway) for Edge services such as Horizon and Web Reverse Proxy. By using the SAML Audiences feature, UAG administrators can restrict the audiences accessing Horizon clients and backend applications.

In the Horizon Edge service, both SAML and SAML and Passthrough authentication methods support SAML Audiences. In the Web Reverse Proxy Edge service, only when Identity Bridging is enabled, SAML authentication method supports SAML Audiences.

If **SAML Audiences** is configured with values, then UAG validates this list of values against the audiences received in SAML assertion. If there is at least one match, then the SAML assertion is accepted. If there is no match, UAG rejects the SAML assertion. If SAML Audiences is not configured, then UAG does not validate the audiences in the SAML assertion.

To restrict audiences for the Horizon Edge service, see Configure Horizon Settings. To restrict audiences for the Web Reverse Proxy Edge service, see Configure a Web Reverse Proxy for Identity Bridging (SAML to Kerberos).

DISA STIG OS Compliance Guidelines for Unified Access Gateway

Unified Access Gateway supports configuration settings to allow Unified Access Gateway to comply with the Photon 3 OS Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG).

This OS compliance requires specific configuration in the Unified Access Gateway appliance.

The configuration changes are listed as follows:

1 Deploy the FIPS version of Unified Access Gateway.

2 Configure the following parameters during deployment.

Note You can configure these parameters only at the time of deployment. If you do not configure during deployment, Unified Access Gateway includes the default values.

Parameter	Description
dsComplianceOS	Set to `true` to enable DISA STIG OS compliance settings.
rootPasswordExpirationDays	Number of days after which the root password must be mandatorily reset. Set the value to `90`.
passwordPolicyMinLen	Minimum length of the root password. Set the value to `8`.
passwordPolicyMinClass	Minimum complexity of the root password. Set the value to `4`.
sshEnabled	Set to `true` to automatically enable SSH access on the deployed appliance.
sshLoginBannerText	Set to an appropriate login banner that includes the text `You are accessing a U.S. Government System`.
rootSessionIdleTimeoutSeconds	Duration in seconds after which an idle session of the root user will expire. Set the value to `900`.
passwordPolicyFailedLockout	Number of failed login attempts after which admin user access is locked out temporarily. Set the value to `3`.
sshInterface	Set to `eth0`, `eth1` or `eth2` according to which Unified Access Gateway NIC SSH is accessed. For example, `sshInterface=eth0`.
sshPort	Set to an unused port value other than port 22. For example, `sshPort=30`.
syslogUrl	Set the syslog URL. For example, `syslog://mysyslog.example.int:514`.
ntpServers	Set the hostname(s) for NTP servers. For example, `mytimesvr1.example.int, mytimesvr1.example.int`.

FedRAMP Guidelines for Unified Access Gateway

The Federal Risk and Management Program (FedRAMP) is a cyber security risk management program for the use of cloud products and services used by U.S. federal agencies.

FedRAMP uses the National Institute of Standards and Technology's (NIST) guidelines and procedures to provide standardized security requirements for cloud services. In addition, FedRAMP leverages NIST's Special Publication [SP] 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations series, the baselines, and test cases.

VMware is seeking FedRAMP compliance and certification of Unified Access Gateway with Horizon on Azure GovCloud. This requires a specific configuration.

Pre-requisites

- Unified Access Gateway 2207 or later FIPS build artifact appliance image used for deployment.
- Package mirror repository in FedRAMP boundary to hold Photon OS packages with security updates for applying periodic security fixes on Unified Access Gateway appliance.
- Syslog server to forward audit events from Unified Access Gateway.
- NTP servers to configure time synchronization on Unified Access Gateway.
- Identity provider setup with SAML authentication support.
- VMware Horizon Cloud for Azure GovCloud.

Deploy the FIPS version of Unified Access Gateway 2207 or later on Azure GovCloud with the following configurations.

1 Configure OS hardening settings specified in the DISA STIG OS Compliance Guidelines for Unified Access Gateway.

2 Configure the following parameters based on the requirement.

Parameter	Description
sshKeyAccessEnabled	Set to `true` to enable the SSH access using keypair. The default value is `false`.
sshPublicKey1 (sshPublicKey2,..)	Configure the SSH public key used for SSH login, if SSH key based access is enabled.
osLoginUsername	Enter the high-privileged non-root username to login into Unified Access Gateway OS console. By default, root login is supported.
osMaxLoginLimit	Enter the maximum allowed concurrent login sessions of a non-root user, if configured.

3 Configure TLS server certificates for Unified Access Gateway with RSA key size of 2048 or higher. See the *[SSLCert]* section in the INI example at Using PowerShell to Deploy the Unified Access Gateway Appliance.

4 Configure automated package update settings to download and apply the security updates from the packages repository maintained within FedRAMP boundary. See Configure Unified Access Gateway to Automatically Apply Authorized OS Updates and *[PackageUpdates]* section in the INI example at Using PowerShell to Deploy the Unified Access Gateway Appliance.

5 Configure Horizon edge service with necessary Auth method settings, such as SAML. For more information, see Configuring Horizon for Unified Access Gateway and Third-Party Identity Provider Integration.

Blast TCP and UDP External URL Configuration Options

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

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

Table 4-1. BEAT Port Options

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

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

Endpoint Compliance Checks for Horizon

In addition to the other user authentication services that are available on the Unified Access Gateway appliance, the endpoint compliance checks feature provides an extra layer of security for accessing Horizon desktops. You can use this feature to ensure compliance to various policies such as an antivirus policy or encryption policy on endpoints.

Endpoint Compliance Checks are advanced settings, which can be configured on the **Endpoint Compliance Check Provider Settings** page. Administrators can use this page to configure the status codes of endpoint devices for which access must be denied or allowed. The settings page also has time interval text boxes, which can be used by the administrators to configure periodic compliance checking of an endpoint during an authenticated user session.

Endpoint compliance is checked after a user authenticates successfully, when a user attempts to start a remote desktop or application from the listed entitlements, and during an authenticated session.

After successful authentication if the endpoint device has a status for which the access is configured to be denied, then even though the user has authenticated successfully, the device is denied access. As a result, the user cannot start a remote desktop or application.

Endpoint compliance policy is defined on a service running in cloud or on-premises. The OPSWAT MetaAccess persistent agent or the OPSWAT MetaAccess on-demand agent are the OPSWAT agents on the Horizon Client that perform the endpoint compliance check. These agents communicate the compliance status to an OPSWAT instance running either in cloud or on-premises.

Configure Workspace ONE Intelligence (Risk Analytics) as the Endpoint Compliance Check Provider for Horizon

When `Workspace_ONE_Intelligence_Risk_Score` is configured as the endpoint compliance check provider on the **Horizon Settings** page, Unified Access Gateway performs a Horizon Client endpoint device check with Workspace ONE Intelligence's risk analytics feature. This check is performed so that end users with high risk score endpoints are denied access to Horizon desktops and applications.

The risk score compliance check feature is available for Workspace ONE UEM-registered devices running a Horizon Client version that passes the hashed value of the device serial number to Unified Access Gateway. These client devices provide information to Workspace ONE Intelligence to allow a risk score to be calculated.

For information about risk scores, see the *Risk Scoring* section in the *Workspace ONE Intelligence Products* documentation at VMware Docs.

Prerequisites

Ensure that you have configured the Workspace ONE Intelligence connection. For more information, see Configure Workspace ONE Intelligence Connection Settings.

Procedure

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

2 Click **Add**.

Note If you have already added `Workspace_ONE_Intelligence_Risk_Score` as the endpoint compliance check provider, you can either edit the settings by clicking the gearbox icon or add new provider settings by deleting the existing one.

3 Select `Workspace_ONE_Intelligence_Risk_Score` as the **Endpoint Compliance Check Provider**.

4 Select the Workspace ONE Intelligence connection setting.

5 Enter the **Compliance Check Interval (mins)** value.

- Valid values (in minutes) - `5` to `1440`
- Default value - `0`

  `0` indicates **Compliance Check Interval (mins)** is disabled.

For more information about periodic compliance checks and **Compliance Check Interval (mins)**, see Time Interval for Periodic Endpoint Compliance Checks.

6 To change the default value of the risk score severities and allow endpoints to access remote desktops and applications, click **Show Allowed Risk Score Severities**.

The following risk score severities are supported: `Low`, `Medium`, `High`, and `Others`.

By default, endpoint devices that have `Low` risk score are always allowed access.

7 If you want to allow devices that have a risk score other than the default value, click to change from **DENY** to **ALLOW**.

By default, endpoint devices with risk score severities other than `LOW` are denied.

8 Click **Save**.

What to do next

1 Navigate to Horizon settings, locate **Endpoint compliance check provider** text box, and select `Workspace_ONE_Intelligence_Risk_Score` from the drop-down menu.

2 Click **Save**.

Configure OPSWAT as the Endpoint Compliance Check Provider for Horizon

When you select OPSWAT as the endpoint compliance check provider, there are certain settings that must be configured for Unified Access Gateway to integrate with OPSWAT. For example, you can configure the time interval at which periodic compliance checks can occur, upload the on-demand agent executable file to Unified Access Gateway, and so on.

When OPSWAT is selected as the endpoint compliance check provider on the **Horizon Settings** page, Unified Access Gateway performs a Horizon Client endpoint device check with OPSWAT. This check is performed so that users with non-compliant endpoints are denied access to Horizon desktops and applications.

If you choose to use any of the time interval settings either for periodic compliance checking or for delaying the compliance check, see Time Interval for Periodic Endpoint Compliance Checks or Time Interval for Delaying Compliance Check respectively.

You can configure the endpoint compliance check provider settings for OPSWAT using PowerShell. For information about the PowerShell parameters, see Using PowerShell to Deploy the Unified Access Gateway Appliance.

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.

Procedure

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

2 Click **Add**.

3 Select `OPSWAT` as the **Endpoint Compliance Check Provider**.

4 Enter **Client Key** and **Client Secret**.

5 Enter the **Hostname** of the compliance check provider.

6 Enter the **Connectivity Check Interval** to check if the compliance server (OPSWAT) is available.

- Valid values (in minutes) - `1` to `120`
- Default value - `0`

  `0` indicates that the connectivity check is deactivated.

If there is a connectivity check failure during test call, an error message is logged on the esmanager logs. The event is sent to the syslog server.

7 Enter the **Compliance Check Interval Timeunit**.

The supported time units for the Endpoint Compliance Check Provider time interval settings are in `minutes` and `seconds`.

8 If you want to delay the first compliance check after successful user authentication, enter the **Compliance Check Initial Delay** time interval.

- Valid values (in minutes) - `1` to `60`
- Valid values (in seconds) - `5` to `3600`
- Default value - `0`

  `0` indicates that the Compliance Check Initial Delay is deactivated.

Note If this time interval is configured, the Horizon setting, `Compliance Check on Authentication` is automatically disabled.Unified Access Gateway does not check compliance on authentication. For more information about this setting, see Configure Horizon Settings.

9 Enter the desired value in **Compliance Check Interval**.

- Valid values (in minutes) - `5` to `1440`
- Valid values (in seconds) - `300` to `84600`
- Default value - `0`

  `0` indicates that the Compliance Check Interval is deactivated.

10 Enter the desired value in **Compliance Check Fast Interval**.

Important To configure **Compliance Check Fast Interval**, ensure that **Compliance Check Interval** is configured and not `0`.

- Valid values (in minutes) - `1` to `1440`
- Valid values (in seconds) - `5` to `84600`
- Default value - `0`

  `0` indicates that the Compliance Check Fast Interval is deactivated.

11 To change the default value of the statuses and allow endpoints to be launched, click **Show Allowed Status Codes**.

The following status codes are supported: `In compliance`, `Not in compliance`, `Out of license usage`, `Assessment pending`, `Endpoint unknown`, and `Others`.

12 For the desired **Status Code**, click to change from **DENY** to **ALLOW**.

The default value of **In Compliance** status code is `ALLOW`. Only compliant endpoints are allowed to be launched.

The default value of all other status codes is `DENY`.

13 To upload the OPSWAT MetaAccess on-demand agent executable file for the Windows and macOS platform to Unified Access Gateway, click **Show OPSWAT On-demand Agent Settings** and configure the required settings.

   See Upload OPSWAT MetaAccess on-demand agent Software on Unified Access Gateway.

14 Click **Save**.

What to do next

1 Navigate to Horizon settings, locate **Endpoint compliance check provider** text box, and select `OPSWAT` from the drop-down menu.

2 Click **Save**.

Upload OPSWAT MetaAccess on-demand agent Software on Unified Access Gateway

Administrators can upload the on-demand agent executable file on Unified Access Gateway. This provides the option for the Horizon Client to automatically download and run the on-demand agent after the user has successfully authenticated.

For an understanding about the on-demand agent, see About OPSWAT MetaAccess on-demand agent.

Prerequisites

Locate the on-demand agent executable file on the relevant OPSWAT website and download the file to your system.

Alternately, you can also place the executable file in a file server and specify the corresponding file server location URL while configuring the settings on the Admin UI. With this URL reference, Unified Access Gateway can download the file from the configured URL.

Important For the Unified Access Gateway to successfully download the file, the file server must have the `Content-Disposition` header with the on-demand agent's file name as the value in the HTTP response.

Procedure

- For Windows platform, perform the following steps as mentioned.
  a Select the **File Upload Type**.
    - If you don't want to upload any file, select `None`.
    - `None` is the default value.
  b Depending on the file upload type selected, enter the required information for uploading the on-demand agent on Unified Access Gateway.

Option	Procedure
Local	1 Locate and select the on-demand agent executable file that you have downloaded from OPSWAT. 2 Enter the following additional information for the on-demand agent: **Name** and **Parameters**.
URL Reference	1 In the **Agent File URL**, enter the URL of the file server location from where Unified Access Gateway can download the on-demand agent executable file. 2 Enter the following additional information for the agent: **Name**, **Parameters**, **Agent URL ThumbPrints**, **Trusted Certificates**, and **Agent File refresh interval (secs)**

The following information helps you understand the settings provided for uploading the on-demand agent to Unified Access Gateway:

Name

Name of the on-demand agent executable file.

Parameters

Command-line parameters used by the Horizon Client to run the on-demand agent on the endpoint.

For command-line parameters that can be used in the **Parameters** text box, see the relevant OPSWAT documentation.

Flags

Enter the flag used by the Horizon Client to run the executable on different environments with customized run-time attributes. If more than one flag values are required, separate them by comma or space.

Examples

- RUN_AS_USER flag allows to run in the User context.
- RUN_AS_SYSTEM flag allows to run in the System context. This includes the copy to the program files area.

Agent URL Thumbprints

Enter the list of Agent URL 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.

Trusted Certificates

If the Agent URL server certificate is not issued by a trusted public CA, you can specify that certificate (in PEM format) to be trusted by Unified Access Gateway while communicating to the Agent URL for downloading the OPSWAT agent. This is an alternative to Agent URL Thumbprints.

To select a certificate in PEM format and add to the trust store, click **+**. To remove a certificate from the trust store, click **-**. By default, the alias name is the filename of the PEM certificate. To provide a different name, edit the alias text box.

Agent File refresh interval (secs)

The periodic time interval, in seconds, at which the on-demand agent executable file is fetched from the URL, which is specified in the **Agent File URL** text box.

c Click **Save**.

- For macOS platform, perform the following steps as mentioned.
  a Select the **File Upload Type**.

    If you do not want to upload any file, select `None`.

  b Depending on the file upload type selected, enter the required information for uploading the on-demand agent on Unified Access Gateway.

Option	Procedure
Local	1 Select the on-demand agent executable file that you have downloaded from OPSWAT. 2 Enter the following additional information for the on-demand agent: **Name** and **Parameters**. 3 In the **Path To Executable** text box, enter the location of the on-demand agent executable file.
URL Reference	1 In the **Agent File URL**, enter the URL of the file server location from where Unified Access Gateway can download the on-demand agent. 2 Enter the following additional information for the agent: **Name**, **Parameters**, **Agent URL ThumbPrints**, **Trusted Certificates**, and **Agent File refresh interval (secs)** 3 In the **Path To Executable** text box, enter the location of the on-demand agent executable file.

    The following information helps you understand the settings provided for uploading the on-demand agent to Unified Access Gateway:

Name

Name of the on-demand agent executable file.

