Content Gateway

VMware Workspace ONE UEM 2011

vmware®

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

https://docs.vmware.com/

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

Contents

Introduction to the VMware Content Gateway

1

The Workspace ONE UEM powered by AirWatch provides VMware Content Gateway as a service on the Unified Access Gateway appliance. The VMware Content Gateway provides a secure and effective medium for end users to access internal repositories.

Using the VMware Content Gateway with VMware Workspace ONE Content provides levels of access to your corporate content. Your end users can remotely access their documentation, financial documents, board books, and more directly from content repositories or internal fileshares. As files are added or updated within your existing content repository, the changes immediately display in VMware Workspace ONE Content. Users are granted access to their approved files and folders based on the existing access control lists defined in your internal repository.

Note VMware Workspace ONE has announced the End of General Support for VMware Content Gateway for Windows and Linux, effective October 17, 2019. Content Gateway solution on Unified Access Gateway (UAG) has been supported since 2017 as an alternative to the standalone solution offered on Windows and Linux servers. For information about migrating Content Gateway to Unified Access Gateway, see *Migrating Content Gateway to Unified Access Gateway* documentation.

This chapter includes the following topics:

Architecture and Security of Content Gateway

Understand the architecture design and security features of VMware Content Gateway deployed as a service on the Unified Access Gateway appliance.

Deploying the Content Gateway as a service on the Unified Access Gateway eliminates manual configuration and maintenance of Content Gateway using security updates. The Unified Access Gateway appliance platform goes through multiple security audits and patches are provided for security vulnerabilities. For information about deploying Content Gateway as a service on Unified Access Gateway, see Unified Access Gateway System and Network Requirements section in the Deploying and Configuring VMware Unified Access Gateway guide available at docs.vmware.com.

VMware Content Gateway offers basic and relay-endpoint architecture models for deployment. Both configurations support load-balancing for high-availability and SSL offloading. Configure your VMware Content