Parameters

Command-line parameters used by the Horizon Client to run the on-demand agenton the endpoint.

For command-line parameters that can be used in the **Parameters** text box, see the relevant OPSWAT documentation.

Flags

Enter the flag used by the Horizon Client to run the executable on different environments with customized run-time attributes. If more than one flag values are required, separate them by comma or space.

Examples

- RUN_AS_USER flag allows to run in the User context.
- RUN_AS_SYSTEM flag allows to run in the System context. This includes the copy to the program files area.

Agent URL Thumbprints

Enter the list of Agent URL 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.

Trusted Certificates

If the Agent URL server certificate is not issued by a trusted public CA, you can specify that certificate (in PEM format) to be trusted by Unified Access Gateway while communicating to the Agent URL for downloading the OPSWAT agent. This is an alternative to Agent URL Thumbprints.

To select a certificate in PEM format and add to the trust store, click **+**. To remove a certificate from the trust store, click **-**. By default, the alias name is the filename of the PEM certificate. To provide a different name, edit the alias text box.

Agent File refresh interval

The periodic time interval, in seconds, at which the on-demand agentexecutable file is fetched from the URL, which is specified in the **Agent File URL** text box.

Path To Executable

Location of the on-demand agent executable file.

For macOS endpoints, the on-demand agent file is bundled as a zip file. The executable file is present in the zip file. Horizon Client unzips the file and runs that executable on the endpoint from the location mentioned in this text box.

c Click **Save**.

What to do next

To finish the next set of tasks, see Configure OPSWAT as the Endpoint Compliance Check Provider for Horizon.

About OPSWAT MetaAccess on-demand agent

OPSWAT MetaAccess on-demand agent is an OPSWAT client. This agent can be used as an alternative to running the OPSWAT MetaAccess persistent agent, which runs continuously on an endpoint when installed on the endpoint. Hence, the on-demand agent provides an option of running the agent only when needed.

OPSWAT MetaAccess has two types of clients: on-demand agent and persistent agent.

The persistent agent is installed on each endpoint by the user and keeps running continously on the endpoint after installation.

In case of the on-demand agent, after successful user authentication, the agent is automatically downloaded from Unified Access Gateway and run by the Horizon Client.

Note The download occurs only if the Horizon Client does not have the same version of the on-demand agent that exists on Unified Access Gateway.

Administrators can upload the on-demand agent executable files for Windows and macOS on Unified Access Gateway.

To upload the agent to Unified Access Gateway, see Upload OPSWAT MetaAccess on-demand agent Software on Unified Access Gateway.

For more information about the persistent agent and on-demand agent, see the relevant OPSWAT documentation.

Time Interval for Delaying Compliance Check

After a user has successfully authenticated with Horizon, the on-demand agent downloaded and run on the Horizon Client might take some time to register with OPSWAT. If Unified Access Gateway performs a compliance check before it has registered, the user session might be denied. To allow the on-demand agent to register with OPSWAT before the check is made, use Compliance Check Initial Delay.

Compliance Check Initial Delay is a time interval, which is an **Endpoint Compliance Check Provider** setting. Administrators can configure this time interval to delay the first compliance check after successful user authentication. Unified Access Gateway performs the first compliance check only after the configured time interval has elapsed. If the user launches a desktop or application within the delay time interval, then Unified Access Gateway allows this request and the compliance is not checked. When the compliance check is done, the session can only continue if the response is configured to allow. This timer ensures that a user with a compliance device is not denied access after initial authentication.

After the configured delay time interval has elapsed, Unified Access Gateway performs periodic endpoint compliance checks using the Compliance Check Interval and Compliance Check Fast Interval settings as per the existing behavior. For more information about this behavior, see Time Interval for Periodic Endpoint Compliance Checks.

For more information about the `Compliance Check on Authentication` option, see Configure Horizon Settings. To configure the initial delay time interval for OPSWAT, see Configure OPSWAT as the Endpoint Compliance Check Provider for Horizon.

Time Interval for Periodic Endpoint Compliance Checks

Administrators can configure time intervals for periodic compliance checking of an endpoint during an authenticated user session. The periodic compliance checking ensures that the device remains compliant throughout the session. **Endpoint Compliance Check Provider** setting has two time intervals: Compliance Check Interval and Compliance Check Fast Interval.

When the **Compliance Check Interval (mins)** is configured, Unified Access Gateway performs compliance checks on an endpoint when a user attempts to run a remote desktop or application session using Horizon Client on that endpoint. Endpoints are periodically checked for compliance as per the configured time intervals.

After the initial compliance check, sometimes an endpoint might become non-compliant due to several reasons such as policy changes done by administrators. Despite compliance assessment pending, endpoints might require access to run a session. If the device status is `Assessment pending` or `Endpoint unknown`, the **Compliance Check Fast Interval (mins)** can be used.

When both intervals are configured and if the device status is either `Assessment pending` or `Endpoint unknown`, Unified Access Gateway first runs the compliance check fast interval. After the endpoint becomes compliant, Unified Access Gateway then runs the compliance check interval.

During the periodic compliance check, if an endpoint is found to be non-compliant then the user session is disconnected.

Compliance Check Interval (mins)

This text box allows you to configure a periodic time interval at which the Horizon Client sends compliance check requests to Unified Access Gateway during a session.

Compliance Check Fast Interval (mins)

This text box allows you to configure a periodic, frequent time interval at which the Horizon Client sends compliance check requests to Unified Access Gateway during a session for an endpoint in specific statuses other than `In compliance`. The statuses are `Assessment pending` and `Endpoint unknown` and must be configured as `ALLOW`.

For example, when the on-demand agent is assessing an endpoint and the device status is either `Assessment pending` or `Endpoint unknown`, you can set the time interval to `1 minute` so that the compliance checks are more frequent at the beginning of a session.

Important **Compliance Check Fast Interval (mins)** can be configured only when the time interval of **Compliance Check Interval (mins)** is configured and the value is not `0`.

To configure the time intervals for the endpoint compliance check provider, see Configure OPSWAT as the Endpoint Compliance Check Provider for Horizon.

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.

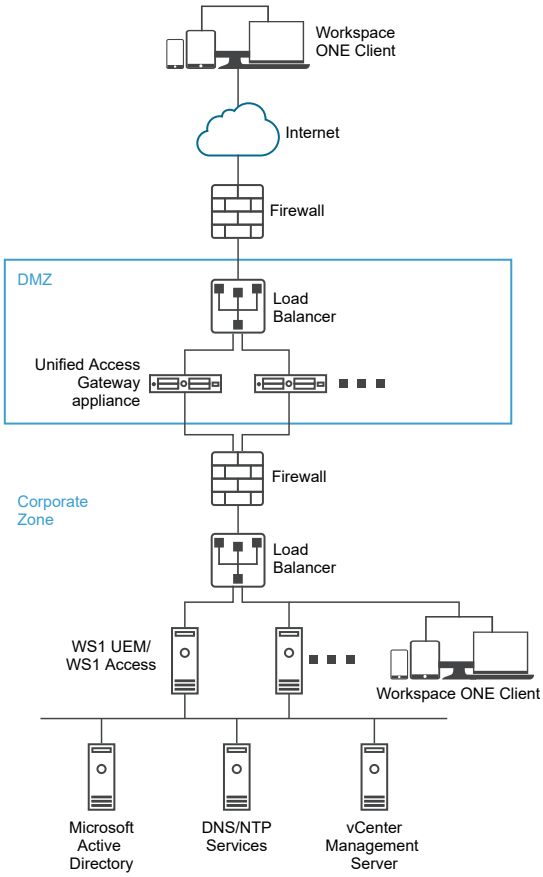
Deployment Scenario

Unified Access Gateway provides secure remote access to an On-Premises deployment of Workspace ONE Access. Unified Access Gateway appliances are typically deployed in a network demilitarized zone (DMZ). With Workspace ONE Access, the Unified Access Gateway appliance operates as a web reverse proxy between a user's browser and the Workspace ONE Access 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 4-4. 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 Workspace ONE Access 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.
- Simple proxy patterns are case sensitive. Page links and proxy patterns must match.

Configure Reverse Proxy With Workspace ONE Access

You can configure the Web reverse proxy service to use Unified Access Gateway with Workspace ONE Access.

Prerequisites

Note the following requirements for deployment with Workspace ONE Access:

- Split DNS. Externally, the host name must get resolved to the IP address of Unified Access Gateway. Internally, on Unified Access Gateway, the same host name must 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.

- Workspace ONE Access 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 must 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's **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 Workspace ONE Access, add the IP address, the Workspace ONE Access host name, and the external DNS on the client machine. On the Admin UI, add the IP address, the Workspace ONE Access host name, and the internal DNS.

Option	Description
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 Workspace ONE Access. 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>`.

Option	Description
UnSecure Pattern	Enter the known Workspace ONE Access 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 instance. Host pattern is optional, when configuring Web reverse proxy instances.
Trusted Certificates	■ To select a certificate in PEM format and add to the trust store, click **+** . ■ To provide a different name, edit the alias text box. By default, the alias name is the filename of the PEM certificate. ■ To remove a certificate from the trust store, click **-**.

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 Workspace ONE Access. 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. `SecurID`, `RADIUS`, `Passthrough`, and `X.509 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	■ To select a certificate in PEM format and add to the trust store, click **+** . ■ To provide a different name, edit the alias text box. By default, the alias name is the filename of the PEM certificate. ■ To remove a certificate from the trust store, click **-**.
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.

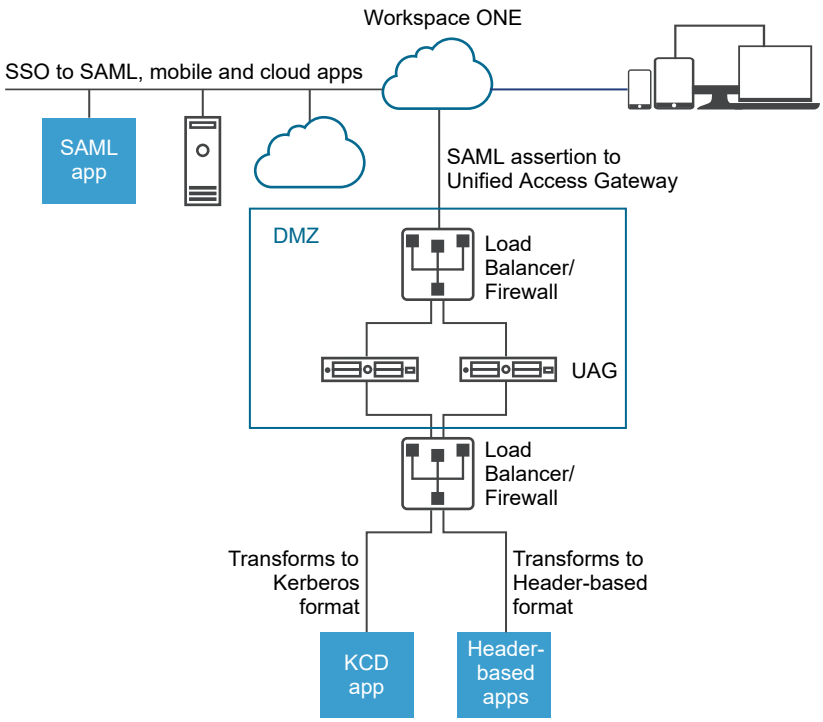
Deployment for Single Sign-on Access to On-Premises Legacy Web Apps

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. Workspace ONE Access acts as an identity provider and provides SSO into SAML applications. When users access legacy applications that require KCD or header-based authentication, Workspace ONE Access 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 4-5. Unified Access Gateway Identity Bridging Mode



Identity Bridging Deployment Scenarios

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

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

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

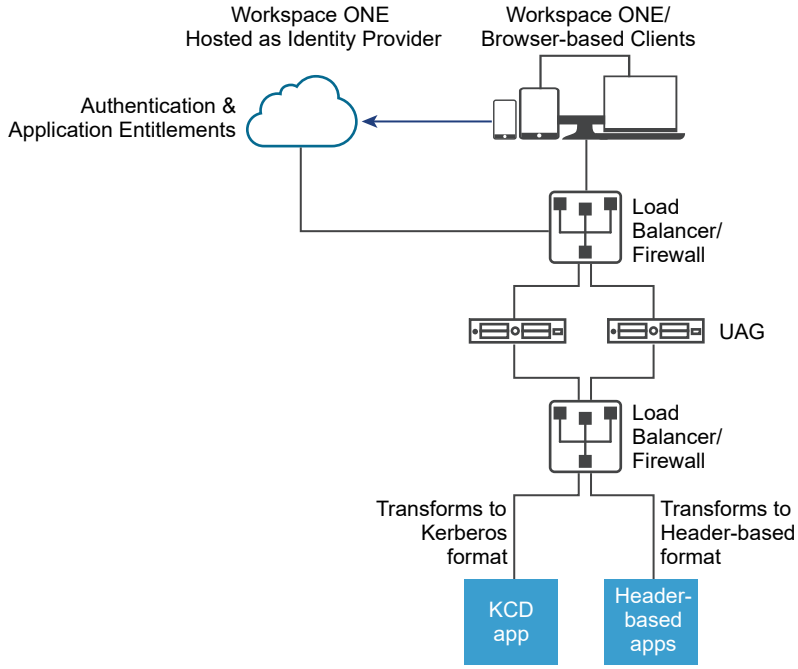
If the user is validated, the identity provider creates a SAML token and sends it to the user. The user passes the SAML token to Unified Access Gateway in the DMZ. Unified Access Gateway validates the SAML token and retrieves the User Principal Name from the token.

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

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

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

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



Using Identity Bridging with Workspace ONE Clients On Premises

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

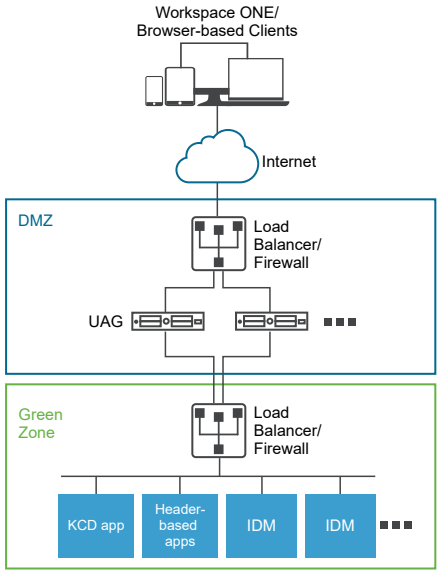
The user passes the SAML token to Unified Access Gateway. Unified Access Gateway validates the SAML token and retrieves the User Principal Name from the token.

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

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

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

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



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 Workspace ONE Access as the identity provider, download and save the SAML metadata file from the Workspace ONE Access 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 Workspace ONE Access 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.

Option	Description
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 Workspace ONE Access. 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>`.

Option	Description
UnSecure Pattern	Enter the known Workspace ONE Access 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 instance. Host pattern is optional, when configuring Web reverse proxy instances.
Trusted Certificates	■ To select a certificate in PEM format and add to the trust store, click **+** . ■ To provide a different name, edit the alias text box. By default, the alias name is the filename of the PEM certificate. ■ To remove a certificate from the trust store, click **-**.

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.
SAML Audiences	Ensure that SAML authentication type is chosen. Enter the audience URL. **Note** If the text box is left empty, audiences are not restricted. To understand how UAG supports SAML Audiences, see SAML Audiences.
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 Workspace ONE Access service.

Add the Metadata File to VMware Workspace ONE Access Service

The Unified Access Gateway service provider metadata file that you downloaded must be uploaded to the Web application configuration page in the Workspace ONE Access 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 Workspace ONE Access 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

Option	Description
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. Turn on the **Enable Cert Revocation** toggle.
   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 the information indicating if 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 Turn on the **Enable Identity Bridging Settings** toggle, 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.

Configuring Horizon for Unified Access Gateway and Third-Party Identity Provider Integration

If you are using a SAML 2.0 identity provider, you can directly integrate the identity provider with Unified Access Gateway to support Horizon Client user authentication. To use SAML third-party integration with UAG, you must use Horizon Connection Server 7.11 or later versions.

The authentication sequence can be SAML and Passthrough for SAML authentication and AD password authentication or only SAML when used with Horizon True SSO.

Unified Access Gateway supports unauthenticated access to a Horizon Client user logging into Unified Access Gateway when integrated with a SAML identity provider. After the initial authentication with Unified Access Gateway, the user can receive entitlements for published applications with no additional authentication. The SAML and Unauthenticated method supports this feature.

With the Unified Access Gateway and third-party SAML identity provider integration support, Workspace ONE Access installation is not used.

Note When Horizon SAML 2.0 is used with Horizon True SSO to avoid the initial AD password prompt, and if the session is manually locked or locks due to inactivity, the user must either enter their AD password to unlock the session or close the client and reconnect. The Horizon True SSO unlock mechanism currently depends on Workspace ONE Access.

To integrate Unified Access Gateway with the identity provider, you must configure the identity provider with service provider (Unified Access Gateway) information, upload the identity provider's metatdata file to Unified Access Gateway and configure Horizon settings on the Unified Access Gateway Admin UI console.

For information about authenticating users to Horizon Client without being prompted for Active Directory credentials, see *Authenticating Users Without Requiring Credentials* and related information in the *Horizon Administration* guide at VMware Docs.

Configure the Identity Provider with Unified Access Gateway Information

To integrate UAG (service provider) with the identity provider, you must configure the identity provider with the service provider information such as entity ID and assertion consumer endpoint URL. In this case, UAG is the service provider.

Procedure

1. Log into the identity provider's Admin console.
2. To create a SAML application, follow the appropriate steps on the identity provider's Admin console.

   If the identity provider has an encrypt assertion feature, ensure that the feature is disabled in the SAML settings for the application that you create on the identity provider.

3 Configure the identity provider with the UAG information in one of the following ways:

Option	Description
Download SAML service provider metadata from the UAG.	To import the SAML metadata into the identity provider, ensure that the identity provider supports import functionality. a In the **Configure Manually** section of the UAG Admin UI, click **Select**. b In the **General Settings** section, for **Edge Service Settings**, click **Show**. c Click the **Horizon Settings** gearbox icon. d On the **Horizon Settings** page, click **More**. e Select the **Auth Methods**. The **Auth Methods** can be `SAML`, `SAML and Passthrough`, or `SAML and Unauthenticated`. **Note** If you choose `SAML and Unauthenticated`, ensure that you configure the Horizon Connection Server setting as mentioned for this **Auth Method** in Configure Horizon Settings on Unified Access Gateway for SAML Integration. f Click **Download SAML service provider metadata**. g On the **Download SAML service provider metadata** window, select the Identity Provider and enter the external host name. h Click **Download**. i Save the `.xml` metadata file to a location on your computer that you have access to. j Log into the identity provider's admin console. k Import the downloaded metadata file into the identity provider.
Configure the following SAML settings on the identity provider's Admin console.	a Set up the entity ID as `https://<uagIP/domain>/portal` b Set up the assertion consumer endpoint URL as `https://<uagIP/domain>/portal/samlsso`.

For more information about the authentication methods for Unified Access Gateway and third-party identity provider integration, see Authentication Methods for Unified Access Gateway and Third-Party Identity Provider Integration.

4 (Optional) Configure the custom attribute with a user name.

In the Unified Access Gateway Admin UI, when `SAML and Unauthenticated` is selected as the authentication method, if **SAML Unauthenticated Username Attribute** is configured with the same attribute name as specified here and when the SAML assertion is validated, Unified Access Gateway provides unauthenticated access to the user name configured for this custom attribute.

To understand how Unified Access Gateway provides unauthenticated access to this user name, see Authentication Methods for Unified Access Gateway and Third-Party Identity Provider Integration.

What to do next

Upload identity provider's SAML metadata XML file to UAG.

Upload Identity Provider's SAML Metadata to Unified Access Gateway

To configure SAML and SAML and Passthrough authentication methods in Horizon, you must upload the identity provider's SAML certificate metadata XML file to UAG (Unified Access Gateway). The upload allows UAG to trust the identity provider by verifying the signature of an assertion using the public key of the identity provider.

Prerequisites

You must have downloaded the SAML metadata XML file from the identity provider and saved this file to a computer you can access.

Procedure

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

   If you do not enter a value in the Entity ID text box, the identity provider name in the metadata file is parsed and used as the entity ID of the identity provider.
4. In the **IDP Metadata** section, click **Select** and browse to the location where you have saved the metadata file.
5. Select **PEM** as the certificate format type from the **Encryption Certificate Type** drop-down menu.

   Note You must select PEM if you want to use encrypted assertion to validate SAML authentication. Encryption and decryption of the assertion requires a combination of a public and private key. The Identity provider encrypts the assertion with a public key which can be decrypted by UAG only with a public and a private key combination, thus ensuring enhanced security.
6. For the **Private Key**, click **Select** and browse to the location where you have saved the private key for the certificate in PEM format.
7. For the **Certificate Chain**, click **Select** and browse to the location where you have saved the certificate chain in PEM format.
8. To enable the **Allow unencrypted SAML assertions** option, turn on the toggle. If the toggle is turned off, unencrypted assertions are not allowed during SAML authentication.

9 To enable the **Always force SAML auth** function, turn on the toggle. When the toggle is turned on, it always forces the SAML auth page to be presented to the user when this Identity provider is used, provided the IDP is also configured to force SAML auth.

Note When you enable the **Always force SAML auth** function, `SAML ForceAuthn="true"` is set as an attribute for the AuthnRequest to the IdP. The IdP is notified to ignore any previous security context while authenticating the user.

10 Click **Save**.

The following message is displayed: `Configuration is saved successfully.`

What to do next

Configure the Horizon settings on UAG for selecting the authentication method and choosing the required identity provider.

Configure Horizon Settings on Unified Access Gateway for SAML Integration

You must select the relevant SAML authentication method and choose the IDP (Identity Provider) supported by your organization in the Horizon settings page on the UAG (Unified Access Gateway). The authentication method determines the login flow for the user when using the Horizon Client with UAG.

For information about authentication methods, see Authentication Methods for Unified Access Gateway and Third-Party Identity Provider Integration

Prerequisites

- Ensure that you use Horizon Connection Server 7.11 or later versions.
- You must have already uploaded the identity provider's metadata to UAG.

  See Upload Identity Provider's SAML Metadata to Unified Access Gateway.

Procedure

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

2 In the **General Settings** section, for **Edge Service Settings**, click **Show**.

3 Click the **Horizon Settings** gearbox icon.

4 On the **Horizon Settings** page, click **More** to configure the following settings:

Option	Description
Auth Methods	Select `SAML`, `SAML and Passthrough`, or `SAML and Unauthenticated` **Note** If TrueSSO is enabled on Horizon Connection Server, only SAML authentication method must be used. **Important** If you choose `SAML and Unauthenticated`, ensure that you configure the **Login Deceleration Level** in the Horizon Connection Server to `Low`. This configuration is necessary to avoid long delay in login time for endpoint while accessing the remote desktop or application. For more information about how to configure **Login Deceleration Level**, see the *Horizon Administration* documentation at VMware Docs.
Identity Provider	Select the Identity Provider that must be integrated with UAG. **Note** An identity provider is available for selection only if the identity provider's metadata is uploaded to UAG.

To configure the other Horizon settings, see Configure Horizon Settings.

Authentication Methods for Unified Access Gateway and Third-Party Identity Provider Integration

SAML, SAML and Passthrough, and SAML and Unauthenticated are the supported authentication methods to integrate UAG (Unified Access Gateway) with a third-party identity provider for controlling access to Horizon desktops and applications. The authentication method determines how the Horizon user is authenticated.

While configuring Horizon settings in the UAG, you must select one of the authentication methods.

SAML

In the SAML authentication method, UAG first validates the SAML assertion. If the SAML assertion is valid, UAG passes the SAML assertion to the Horizon Connection Server. For the Horizon Connection Server to accept the assertion, the Connection Server must be configured with the identity provider's metadata. When a user accesses the Horizon Client, the user is presented with entitlements without being prompted to provide the Active Directory credentials.

Note If the TrueSSO setting is enabled on Horizon Connection Server, SAML authentication method must be used.

SAML and Passthrough

In the SAML and Passthrough authentication method, UAG validates the SAML assertion. If the SAML assertion is valid, the user is prompted to provide the Active Directory authentication credentials when accessing the Horizon Client. In this authentication method, UAG does not pass the SAML assertion to the Horizon Connection Server.

SAML and Unauthenticated

In the SAML and Unauthenticated method, Unified Access Gateway combines SAML user authentication with Horizon's unauthenticated access feature. If the SAML assertion is valid, the user can access RDS hosted applications with no further authentication required. In the Horizon unauthenticated access feature, a role-based user alias is used with Horizon to determine application entitlements. The user alias can be used as the default alias by Horizon. This alias can also be specified as a default in Unified Access Gateway configuration (**Default Unauthenticated Username**) or this can be the value of a named SAML attribute presented as a claim in the SAML assertion sent by the identity provider.

Unified Access Gateway Admin UI has two text boxes - **SAML Unauthenticated Username Attribute** and **Default Unauthenticated Username** - which can be used to specify the user alias. These text boxes are available on the Admin UI when the authentication method is SAML and Unauthenticated.

If the **SAML Unauthenticated Username Attribute** text box is set in the Admin UI, when Unified Access Gateway validates the SAML assertion and if the name is present in the SAML assertion, Unified Access Gateway uses that value as Horizon's unauthenticated access user alias.

When the **SAML Unauthenticated Username Attribute** text box is empty or the attribute name specified in this text box is missing in the SAML assertion, Unified Access Gateway uses the default user name configured in the **Default Unauthenticated Username** text box as Horizon's unauthenticated access user alias.

If **SAML Unauthenticated Username Attribute** is not used and the **Default Unauthenticated Username** text box is empty, Unified Access Gateway uses the default user alias configured in Horizon.

For more information about setting up configuration for the unauthenticated access users, see *Providing Unauthenticated Access for Published Applications* and related information in the *Horizon Administration* guide at VMware Docs.

For more information about providing entitlements (published applications) to the unauthenticated access users, see *Entitle Unauthenticated Access Users to Published Applications* and related information in the *Horizon Administration* guide at VMware Docs.

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.

VMware Tunnel on Unified Access Gateway

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

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

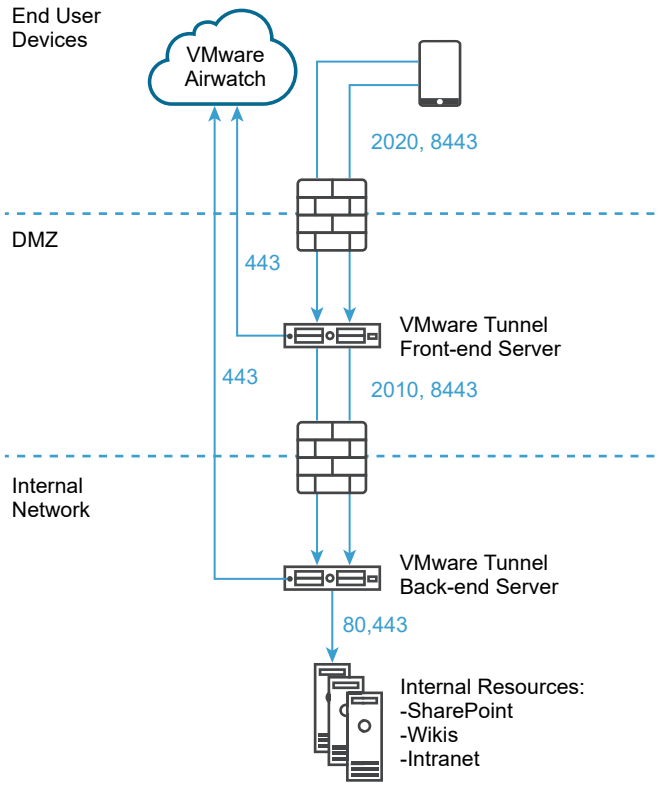
Both Tunnel Proxy and Per-App Tunnel deployment models can be used for a multi-tier network on the UAG appliance. The deployment consists of a front-end Unified Access Gateway server deployed in the DMZ and a back-end server deployed in the internal network.

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

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

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

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



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

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

Configure VMware Tunnel 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, hostnames and ports, and which features of VMware Tunnel to implement. You can consider to change the 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 you are configuring VMware Tunnel for the first time, then select **Configure** and follow the configuration wizard screens.
   - If you are configuring VMwareTunnel for the first time, then select **Override**, then select the **Enabled VMware Tunnel** toggle switch, and then select **Configure**.

     Note Overriding VMware Tunnel Proxy settings does not override VMware Tunnel configuration settings.

2 On the **Deployment Type** screen, select **Enable Proxy (Windows & Linux)** the 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. To see an example for the selected type, select the information icon.

4 Select **Next**.

5 On the **Details** screen, configure the following settings. The options that are displayed on the **Details** screen depend on the configuration type you have selected in 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 check box if you want to use SSL Offloading to ease the burden of encrypting and decrypting traffic from the VMware Tunnel server.
Use Kerberos Proxy	To allow access to Kerberos authentication for your target back-end Web services, select the Kerberos proxy support This feature does not currently support Kerberos Constrained Delegation (KCD). 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://, and so on.
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 must use different values.
Enable SSL Offloading	Select this check box if you want to use SSL Offloading to ease the burden of encrypting and decrypting traffic from the VMware Tunnel server.
Use Kerberos Proxy	To allow access to Kerberos authentication for your target back-end Web services, select the Kerberos proxy support This feature does not currently support Kerberos Constrained Delegation (KCD). The Endpoint server must be on the same domain as KDC for the Kerberos Proxy to communicate successfully with the KDC. In the **Realm** text box, enter the Realm of the KDC server.

6 Select **Next**.

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

   a Select the **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 use AirWatch issued certificates. To use Enterprise CA certificates for the 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, republish 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 use access logs for the proxy or Per-App Tunnel components. Enable the **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 access logs and syslog integration 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 an 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**.

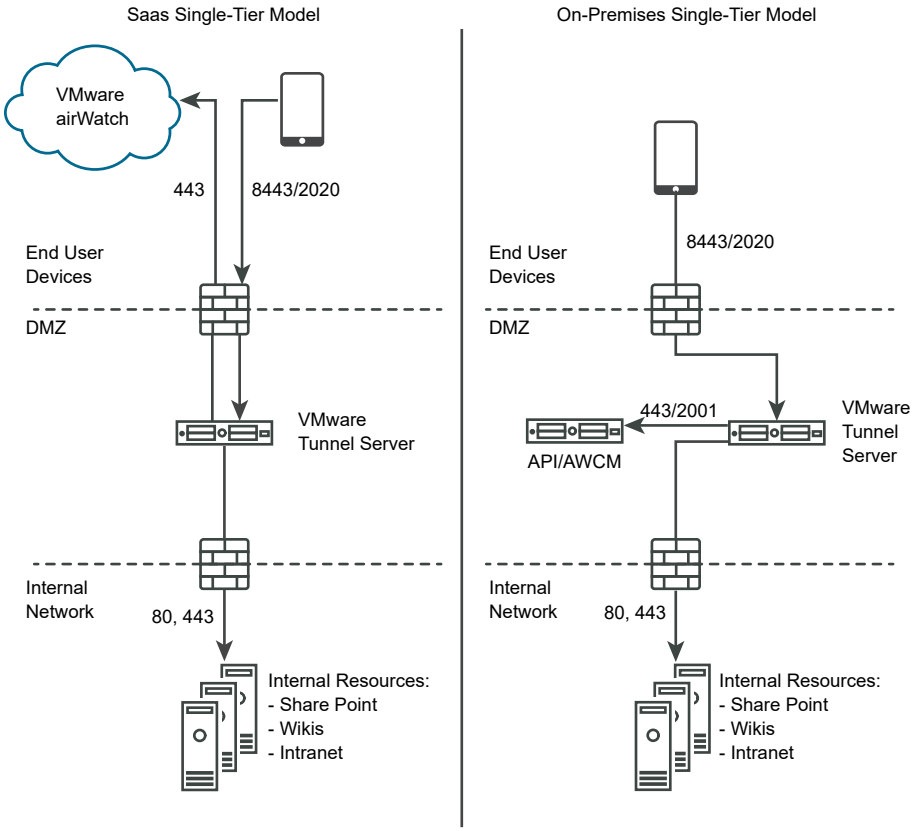
Deploying VMware Tunnel using Single-Tier Deployment

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.

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.



Deploying VMware Tunnel using Cascade Mode

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 Deploying VMware Tunnel using Relay-Endpoint .

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.

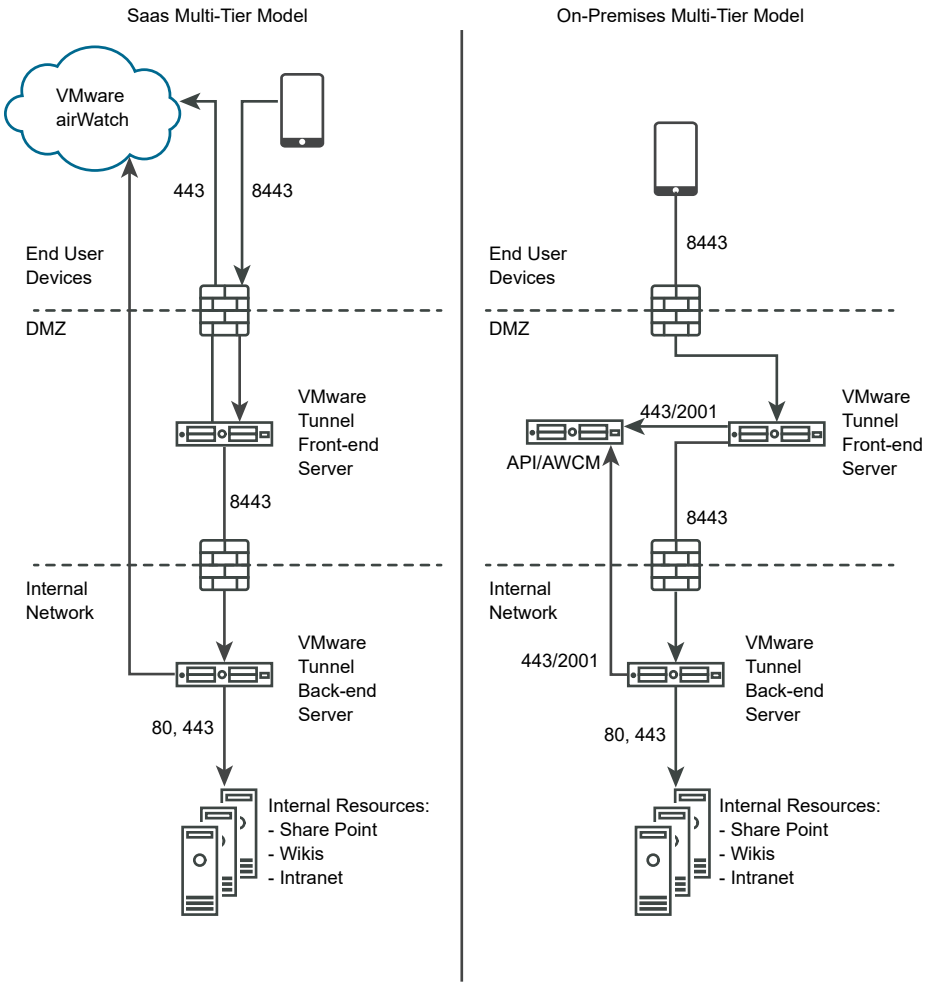
The front-end server facilitates authentication of devices by connecting to AWCM when requests are made to the VMware Tunnel. When a device makes a request to the VMware Tunnel, the front-end server determines if the device is authorized to access the service. Once authenticated, the request is forwarded 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 *Configure Network Traffic Rules for the Per-App Tunnel* in the VMware Workspace ONE UEM Product Documentation at VMWare Docs.

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



Deploying VMware Tunnel using Relay-Endpoint

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 Deploying VMware Tunnel using Cascade Mode.

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 4-9. On-premises configuration for Relay-Endpoint deployments

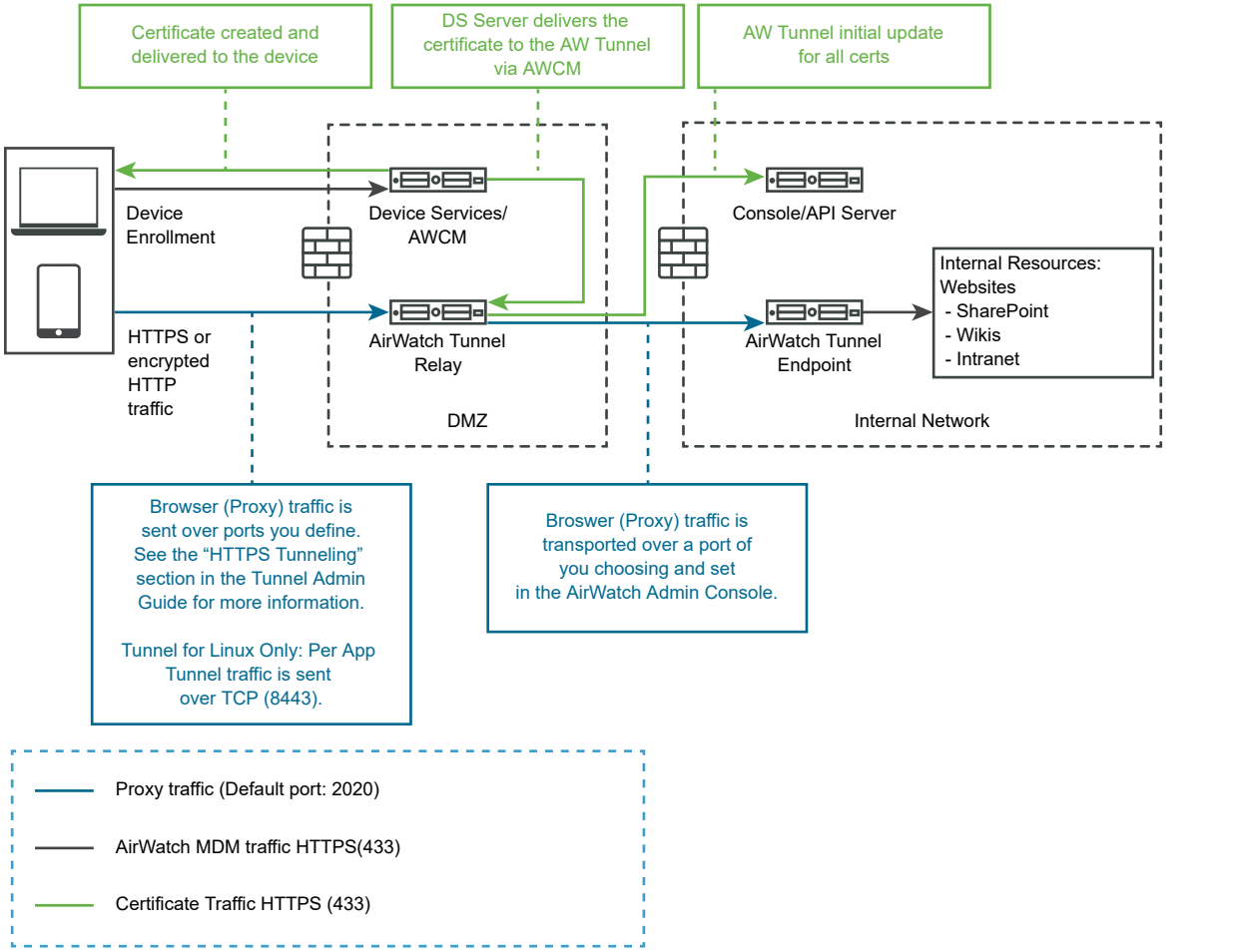
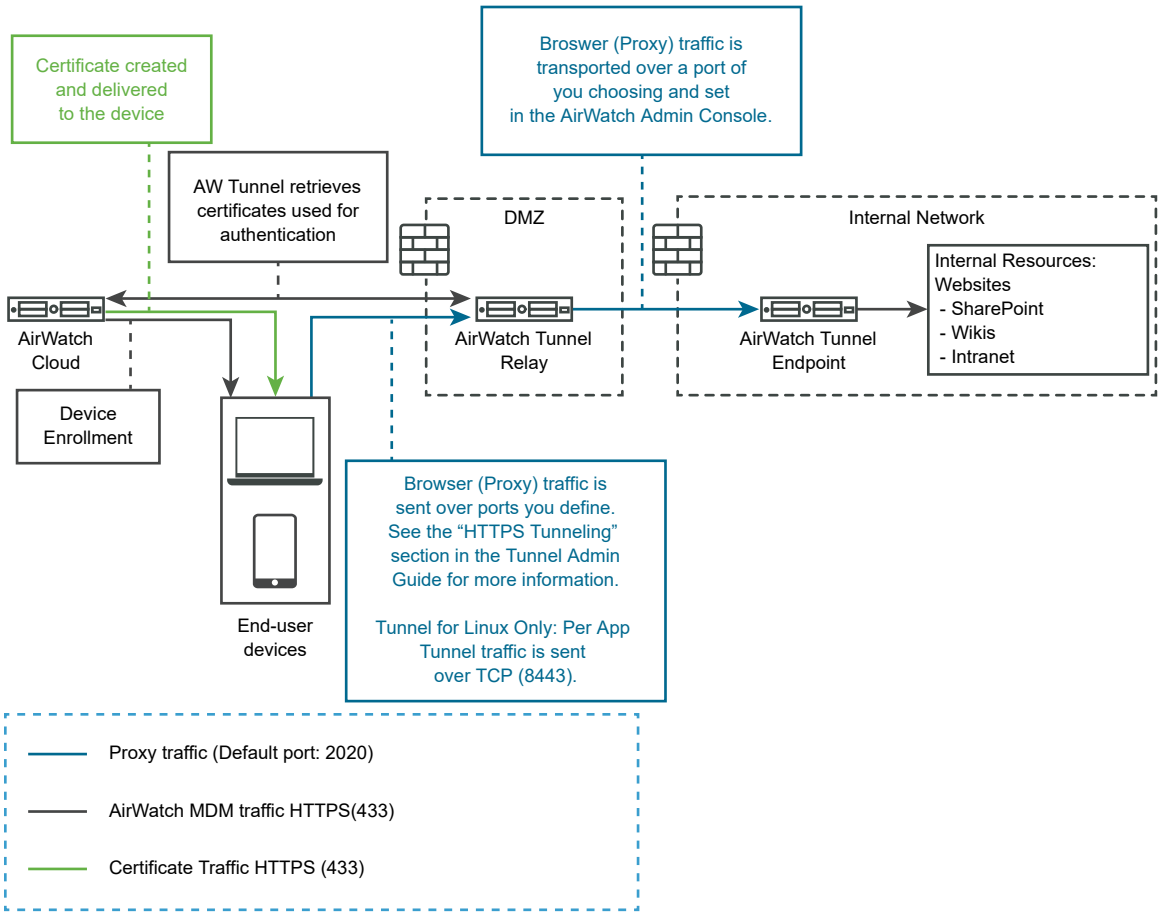


Figure 4-10. SaaS configuration for Relay-Endpoint deployments



ConfigureVMware 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.
API Server Password	Enter the password to log in to the API server.

Option	Description
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 example2.com example-alias`**. Click the '+' sign to add multiple host entries. **Important** The host entries are saved only after you click **Save**.
Trusted Certificates	■ To select a certificate in PEM format and add to the trust store, click **+**. ■ To provide a different name, edit the alias text box. By default, the alias name is the filename of the PEM certificate. ■ To remove a certificate from the trust store, click **-**.

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)

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, Secure Email 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. To enable Content Gateway settings, select **YES**.
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	■ To select a certificate in PEM format and add to the trust store, click **+**. ■ To provide a different name, edit the alias text box. By default, the alias name is the filename of the PEM certificate. ■ To remove a certificate from the trust store, click **-**.
Host Entries	Enter the details to be added in `/etc/hosts` file. Each entry must 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**.

Configure Content Gateway on the UEM Console

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. The pre-configured settings eliminate the need to configure the settings manually post-installation on the server.

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

Note Content Gateway services are now supported only on the Unified Access Gateway. Legacy Linux and Windows versions of Content Gateway are no longer supported.

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 text boxes that appear to configure a Content Gateway instance.

a Configure the **Installation Type**.

Setting	Description
Installation Type	Unified Access Gateway appears as the default available platform for Content Gateway.

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
Ignore SSL Errors (not recommended)	If you are using a self-signed certificate, then enable this setting. If enabled, Content Gateway ignores certificate trust errors and certificate name mismatches.

d Configure the **Certificate Authentication** settings.

Setting	Description
Enable Cross-domain KCD Authentication	Enable this setting to authenticate users with the PIV-D Derived Credentials instead of user names and passwords. PIV-D certificate authentication is for the users who access the on-prem SharePoint repositories from their devices.
Client Certificate Chain	The certificate chain used to issue client certificates.
Target SPN	SPN of the target service.
Service Account Username	User name of the service account that has delegation rights.
Service Account Password	Password for the service account.
Domain	Name of the domain in the Active Directory (AD) containing the users.
Domain Controller	Hostname or IP address of the domain controller for the domain.

e Enter the Content Gateway edge service values under the **Custom Gateway Settings**.

This step is optional. You must perform this step only if you want to override the default configuration values for Content Gateway.

With the edge service values set on the UEM console, the configuration file changes are automated and do not require manual updates to the configuration files each time the UAG is upgraded. For more information about the custom values for Content Gateway, see #unique_114.

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://kb.vmware.com/s/article/2960835

5 Select **Add** and then select **Save**.

What to do next

After configuring settings in the UEM Console, download the installer, configure additional nodes, or manage configured nodes.

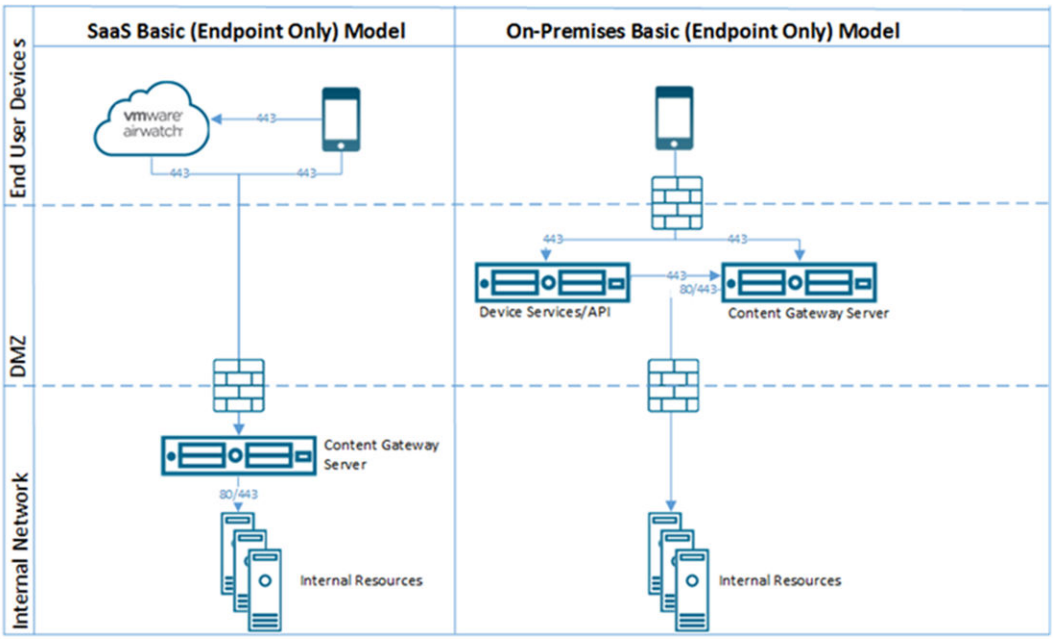
Basic (Endpoint Only) Deployment Model for Content Gateway

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

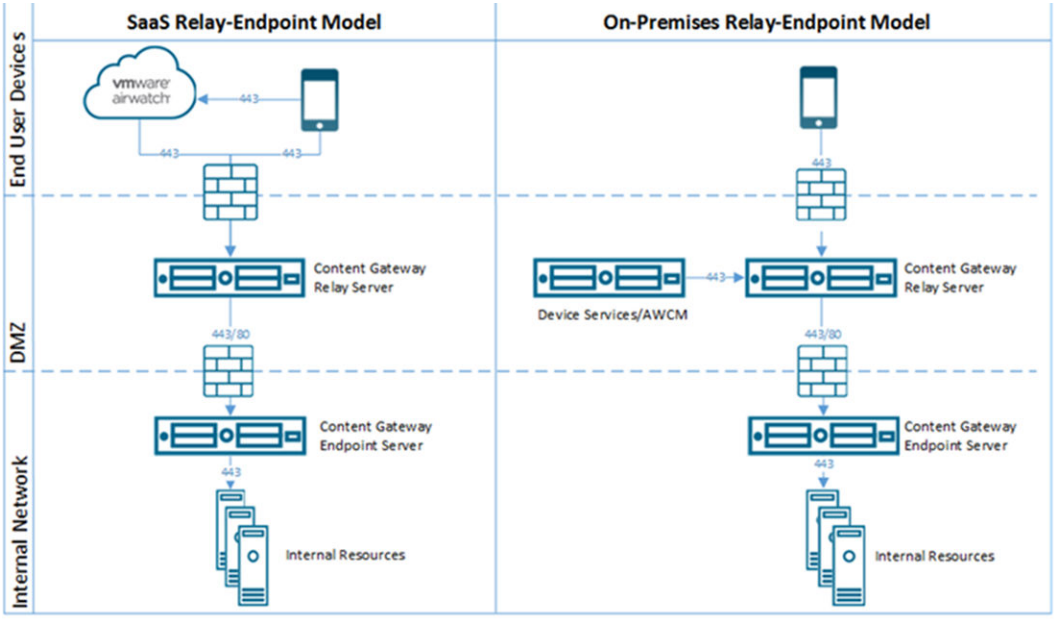
The relay-endpoint deployment model architecture includes two instances of the VMware Content Gateway with separate roles.

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

Ensure that you have configured MEM settings in **Email Settings** on the Workspace ONE UEM console. After configuring MEM, note down the auto-generated MEM Config GUID. For more information, see Secure Email Gateway documentation.

Note

- Secure Email Gateway is supported by all the Unified Endpoint Management (UEM) versions.
- Secure Email Gateway is configured to follow the Syslog configurations which is configured as part of Unified Access Gateway System Settings. By default only the contents of app.log in Secure Email Gateway will be triggered as Syslog events. For more information, see Unified Access Gateway System Settings.

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 console. The Configuration GUID is displayed on the Mobile Email Management configuration page on the UEM console.
Add SSL Certificate	Toggle to add the SSL Certificate if the option to locally upload SSL certificate is enabled under Email Settings in UEM Console.
SSL Certificate	Click Select to upload a .PFX or .P12 certificate file. **Note** You can also upload the SSL Certificate in the Workspace ONE UEM console. When the certificate is uploaded locally, the thumbprint of the certificate is displayed on the Admin GUI.
Password	Enter the password for the SSL certificate.
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	■ To select a certificate in PEM format and add to the trust store, click **+**. ■ To provide a different name, edit the alias text box. By default, the alias name is the filename of the PEM certificate. ■ To remove a certificate from the trust store, click **-**.
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.

You can also change the logging levels by configuring the Secure Email Gateway key-value pairs on the Workspace ONE UEM console. To use the key-value pairs, you must have the required Secure Email Gateway custom settings features (specific Windows and Unified Access Gateway versions). For more information, see the *SEG Custom Gateway Settings* section in the Secure Email Gateway V2 documentation.

By using the key-value pairs from the Workspace ONE UEM console, you can change the logging levels for all Unified Access Gateway appliances at once.

Prerequisites

If not already done, you must enable SSH on the Linux virtual machine.

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 Secure Email Gateway

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

You can also enable EWS proxy by configuring the Secure Email Gateway key-value pairs on the Workspace ONE UEM console. To use the key-value pairs, you must have the required Secure Email Gateway custom settings features (specific Windows and Unified Access Gateway versions). For more information, see the *SEG Custom Gateway Settings* in the Secure Email Gateway documentation.

By using the key-value pairs from the Workspace ONE UEM console, you can enable the EWS proxy for all Unified Access Gateway appliances at once.

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, Secure Email 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.

Configure Workspace ONE Intelligence Connection Settings

To use the Workspace ONE Intelligence features such as data settings and risk score in Unified Access Gateway, a connection setting must be created on Unified Access Gateway. A connection setting can be used for sending Unified Access Gateway-specific or edge-services related data to Workspace ONE Intelligence or for gathering risk score-related information from Workspace ONE Intelligence as part of the endpoint compliance check.

Any number of Workspace ONE Intelligence connection settings can be configured. The same connection setting can be used across multiple use cases (risk score and data setting). Note that for each use case, only one connection setting can be used at a time. For example: to change the connection used for the Workspace ONE Intelligence risk score provider, you must edit the provider settings and select another connection.

The Workspace ONE Intelligence credentials file is a `JSON` file containing Workspace ONE Intelligence URL, access token endpoint URL, client ID, and client secret for authorizing Unified Access Gateway to communicate with Workspace ONE Intelligence. You can download this file from the Unified Access Gateway integrations page on the Workspace ONE Intelligence console.

Prerequisites

- You must have already registered the Unified Access Gateway widget on Workspace ONE Intelligence.
- You must have already downloaded the credentials file from Workspace ONE Intelligence and saved this file on a computer which you can access.

To integrate Unified Access Gateway in Workspace ONE Intelligence and download the credentials file, see the *Integrations in Workspace ONE Intelligence* and *Register VMware Unified Access Gateway* sections in the VMware Workspace ONE Intelligence Products documentation.

Procedure

1. In the **Configure Manually** section of the Unified Access Gateway Admin console, click **Select**.
2. In **Advanced Settings**, click the **Workspace ONE Intelligence Connection Settings** gearbox icon.
3. To configure the settings for a connection, click **Add**.

   Ensure that Unified Access Gateway is able to reach the Workspace ONE Intelligence endpoint hosts present in the uploaded credentials `JSON` file.

4 Configure the following Workspace ONE Intelligence settings :

Option	Description
Name	Name of the Workspace ONE Intelligence connection setting. Every connection setting must have a unique name.
Workspace ONE Intelligence URL Thumbprints	Enter the list of Workspace ONE Intelligence URL 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. **Note** This UI option can be used when the connection to Workspace ONE Intelligence is through a TLS reverse proxy or a security appliance that presents a TLS server certificate, which is not issued by a trusted CA.
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. To give a different name, edit the alias text box. **Note** This UI option can be used when the connection to Workspace ONE Intelligence is through a TLS reverse proxy or a security appliance that presents a TLS server certificate, which is not issued by a trusted CA.

5 To upload the **Workspace ONE Intelligence Credentials file**, navigate to the file location and select the desired file.

6 (Optional) After you save the file on Unified Access Gateway, to ensure that the client secret in the credentials file is secure, you can either encrypt or delete the file.

Results

The following message is displayed: `Configuration is saved successfully.`

Select the Workspace ONE Intelligence Data Setting

Unified Access Gateway communicates with Workspace ONE Intelligence to send Unified Access Gateway-specific and edge services-related data to Workspace ONE Intelligence. By using the data settings configuration page, a connection setting can be enabled for sending data to Workspace ONE Intelligence at regular intervals.

For example: Unified Access Gateway can now send data to Workspace ONE Intelligence about different application IDs, user names, destination hostnames, ports, and so on, connected through VMware Tunnel at specific time intervals.

Administrators can use the Unified Access Gateway data sent to Workspace ONE Intelligence to understand how Unified Access Gateway and the edge services on Unified Access Gateway are used. Administrators can also create custom reports to understand the behavior of clients connected to Unified Access Gateway through the edge services.

Prerequisites

You must have already added and configured the connection by using the **Workspace ONE Intelligence Connection Settings** window. For more information, see Configure Workspace ONE Intelligence Connection Settings.

Procedure

1. In the **Configure Manually** section of the Unified Access Gateway admin console, click **Select**.
2. In the **Advanced Settings** section, click the **Workspace ONE Intelligence Data Settings** gearbox icon.
3. To enable sending data for the desired connection setting, toggle the **Opt In/Opt Out** button to `OPT IN`.

   By default, the value is `OPT OUT`.
4. Select the connection name.
5. In the **Update Interval** field, enter the maximum time period at which the data is sent from Unified Access Gateway to Workspace ONE Intelligence.

   Note If the local cache is filled up and reaches its maximum size before the scheduled interval, Unified Access Gateway will immediately post the data to Workspace ONE Intelligence.

   - Time period is in seconds.
   - Values can be between `10` seconds and `86400` seconds.
   - Default value is `300` seconds (`five` minutes).
   - If value is `0`, data is posted to Workspace ONE Intelligence once for every `Enabled` state of Workspace ONE Intelligence settings on the Unified Access Gateway.

What to do next

1. Configure VMware Tunnel.

   See ConfigureVMware Tunnel Settings for Workspace ONE UEM

   Important If you have already configured VMware Tunnel, you must enable and save the Tunnel settings again.
2. Access the Unified Access Gateway dashboard on the Workspace ONE Intelligence console to view the data sent by Unified Access Gateway to Workspace ONE Intelligence.

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.

Read the following topics next:

- 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. To see the cipher list format, you can search for "openssl cipher string" in a web browser.
- 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` (certificate and key) 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 TLS 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 v1.2 are enabled. TLS v1.0, TLS v1.1, 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`, `ssl30Disabled`, `tls10Enabled`, `tls11Disabled`, 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_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_
WITH_AES_128_CBC_SHA256
, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384",
  "ssl30Enabled": "false",
  "tls10Enabled": "false",
  "tls11Enabled": "false",
  "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, and RADIUS authentication.

- Only one of the two factor user authentication methods can be specified for an Edge Service. In addition, Unified Access Gateway allows fallback authentication with a combination of Smart Card certificate and RADIUS authentication. Initially, UAG attempts to authenticate using Smart Card. If a certificate is not found, it will fall back to RADIUS authentication.
- Password authentication with Active Directory is the only authentication method that can be used with a deployment.
- You can modify a previously configured authentication setting. However, the authentication setting cannot be disabled. For example, if you have configured RADIUS authentication previously, you cannot disable the configuration. Instead, the authentication method can be changed to a different method such as Passthrough.

Read the following topics next:

- 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
- 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 Workspace ONE Access, authentication is always passed through Unified Access Gateway to the Workspace ONE Access 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 Unified Access Gateway admin UI, navigate to the **Configure Manually** section and click **Select**.

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

3 Click the X.509 Certificate gearbox.

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**	To upload the certificate files, click **Select**. You can select multiple root CA and intermediate CA certificates that are encoded as DER or PEM. **Note** With version 2012 and later, UAG supports the configuration of multiple CA certificates with the same Subject DN. This multiple certificates support is useful when an updated CA issuer certificate is used with the same subject DN but a different key pair. This feature allows to use the old and the new CA certificates together to support client certificates issued by either. UAG uses the authority key identifier to identify the public key corresponding to the private key used to sign a certificate. This extension is used where an issuer has multiple signing keys (either due to multiple concurrent key pairs or due to changeover).
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.

Option	Description
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 the load-balancer is configured with SSL pass-through at the load balancer and not configured to terminate SSL. 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.

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.

   Use the default file type CER for the file that you want to export.

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

Configure RSA SecurID Authentication in 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 configured with Unified Access Gateway-specific information.
- Ensure that you have obtained the access key from the RSA SecurID Authentication Manager server.
- If you choose to use SSL certificates, you must have downloaded the required certificate from the RSA SecurID Authentication Manager server.

Procedure

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

2 In the **General Settings**, toggle the button to show the **Authentication Settings**.

3 Click the RSA SecurID gearbox icon.

4 Configure the **RSA SecurID** options and save this configuration.

Option	Action
Enable RSA SecurID	To enable the SecurID authentication, toggle the button.
Number of Authenticati on Attempts	Indicates the maximum number of authentication attempts allowed to RSA SecurID Authentication Manager. 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 this option with the same value for each RSA SecurID configuration. If the value is not the same, SecurID authentication fails.
Server Hostname	Enter the host name of the RSA SecurID Authentication Manager server. The host name can be either an individual server hostname or a load balancer hostname supporting load balancing and high availability requirements amongst multiple RSA SecurID Authentication Manager servers.
Port Number	Enter the port number for communication between Unified Access Gateway and RSA SecurID Authentication API requests. By default, the port number is `5555`.
Access Key	Enter the access key for RSA SecurID Authentication API requests.
SSL Certificate	Upload the SSL certificate of the RSA SecurID Authentication Manager server.
Hostname of UAG Connector Instance	Enter the host name or IP address of the Unified Access Gateway appliance as specified in the RSA Authentication Manager server's agent configuration.
Timeout (seconds)	Enter the time in seconds after which a SecurID authentication attempt to RSA SecurID Authentication Manager server times out.

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	Turn on this toggle 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. The **Max Server Timeout** value depends on the RADIUS Servers configured. ■ If only primary RADIUS server is configured, `Number of attempts to RADIUS server * Server Timeout in Seconds <= 120 seconds`. ■ If both primary and secondary RADIUS server is configured, `2 * Number of attempts to RADIUS server * Server Timeout in Seconds <= 120 seconds`.
Radius Server Host name *	Enter the host name or the IP address of the RADIUS server.
Authentication Port*	Enter the Radius authentication port number. The port is usually 1812.
Realm Prefix	(Optional) The user account location is called the realm. If you specify a realm prefix string, the string is placed at the beginning of the user name when the name is sent to the RADIUS server. For example, if the user name is entered as jdoe and the realm prefix DOMAIN-A\ is specified, the user name DOMAIN-A\jdoe is sent to the RADIUS server. If you do not configure these fields, only the user name that is entered is sent.
Realm Suffix	(Optional) If you configure a realm suffix, the string is placed at the end of the user name. For example, if the suffix is *@myco.com*, the user name *jdoe@myco.com* is sent to the RADIUS server.
Name Id Suffix	Enter the NameId 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. The default text string is **Radius**. You can customize the labels for *username* and *passcode* in Horizon settings. For example, if this field is configured with **AD password first and then SMS passcode**, the login page message would read **Enter your Radius (For password: AD password first and then SMS passcode) user name and passcode**.

Option	Action
Enable basic MS-CHAPv2 validation	Turn on this toggle to enable basic MS-CHAPv2 validation. If this toggle turned on, then the additional validation of response from the RADIUS server is skipped. By default, full validation will be performed.
Enable secondary server	Turn on this toggle to configure a secondary RADIUS server for high availability. Configure the secondary server information as described in step 3.

4 Click **Save**.

Generate Unified Access Gateway SAML Metadata

You must generate SAML metadata on the Unified Access Gateway manament appliance and exchange metadata with the server to establish the mutual trust required for smart card authentication. For more information see, Deploying and Configuring Unified Access Gateway.

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.

Procedure

1 Log in to the Management Appliance and go to Configuration Templates

2 Click Add.

3 In the Advanced Settings section, click Configure.

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

5 Expand the **SAML Identity Provider Settings**

6 Select the **Provide Certificate** check box.

7 To add the Private Key file, click **Select** and browse to the private key file for the certificate.

8 For add the Certificate Chain file, click **Select** and browse to the certificate chain file.

9 Click **Done**.

10 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 management 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 management appliance 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.

Read the following topics next:

- Monitoring Edge Service Session Statistics
- Monitoring the SEG Health and Diagnostics
- 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
- Syslog Formats and Events
- Export Unified Access Gateway Settings
- Import Unified Access Gateway Settings
- Troubleshooting Errors: Content Gateway
- Troubleshooting High Availability
- Troubleshooting Security: Best Practices
- User Sessions Impacted by Changes in Unified Access Gateway Admin UI Settings
- Troubleshooting Unified Access Gateway Configuration for Horizon RSA SecurID Authentication

- Configurable Boot Time Commands for First Boot and Every Boot

Monitoring Edge Service Session Statistics

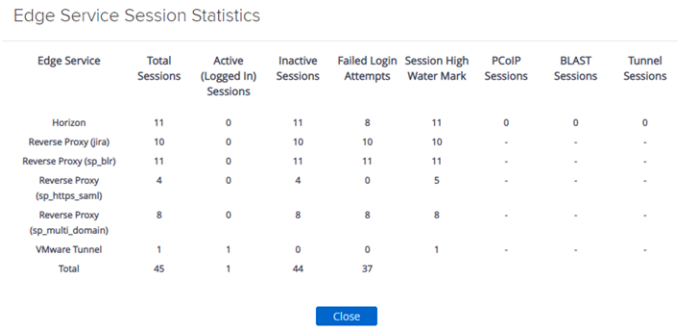
Unified Access Gateway provides information on active sessions of each edge service. You can quickly see that services you deployed are configured, up and running successfully from the admin UI for each Edge Service.

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.

  Note When Horizon sessions are launched from Horizon Universal Broker, the count for these sessions is not included in this number.

- **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	-	-	-
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. Generic Status and Stats

Attribute	Description
`date`	Indicates the date of statistics collected in the timezone of Unified Access Gateway appliance.
`version`	Indicates the current version of the Unified Access Gateway applicance running on the user's environment.
`uptimeInMins`	Indicates the time (in minutes) that Unified Access Gateway appliance is up and running.
`authenticatedSessionCount`	Indicates the overall count of authenticated sessions.
`sessionCount`	Indicates the overall count of the sessions.

Table 7-3. 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	
`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 7-4. 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**

Table 7-4. Web Reverse Proxy (continued)

Attribute	Description
`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 7-5. 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 Tunnelservice. 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 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.
`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.

Table 7-6. Unified Access Gateway Appliance

Attribute	Description
`cpuCores`	Indicates the number of processor cores assigned to the appliance.
`totalCpuLoadPercent`	Indicates the CPU load in percentage.
`totalMemoryMb`	Indicates the total memory in megabytes.
`freeMemoryMb`	Indicates the available unused memory in megabytes.

Table 7-6. Unified Access Gateway Appliance (continued)

Attribute	Description
`cpuDetailedStats`	Provides the detailed statistics of the CPU used. ■ `idle` - CPU does not perform any task. ■ `ioWait` - CPU waits for the disk input/output operations to complete. ■ `irq` - CPU allocated to hardware interrupts. ■ `nice` - CPU used to allocate multiple processes that demand more cycles than the CPU can provide. ■ `softIrq` - CPU services the soft interrupts. ■ `steal` - Xen hypervisor allocates cycles to other tasks. ■ `system` - CPU used by the operating system. ■ `user` - CPU used by the user applications.
`usedDiskSpacePercentage`	Indicates the disk usage in percentage.

Unified Access Gateway Session Flow For Horizon

To help you understand how the session statistics change in a Unified Access Gateway session for the Horizon edge service, a flow of events is described in this topic.

The session flow described here does not include any authentication method configured for Horizon in the Unified Access Gateway Admin UI.

Edge service health check occurs as per the value configured in **Monitor Interval**, an advanced system configuration setting in the Unified Access Gateway Admin UI.

To see definition about the session statistics mentioned here, see Monitoring Edge Service Session Statistics.

1 When the Horizon Client sends an XMLAPI request through Unified Access Gateway to the Horizon Connection Server, a new session is created in Unified Access Gateway.

   In the subsequent edge service health check, the session statistics have the following values:

Session statistics	Values
`Total Sessions`	1
`Active Sessions`	0
`Inactive Sessions`	1
`Failed Login Attempts`	0
`Session High Water Mark`	1

   After receiving the response from the Horizon Connection Server, Unified Access Gateway sends the response to the Horizon Client and an authentication prompt is displayed on the end user's device.

2 At the authentication prompt, the end user's action can vary. Depending on the action, the session statistics have different values.

a If an end user's authentication is successful, in the subsequent edge service health check, session statistics have the following values:

Session statistics	Values
`Total Sessions`	1
`Active Sessions`	1
`Inactive Sessions`	0
`Failed Login Attempts`	0
`Session High Water Mark`	1

b If an end user submits incorrect credentials for authentication, the change in session statistics depends on the number of login attempts, as allowed by the Horizon Connection Server.

- If the number of login attempts allowed is more than one, the session remains inactive until the number of login attempts reaches the maximum limit as allowed by the Horizon Connection Server.

  The `Failed Login Attempts` parameter increases by one for every failed login attempt.

  In the subsequent edge service health check, session statistics have the following values:

Session statistics	Values
`Total Sessions`	1
`Active Sessions`	0
`Inactive Sessions`	1
`Failed Login Attempts`	1
`Session High Water Mark`	1

- If the number of attempts allowed is only one, then the session is removed.

  Note When a session is removed, `Total Sessions` and `Inactive Sessions` decrease by one.

  In the subsequent edge service health check, session statistics have the following values:

Session statistics	Values
`Total Sessions`	0
`Active Sessions`	0

Session statistics	Values
Inactive Sessions	0
Failed Login Attempts	1
Session High Water Mark	1

c If an end user attempts to authenticate after the **Authentication Timeout** (a system configuration setting, configured in the Unified Access Gateway Admin UI), authentication fails and the session is removed.

In the subsequent edge service health check, session statistics have the following values:

Session statistics	Values
Total Sessions	0
Active Sessions	0
Inactive Sessions	0
Failed Login Attempts	1
Session High Water Mark	1

d If an end user cancels the authentication prompt, the session is not authenticated and remains in this state until the time from when the session was created exceeds the **Authentication Timeout**. When the **Authentication Timeout** is exceeded, the session expires.

Note Expired sessions are included as part of `Total Sessions` until the limit for the total number of sessions is reached. This limit depends on the sizing of the Unified Access Gateway appliance.

In the subsequent edge service health check, session statistics have the following values:

Session statistics	Values
Total Sessions	1
Active Sessions	0
Inactive Sessions	1
Failed Login Attempts	0
Session High Water Mark	1

3 After successful authentication, if VMware Tunnel is enabled in Unified Access Gateway and the Horizon Client is used, a tunnel session is created in Unified Access Gateway.

In the subsequent edge service health check, session statistics have the following values:

Session statistics	Values
Total Sessions	1
Active Sessions	1

Session statistics	Values
Inactive Sessions	0
Failed Login Attempts	0
Session High Water Mark	1
Tunnel Sessions	1 **Note** If Tunnel is disabled in Unified Access Gateway, then the value is 0.

4 Depending on the display protocol (PCOIP or Blast) selected by the end user for launching desktops or applications, the corresponding protocol's session statistics are affected.

For example, if Blast protocol is configured to be used, then in the subsequent edge service health check, session statistics have the following values:

Session statistics	Values
Total Sessions	1
Active Sessions	1
Inactive Sessions	0
Failed Login Attempts	0
Session High Water Mark	1
Tunnel Sessions	1
Blast Sessions	1
PCoIP Sessions	0

5 If the end user disconnects the launched desktop or application, then in the subsequent edge service health check, session statistics have the following values:

Session statistics	Values
Total Sessions	1
Active Sessions	1
Inactive Sessions	0
Failed Login Attempts	0
Session High Water Mark	1
Tunnel Sessions	1
Blast Sessions	0
PCoIP Sessions	0

6 End-user logout can occur due to various reasons such as user-initiated logout, inactivity after user authentication, or session expiry. When the end user is logged out, in the subsequent edge service health check, session statistics have the following values:

Session statistics	Values
`Total Sessions`	0
`Active Sessions`	0
`Inactive Sessions`	0
`Failed Login Attempts`	0
`Session High Water Mark`	1
`Tunnel Sessions`	0
`Blast Sessions`	0
`PCoIP Sessions`	0

Monitoring the SEG Health and Diagnostics

You can use the SEG V2 Admin page to monitor the health and diagnostics of your SEG.

The following procedure describes the steps to view the SEG health and diagnostics information.

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

2 Click the **Edge Service Session Statistics** gearbox icon, in the **Support Settings** section.

3 Click **Active** to open the SEG Health and Diagnostics monitoring screen.

The SEG diagnostics screen provides the following options to the user:

- View or download the SEG diagnostic JSON.
- Look up the specific policy from the SEG cache.
- Archive and download the SEG cached policies, redirect mappings, and diagnostic information.
- Clear redirect mappings from the SEG cache.

SEG Diagnostic APIs

The following table describes the API path and parameters for accessing the SEG diagnostics information.

SEG Diagnostics URL: GET https://<UAGIP>:9443/rest/v1/monitor/seg/diagnostics/<apiPath>.

API Path	Description
Diagnostic	View the SEG diagnostic JSON.
`policy/device/<easDeviceId>`	Look up the device policy for a given EAS device ID.

API Path	Description
`policy/account/<accountId>`	Look up the policy for a given user or group using the account ID.
`policy/easdevicetype/<easdevicetype>`	Look up the policy for a given EAS device type.
`policy/mailclient/<mailclientname>`	Look up the policy for a given mail client.
`cache/archive`	Archive and download the SEG cached policies, redirect mappings, and diagnostic information.
`policy/account/<accountId>`	Look up the device policy for a given EAS device ID.

The following table lists the APIs for clearing the redirect mappings from the SEG cache.

Clear Redirect Cache Mappings URL: DELETE https://<UAGIP>:9443/rest/v1/monitor/seg/cache/<parameter>

Parameter	Description
451	Clear 451 redirect mappings from the SEG cache.
302	Clear 302 redirect mappings from the SEG cache.

SEG Health APIs

The following table describes the SEG health statistic response attributes.

SEG Health URL: GET https://<UAGIP>:9443/rest/v1/monitor/seg/healthStats

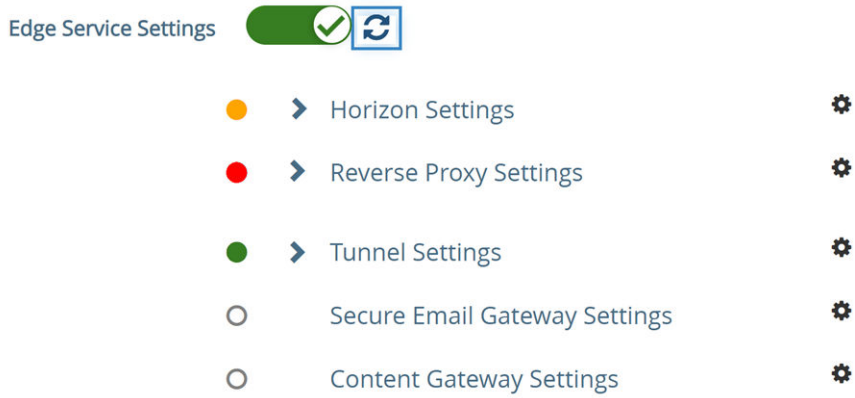
Response Attribute	Description
diagnosticExportTime	Specify the time of generation of the statistics, in milliseconds, since the UNIX epoch time.
apiConnectivity	Status of connectivity from the SEG to the API server. The status value can be **Success** or **Failed**.
policyDataLoaded	Status of the policy data loading into the SEG cache. The status value can be **Success**, **In Progress**, or **Failed**.
totalDevicePolicyCount	Specify the count of the device policies loaded into the SEG cache.
lastPolicyPartialUpdate	Specify the time of the latest successful partial policy update execution, in milliseconds, since the UNIX epoch time.
lastPolicyFullUpdate	Specify the time of the latest successful policy update execution, in milliseconds, since the UNIX epoch time.
lastPolicyDeltaUpdate	Specify the time of the latest delta policy update execution, in milliseconds, since the UNIX epoch time.
policyDeltaSyncEnabled	Flag to indicate if the policy delta sync is enabled.

Response Attribute	Description
emailServerConnectivity	Status of connectivity from the SEG to the API server. The attribute values can be **Success** or **Failed**.
requestsSinceSEGstartup	Number of ActiveSync requests since the SEG server was launched.
lastHourRequests	Number of ActiveSync requests in the last one hour.
last24hourRequests	Number of ActiveSync requests in the last 24 hours.
syncStat ■ count ■ latency	Specify the corresponding statistics to the **Sync** requests. ■ Request count for the last one hour duration. ■ Average latency for the last 24 hours duration.
itemOperationsStat ■ count ■ latency	Specify the corresponding statistics to the **itemOperations** requests. ■ Request count for the last one hour duration. ■ Average latency for the last 24 hours duration.
sendMailStat ■ count ■ latency	Specify the corresponding statistics to the **sendMail** requests. ■ Request count for the last one hour duration. ■ Average latency for the last 24 hours duration.
smartForwardStat ■ count ■ latency	Specify the corresponding statistics to the **smartForward** requests. ■ Request count for the last one hour duration. ■ Average latency for the last 24 hours duration.
smartReplyStat ■ count ■ latency	Specify the corresponding statistics to the **smartReply** requests. ■ Request count for the last one hour duration. ■ Average latency for the last 24 hours duration.
clusteringEnabled	Flag to indicate if the clustering is enabled.
nodesOnline	List of nodes that are active in the cluster.
nodesOffline	List of nodes that are listed in the MEM configuration, but not active in the cluster.
nodesSynchronized	Flag to indicate if all the nodes in the cluster are in synchronization.

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 version 1.2 is 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 Workspace ONE Access

After deploying Unified Access Gateway as a web reverse proxy from Workspace ONE Access, 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 Workspace ONE Access 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 Workspace ONE Access 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.

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 in the appropriate OPSWAT page. For more information, see OPSWAT documentation.

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.

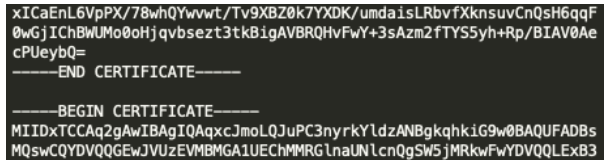
Unified Access Gateway displays "The request timed out while connecting to the host `https://gears.opswat.com`"

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.
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 7-3. 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:

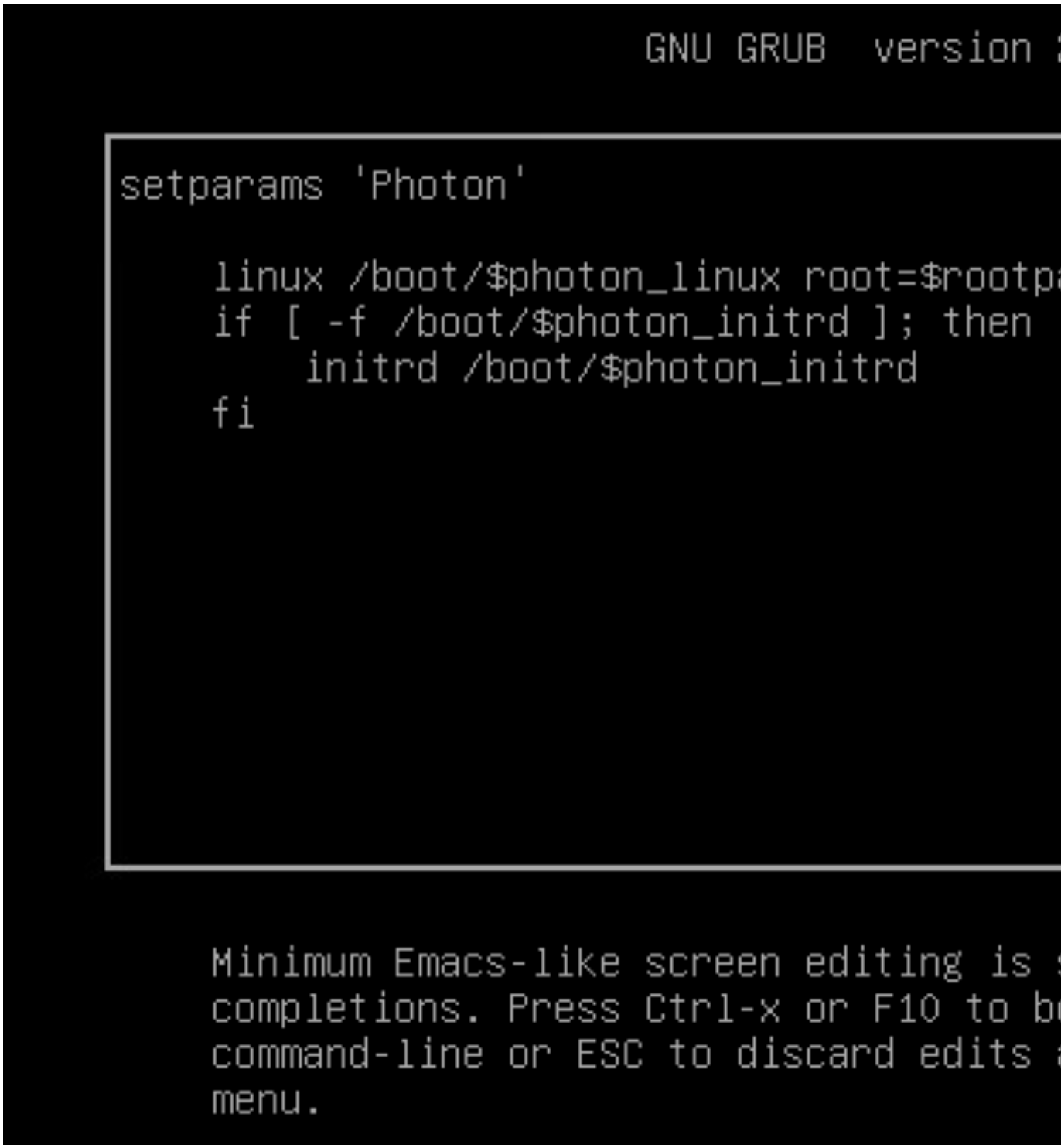
- have login access to vCenter
- know the vCenter login password
- have permission to access the appliance console

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, change the line that starts with `linux` so that it contains `linux /boot/$photon_linux root=$rootpartition rw init=/bin/bash`. After changing this line, 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`

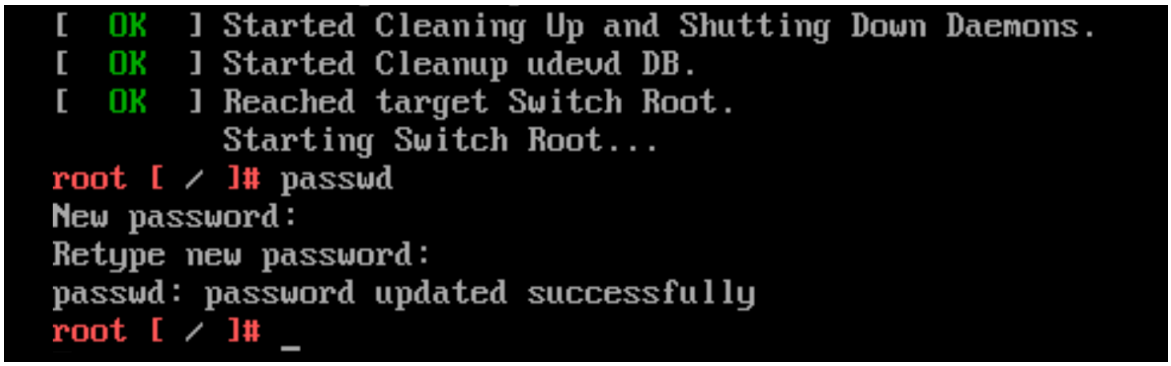
4 Press the F10 key and at the bash command prompt enter **passwd** to change the password.

```
passwd

New password:

Retype new password:

passwd: password updated successfully
```



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. This `ZIP` file contains all logs from your Unified Access Gateway appliance.

Set the Logging Level

You can configure log levels for the entire Unified Access Gateway appliance or only for specific Unified Access Gateway components such as the Horizon edge service (and sub-components), admin UI, and Web Reverse Proxy. The log levels that can be generated are ERROR, WARN, INFO, DEBUG, and TRACE.

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

Table 7-7. 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 might 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.
TRACE	Indicates information such as collection of Unified Access Gateway statistics, details of requests sent from Unified Access Gateway to backend servers and so on.

To configure these log level settings, see Configure Log Level Settings in Unified Access Gateway.

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 7-8. Files That Contain System Information to Aid in Troubleshooting

Filename	Description	Linux Command (if applicable)
`version.info`	Contains the versions of the OS, Kernel, GCC, and 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 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`

Table 7-8. Files That Contain System Information to Aid in Troubleshooting (continued)

Filename	Description	Linux Command (if applicable)
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
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)	
system_logs_archive	Directory contains the following log files: cpu.info, mem.info, sysctl.log, and journalctl_archive.	
cpu.info	Contains CPU information of the virtual machine collected from /proc/cpuinfo.	
mem.info	Contains information about the virtual machine memory such as total memory available, free memory available, and so on collected from /proc/meminfo.	
sysctl.log	Contains information about all the kernel parameters of the virtual machine.	sysctl -a
journalctl_archive	Files contain journalctl log information that spans over 7 days until the time at which the archive is downloaded. For example, if an admin downloads the Logs Archive from the Unified Access Gateway Admin UI at 9 A.M. today then the archive contains information for the past 7 days including until 9 A.M. If the size of the logs collected is less than or equal to 25 MB, then only a single file, journalctl.log, is generated. If the size of the logs collected is more than 25 MB, then the journalctl_archive folder is created with multiple journalctl.log files.	journalctl -x --since '1 week ago'
journald.conf	Contains configuration information for the journalctl logs.	
system-logs-collection-status.log	Contains information that indicates whether the following log files are successfully collected: cpu.info, mem.info, sysctl.log, and journalctl_archive.	
hosts	Contains the /etc/hosts entries.	
firstboot	Contains information that is generated when the Unified Access Gateway is booted for the first time.	

Table 7-8. Files That Contain System Information to Aid in Troubleshooting (continued)

Filename	Description	Linux Command (if applicable)
subsequentboot	Contains information that is generated during subsequent reboots of Unified Access Gateway.	
trustedCertificatesStore.log	Contains information about the certificate processing status when a trusted certificate is uploaded on Unified Access Gateway.	
vami-ovf.log	Contains configuration-related information such as OVF properties, network, and so on of the Unified Access Gateway appliance during deployment.	

Table 7-9. Log Files for Unified Access Gateway

Filename	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	One or more Edge service manager logs, 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.	

Table 7-9. Log Files for Unified Access Gateway (continued)

Filename	Description	Linux Command (if applicable)
package-updates.log	Contains log messages about the status of package updates (OS and Unified Access Gateway) applied to a Unified Access Gateway version, which has already been released and deployed in your environment.	
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 to see this log.	
tunnel_snap.log	Contains information that indicates whether the VMware Tunnel server and proxy logs are collected successfully.	
tunnel-snap.tar.gz	Tarball containing VMware Tunnel server and proxy logs.	
appliance-agent.log	Appliance agent (for starting up Workspace ONE UEM services) logs.	
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.

Table 7-10. Log Rotation Information for Unified Access Gateway Log Files

Log filename	Location	Property
admin-zookeeper.log	/opt/vmware/gateway/conf/log4j-admin.properties	log4j.appender.zookeeper.MaxFileSize=10MB log4j.appender.zookeeper.MaxBackupIndex=5
admin.log	/opt/vmware/gateway/conf/log4j-admin.properties	log4j.appender.default.MaxFileSize=10MB log4j.appender.default.MaxBackupIndex=5
audit.log	/opt/vmware/gateway/conf/log4j-admin.properties	log4j.appender.adminAudit.MaxFileSize=10MB log4j.appender.adminAudit.MaxBackupIndex=5
authbroker.log	/opt/vmware/gateway/conf/log4j-authbroker.properties	appender.rollingFile.policies.size.size=10MB appender.rollingFile.strategy.max=5
bsg.log	/opt/vmware/gateway/lib/bsg/absg.properties	logFilesize=8*1024*1024 logBackupCount=5

Table 7-10. Log Rotation Information for Unified Access Gateway Log Files (continued)

Log filename	Location	Property
esmanager.log	/opt/vmware/gateway/conf/log4j-esmanager.properties	log4j.appender.default.MaxFileSize=25MB log4j.appender.default.MaxBackupIndex=10
tunnel.log	/opt/vmware/gateway/conf/log4j-tunnel.properties	log4j.appender.default.MaxFileSize=25MB log4j.appender.default.MaxBackupIndex=5
Files present at /var/log/journal	/etc/systemd/journald.conf	SystemMaxUse=1G
keepalived.log	/etc/logrotate.d/keepalived	rotate 5 size 5M
haproxy.log	/etc/logrotate.d/haproxy	rotate 5 size 25M
auth.log	/etc/logrotate.d/auth	rotate 10 size 10M
audit.log	/etc/logrotate.d/audit **Note** /var/log/audit/audit.log contains events of the linux auditing service (auditd)	rotate 10 size 10M
/var/log/messages /var/log/cron	/etc/logrotate.d/messages_and_cron	rotate 20 size 50M maxage 30

Configure Log Level Settings in Unified Access Gateway

Administrators can apply log levels to specific Unified Access Gateway components or sub-components in addition to the entire Unified Access Gateway appliance. By applying log levels to specific components, you can control the amount of log information generated and you have only the relevant information.

Log levels determine the type of information collected. These levels help you collect information messages, errors and warnings, and events that help in debugging issues related to the Unified Access Gateway appliance.

Note Log levels can also be applied to a specific named class or a package in the Unified Access Gateway appliance. This functionality is an advanced setting and must be used as advised by VMware Support only.

For more information about log files, supported log levels, and the type of information collected for each log level, see Collecting Logs from the Unified Access Gateway Appliance.

Procedure

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

2 Navigate to **Support Settings > Log Level Settings**.

3 On the **Log Level Settings** window, configure the log level for the desired Unified Access Gateway component and sub-component.

   a In the first drop-down box, select the component and sub-component.

      - `All` indicates that the configured log level is applied to the entire Unified Access Gateway appliance.
      - `Admin` indicates that the configured log level is applied to the admin UI component of Unified Access Gateway.
      - `Horizon Edge Service` has sub-components such as `XMLAPI`, `BLAST`, `TUNNEL`, and so on.

        A log level can be applied to the entire Horizon edge service by choosing `Horizon Edge Service-All`.

      For a complete list of supported components and sub-components, see the Unified Access Gateway admin UI.

   b In the second drop-down box, select the log level.

      DEBUG and TRACE log levels must be applied only during troubleshooting as these levels can reduce performance and increase the verbose log messages. After you complete troubleshooting using the DEBUG or TRACE log levels, the log level must be reset to INFO or the component or sub-component must be removed.

   You can configure multiple log level settings for the supported components and sub-components of Unified Access Gateway.

   For example: If you can select the component as `All` and log level as `INFO`, then you can collect information messages that highlight the progress of the Unified Access Gateway services for the entire appliance. In addition to this setting, you can configure another log level, `ERROR` for the entire Horizon edge service or for specific sub-components such as `BLAST`, `TUNNEL`, and so on.

4 Click **Save**.

Syslog Formats and Events

The Syslog server logs events that occur on the Unified Access Gateway appliance. These events are captured in log files that have a specific format. To help you understand some of the information captured when the events are generated, this topic lists the events, event samples, and the syslog formats.

Syslog Format

Syslog audit events are logged in the `audit.log` and syslog events are logged in the `admin.log` and `esmanager.log` files. All log files follow a certain format.

The following tables list the log files (`audit.log`, `admin.log`, and `esmanager.log`), their respective formats, and field descriptions:

Note The generated events follow the log format; however, the events might contain only some of the fields present in the format.

Log File	Log Format
■ audit.log ■ admin.log	`<timestamp> <UAG hostname> <app name> <thread id> <log level> <file name> <function name> <line no.> <log message>`
esmanager.log	`<timestamp> <UAG hostname> <app name> <thread id> <log level> <file name> <function name> <line no.> <client IP> <username> <session type> <session id> <log message>`

Field	Description
`<timestamp>`	Indicates the time at which the event was generated and logged in the syslog server.
`<UAG hostname>`	Hostname of the Unified Access Gateway appliance.
`<appname>`	Application that generates the event. **Note** Depending on the log file, the values of this field are as follows: `UAG-AUDIT`, `UAG-ADMIN`, and `UAG-ESMANAGER`.
`<thread id>`	ID of the thread in which the event gets generated.
`<log level>`	Type of information collected in the log message. For more information about logging levels, see Collecting Logs from the Unified Access Gateway Appliance.
`<file name>`	Name of the file from which the log is generated.
`<function name>`	Name of the function in that file from which the log is generated.
`<line no.>`	Line number of the log in the file.
`<client IP>`	IP Address of the component (such as Horizon Client, load balancer, and so on) that sends a request to Unified Access Gateway appliance.

Field	Description
`<session type>`	Edge service (such as Horizon and Web Reverse Proxy) for which the session is created. If the session is for Web Reverse Proxy, the session type is mentioned as WRP- *<instanceId>*. **Note** *<instanceId>* is the instance ID of the Web Reverse Proxy edge service.
`<session id>`	Unique identifier of the session.
`<log message>`	Provides a summary about what has occurred in the event.

Syslog Audit Events

The following table describes the audit events with examples:

Event Description	Event Sample
Events are logged when an admin logs into the Unified Access Gateway Admin UI, performs configuration changes within the Admin UI, logs out of the Admin UI, and at login failure. Events are logged when a session is created at user login and when a session is destroyed after user logout.	■ `Sep 8 08:50:04 UAG Name UAG-AUDIT: [qtp1062181581-73]INFO utils.SyslogAuditManager[logAuditLog: 418] - LOGIN_SUCCESS: SOURCE_IP_ADDR=Client_Machine_IP_Address USERNAME=admin` ■ `05/20 14:03:59,288 INFO: SESSION_CREATED: SOURCE_IP_ADDR=Client_Machine_IP_Address: USERNAME=admin: INFO=HttpSession@1165374987, Active session count for this user is 1` ■ `Sep 8 08:50:13 UAG Name UAG-AUDIT: [qtp1062181581-79]INFO utils.SyslogAuditManager[logAuditLog: 418] - LOGOUT_SUCCESS: SOURCE_IP_ADDR=Client_Machine_IP_Address USERNAME=admin` ■ `Sep 8 08:50:13 tunneltest UAG-AUDIT: [qtp1901824111-61]INFO utils.SyslogAuditManager[logAuditLog: 452] - LOGIN_FAILED: SOURCE_IP_ADDR=Client_Machine_IP_Address USERNAME=admin: REASON=Incorrect Password. 2 attempts are remaining.` ■ `05/20 14:07:46,841 INFO: SESSION_DESTROYED: SOURCE_IP_ADDR=Client_Machine_IP_Address: USERNAME=admin: INFO=HttpSession@1165374987, Active session count for this user is 0` ■ `Sep 8 08:52:24 UAG Name UAG-AUDIT: [qtp1062181581-80]INFO utils.SyslogAuditManager[logAuditLog: 418] - CONFIG_CHANGE: SOURCE_IP_ADDR=Client_Machine_IP_Address USERNAME=admin: CHANGE=allowedHostHeaderValues:(null->) - tlsSyslogServerSettings:(null->[]) - dns: (null->) - sshPublicKeys:(null->[]) - ntpServers:(- null->) - adminPasswordExpirationDays:(90->50) - dnsSearch:(null->) - fallBackNtpServers: (null->) -` ■ `Sep 8 07:32:01 UAG Name UAG-ADMIN: [qtp1062181581-27]INFO utils.SyslogManager[save: 57] - SETTINGS:CONFIG_CHANGED:allowedHostHeaderVal ues:(null->) - tlsSyslogServerSettings: (null->[]) - dns:(null->) - sessionTimeout: (9223372036854775807->36000000) - sshPublicKeys:(null->[]) - ntpServers:(null- >) - dnsSearch:(null->) - fallBackNtpServers:(null->) -`

Event Description	Event Sample
	■ 08/22 13:52:22,815 INFO: CONFIG_CHANGE: SOURCE_IP_ADDR=*Client_Machine_IPAddress*: USERNAME=admin: CHANGE=httpproxyalias SSL_CERTIFICATE_METHOD_SETTINGS:CONFIG_CHANGED:certificate updated. OldValue:*[Subject, Issuer, SerialNumber, Expiry and SHA1 thumbprint details of existing certificate]*, NewValue:*[Subject, Issuer, SerialNumber, Expiry and SHA1 thumbprint details of new certificate]*

Syslog Events

The following table describes the system events with examples:

Event Description	Event Sample
An event is logged when any of the edge services configured within the Unified Access Gateway are started and stopped accordingly.	In the following event samples, *UAG Name* is the option which is configured as part of Unified Access Gateway's **System Configuration** in the Admin UI: ■ Sep 9 05:36:55 *UAG Name* UAG-ESMANAGER: [Curator-QueueBuilder-0]INFO utils.SyslogManager[start: 355][][][][] - Edge Service Manager : started ■ Sep 9 05:36:54 *UAG Name* UAG-ESMANAGER: [Curator-QueueBuilder-0]INFO utils.SyslogManager[stop: 1071][][][][] - Edge Service Manager : stopped
Events are logged when the Web Reverse Proxy settings are enabled or disabled on the Unified Access Gateway Admin UI.	■ Sep 8 09:34:52 *UAG Name* UAG-ESMANAGER: [main-EventThread]INFO utils.SyslogManager[stopService: 287][][][][] - Reverse Proxy Edge Service with instance id 'wiki' : stopped ■ Sep 8 12:08:18 *UAG Name* UAG-ESMANAGER: [main-EventThread]INFO utils.SyslogManager[startService: 211][][][][] - Reverse Proxy Edge Service with instance id 'wiki' : started

Event Description	Event Sample
Events are logged when the Horizon edge service settings are enabled or disabled on the Unified Access Gateway Admin UI.	■ `Sep 8 09:15:21 UAG Name UAG-ESMANAGER: [main-EventThread]INFO utils.SyslogManager[startService: 335][][][][] - Horizon Edge Service : started` ■ `Sep 8 09:15:07 UAG Name UAG-ESMANAGER: [main-EventThread]INFO utils.SyslogManager[stopService: 702][][][][] - Horizon Edge Service : stopped`
Events are logged when a Horizon session is established which constitutes of session creation, user login, user authentication, desktop start, and session termination.	While multiple events are logged through the flow, sample events include login scenarios, user authentication success and failure scenarios, and authentication timeout. In one of the samples, Horizon has been configured with the `RADIUS` authentication method: ■ `Sep 8 07:28:46 UAG Name UAG-ESMANAGER: [nioEventLoopGroup-46-1]INFO utils.SyslogManager[write: 163][Client_Machine_IP_Address][][][5a0b-***-7cfa] - Created session : 5a0b-***-7cfa` ■ `Sep 8 07:28:51 UAG Name UAG-ESMANAGER: [nioEventLoopGroup-46-1]INFO utils.SyslogManager[putUserNameInMDC: 494][Client_Machine_IP_Address][testradius][Horizon][5a0b-***-7cfa] - UAG sessionId:5a0b-***-7cfa username:testradius` ■ `Sep 8 07:28:51 UAG Name UAG-ESMANAGER: [jersey-client-async-executor-1]INFO utils.SyslogManager[logMessage: 190][Client_Machine_IP_Address][testradius][Horizon][5a0b-***-7cfa] - Authentication successful for user testradius. Auth type: RADIUS-AUTH, Sub type: passcode` ■ `Sep 8 07:28:52 UAG Name UAG-ESMANAGER: [nioEventLoopGroup-46-1]INFO utils.SyslogManager[processDocument: 110][Client_Machine_IP_Address][testradius][Horizon][5a0b-***-7cfa] - Authentication attempt response - partial` ■ `Sep 8 07:29:02 UAG Name UAG-ESMANAGER: [nioEventLoopGroup-46-1]INFO utils.SyslogManager[putUserNameInMDC: 494][Client_Machine_IP_Address][user name][Horizon][5a0b-***-7cfa] - UAG sessionId:5a0b-***-7cfa username:user name` ■ `Sep 8 07:29:02 UAG Name UAG-ESMANAGER: [nioEventLoopGroup-46-1]INFO utils.SyslogManager[processXmlString: 190][Client_Machine_IP_Address][user name][Horizon][5a0b-***-7cfa] - Authentication attempt - LOGIN initiated`

Event Description	Event Sample
	■ Sep 8 07:29:03 *UAG Name* UAG-ESMANAGER: [nioEventLoopGroup-46-1]INFO utils.SyslogManager[processDocument: 110] [*Client_Machine_IP_Address*][*user name*] [Horizon][5a0b-***-7cfa] - Authentication attempt response - ok ■ Sep 8 07:29:03 *UAG Name* UAG-ESMANAGER: [nioEventLoopGroup-46-1]INFO utils.SyslogManager[setAuthenticated: 384][*Client_Machine_IP_Address*][*user name*][Horizon][5a0b-***-7cfa] - HORIZON_SESSION:AUTHENTICATED:Horizon session authenticated - Session count:9, Authenticated sessions: 2 ■ Sep 8 07:29:04 *UAG Name* UAG-ESMANAGER: [nioEventLoopGroup-41-1]INFO utils.SyslogManager[onSuccess: 109] [*Client_Machine_IP_Address*][*user name*] [Horizon][5a0b-***-7cfa] - Horizon Tunnel connection established ■ Sep 8 07:29:16 *UAG Name* UAG-ESMANAGER: [nioEventLoopGroup-46-1]INFO utils.SyslogManager[resolveHostName: 234] [*Client_Machine_IP_Address*][*user name*] [Horizon][5a0b-***-7cfa] - Accessing virtual/rdsh desktop using protocol BLAST with IP Address *IP_Address* ■ Sep 8 07:29:16 *UAG Name* UAG-ESMANAGER: [nioEventLoopGroup-42-1]INFO utils.SyslogManager[onSuccess: 293] [*Client_Machine_IP_Address*][*user name*] [Horizon][5a0b-***-7cfa] - BSG route 5504-***-2905 with auth token Ob6NP-***-aEEqK added ■ Sep 8 07:29:55 *UAG Name* UAG-ESMANAGER: [nioEventLoopGroup-46-1]INFO utils.SyslogManager[terminateSession: 450][*Client_Machine_IP_Address*][*user name*][Horizon][5a0b-***-7cfa] - HORIZON_SESSION:TERMINATED:Horizon Session terminated due to logout - Session count:9, Authenticated sessions: 2

System Messages Sent to Syslog Server

The following table describes the events that are generated when system messages are sent to the syslog server:

Event Description	Event Sample

Events are logged when the root user logs into the Unified Access Gateway virtual machine console, logs out of the console, and at authentication failure.	■ `May 10 07:39:44 UAG Name login[605]: pam_unix(login:session): session opened for user root by (uid=0)`
	`May 10 07:39:44 UAG Name systemd-logind[483]: New session c14 of user root.`
	`May 10 07:39:44 UAG Name login[10652]: ROOT LOGIN on '/dev/tty1'`
	■ `May 10 07:46:24 UAG Name login[605]: pam_unix(login:session): session closed for user root`
	`May 10 07:46:24 UAG Name systemd-logind[483]: Session c14 logged out. Waiting for processes to exit.`
	`May 10 07:46:24 UAG Name systemd-logind[483]: Removed session c14.`
	■ `May 10 07:39:08 UAG Name login[605]: pam_unix(login:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/tty1 ruser= rhost= user=root`
	`May 10 07:39:12 UAG Name login[605]: FAILED LOGIN (1) on '/dev/tty1' FOR 'root', Authentication failure`

Events are logged when the root user logs into and logs out of Unified Access Gateway using SSH and at authentication failure.	■ `May 10 04:30:40 UAG Name sshd[2880]: Accepted password for root from Client_Machine_IP_Address port 53599 ssh2`
	`May 10 04:30:40 UAG Name sshd[2880]: pam_unix(sshd:session): session opened for user root by (uid=0)`
	`May 10 04:30:40 UAG Name systemd-logind[483]: New session c2 of user root.`
	■ `Jun 11 09:53:34 BVT_NONFIPS sshd[2852]: pam_unix(sshd:session): session closed for user root`
	`Jun 18 05:47:13 rootPasswd sshd[6857]: Received disconnect from Client_Machine_IP_Address port 31389:11: disconnected by user`
	`Jun 18 05:47:13 rootPasswd sshd[6857]: Disconnected from user root Client_Machine_IP_Address port 31389`
	`Jun 18 05:45:12 rootPasswd sshd[6772]: Failed password for root from Client_Machine_IP_Address port 31287 ssh2`

Events are logged when the CPU, memory, heap, or disk usage exceeds the threshold value on Unified Access Gateway	■ `Feb 2 08:28:35 uag-620c787e-440b-494e-91b2-54d2d8905c80 uag-esmanager: [Monitoring]WARN utils.SyslogManager[lambda$getConfiguredPerf`

Event Description	Event Sample
	ormanceCounters$2: 655][][][][] - UAGW00283: 93% of disk space usage is above threshold: 90% ■ Feb 2 08:31:16 uag-620c787e-440b-494e-91b2-54d2d8905c80 uag-esmanager: [Monitoring]WARN utils.SyslogManager[lambda$getConfiguredPerformanceCounters$2: 655][][][][] - UAGW00283: 100.0% of System CPU usage is above threshold 95% ■ Feb 2 08:34:17 uag-620c787e-440b-494e-91b2-54d2d8905c80 uag-esmanager: [Monitoring]WARN utils.SyslogManager[lambda$getConfiguredPerformanceCounters$2: 655][][][][] - UAGW00283: 99.0% of memory usage is above threshold: 95%

Secure Email Gateway

Secure Email Gateway is configured to follow the Syslog configurations which is configured as part of Unified Access Gateway System Settings. By default, only the contents of `app.log` in Secure Email Gateway is triggered as Syslog events.

For more information about the Syslog configurations, see Configure Unified Access Gateway System Settings.

VMware Tunnel

For more information, see *Access Logs and Syslog Integration* and *Configure VMware Tunnel* in the *VMware Workspace ONE UEM Product Documentation* at VMware Docs.

Export Unified Access Gateway Settings

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

You can export 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.

Note The exported files do not contain sensitive data such as shared secrets and passwords.

Due to security reasons, the keyTab information in the `UAG_Settings.json` file is cleared. If you choose to deploy a new Unified Access Gateway instance and you have uploaded KeyTab files in the old Unified Access Gateway instance, then after importing the `.json` file, you must upload the KeyTab files that were used in the old Unified Access Gateway instance. On the Import Settings window, you will be prompted to upload the KeyTab files. Hence, ensure that you keep these Keytab files easily accessible while uploading these files in the old Unified Access Gateway instance.

If you want to deploy Unified Access Gateway versions earlier than Unified Access Gateway 2106, by importing the exported `.json` settings from Unified Access Gateway 2106 or later, then after the import, you must once again upload the Keytab Files which were used in the old instance (Unified Access Gateway 2106 or later). This upload is done by navigating to the **Upload Keytab Files** section in the Unified Access Gateway instance's admin UI. Hence, ensure that you keep the Keytab files easily accessible when uploading the files in the older instances.

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 by clicking **Select** in the **Import Settings** section.
6. Click **Browse** and navigate to the previously exported JSON file and then click **Import**.

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.

1 Log into the Workspace ONE UEM console.

2 Navigate to the **Content Gateway Configuration** page.

3 In the **Custom Gateway Settings** section, click **Add Row**.

4 In the table displayed, enter the following values:

- **Key** = `aw.fileshare.jcifs.active`
- **Type**=`Boolean`
- **Value**=`true`

  The default value is `false`.

5 Click **Save**.

6 On the Unified Access Gateway Admin UI, navigate to the **Content Gateway Settings** page.

7 Click **Save**.

Note When the settings on the Unified Access Gateway Admin UI are saved, Content Gateway configuration is fetched from the Workspace ONE UEM console and the Content Gateway service is restarted.

For Content Gateway configuration changes to be effective, you must update the **Value** in the Workspace ONE UEM console and then save the Content Gateway settings in the Unified Access Gateway Admin UI.

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 primary
                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 7-11. 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 primary 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.

User Sessions Impacted by Changes in Unified Access Gateway Admin UI Settings

When certain Unified Access Gateway Admin UI settings are changed, the existing XMLAPI sessions (Unified Access Gateway sessions) might get terminated and so end users cannot access launched desktops and applications. The changed settings might affect only the launched desktops and applications or both XMLAPI and desktop or application sessions.

You must plan to change the Unified Access Gateway Admin UI settings during a maintenance window.

Admin UI Settings	Affects existing Unified Access Gateway session	Affects launched desktops and applications
Import Settings You can use this Admin UI section to import the previously exported `JSON` file (from the previous deployment) to configure a newly deployed version of the Unified Access Gateway appliance.	Yes	Yes
Horizon Settings		
Enable PCOIP	No	Yes
Enable Blast	No	Yes
Enable UDP Tunnel Server	No	Yes
Enable Tunnel	Yes	Yes
Disable Horizon edge service	Yes	Yes
Authentication Settings		
X.509 Certificate	Yes	Yes
System Configuration		
TLS Named Group	Yes	Yes
TLS Signature Schemes	Yes	Yes
SSL provider	Yes	Yes
Import JSON	Yes	Yes
Network Settings	Yes	Yes
High Availability Settings	Yes	Yes
TLS Server Certificate Settings (Internet facing interface only)	Yes	Yes

Troubleshooting Unified Access Gateway Configuration for Horizon RSA SecurID Authentication

You might experience configuration issues when setting up SecurID between Unified Access Gateway version 2111 and later and RSA Authentication Manager. You can use various procedures for diagnosing and fixing configuration issues.

Starting with Unified Access Gateway version 2111, support for RSA SecurID Authentication with RSA Authentication Manager (AM) Server uses the latest REST API. Earlier Unified Access Gateway versions used a configuration method based on an `sdconf.rec` file.

Common Issues

Firewall Block or Routing Issues

To communicate with the user's RSA AM Server, Unified Access Gateway uses the RSA SecurID client which connects on TCP port 5555. If there is a firewall in between that blocks this TCP port, or the RSA AM Server is not reachable, SecurID authentication fails. For more information, see KB 88002.

RSA API on RSA Authentication Manager is not enabled

By default, the **Enable Authentication API** setting is not enabled in the **RSA SecurID Authentication API** section of **RSA AM Server**. For more information, see KB 88003.

RSA AM Certificate issues with UAG 2111 and later

When configuring RSA SecurID on Unified Access Gateway, the SSL certificate on the RSA AM Server might not be trusted if it is a self-signed certificate, or a certificate not issued by a trusted Certificate Authority. In such scenarios, it is necessary to obtain the public certificate or issuer certificate from the RSA AM Server and upload it to Unified Access Gateway to allow this trust. For more information, see KB 88004.

FAIL reason-code: VERIFY_ERROR logged in UAG authbroker.log

When Unified Access Gateway performs an RSA SecurID authentication attempt against RSA AM Server with the credentials entered by the user, the outcome is logged in the `/opt/vmware/gateway/logs/authbroker.log` file included with the logs .zip set.

To grant access for the user, Unified Access Gateway must receive `CREDENTIAL_VERIFIED` response from RSA AM. However, there can be several scenarios when the response code returned is `VERIFY_ERROR`. For more information, see KB 88005.

Configurable Boot Time Commands for First Boot and Every Boot

Use these commands when you are deploying Unified Access Gateway and configuring shell commands to run on the first boot and every boot.

Caution This feature is restricted by guidelines to indicate VMware supported use cases only. VMware strictly recommends not to use these fields for running any other commands.

Example of the `INI` File

```
[General]
...
commandsFirstBoot=<commands_to_run>
commandsEveryBoot=<commands_to_run>
...
```

Configuration Parameter	Description
commandsFirstBoot	Semi-colon separated list of commands to be executed during the first boot of Unified Access Gateway . The maximum length of the commands is 8 kB.
commandsEveryBoot	Semi-colon separated list of commands to be executed during every boot of Unified Access Gateway. The maximum length of the commands is 8 kB.

Supported Use Cases

Enable the conventional DNS lookup for .local addresses instead of attempting mDNS

```
commandsFirstBoot=mkdir -p /etc/systemd/resolved.conf.d; chmod 755 /etc/systemd/
resolved.conf.d; echo -e "[Resolve]\nDomains=local\n" > /etc/systemd/resolved.conf.d/
DomainsLocal.conf; chmod 644 /etc/systemd/resolved.conf.d/DomainsLocal.conf; systemctl
restart systemd-resolved
```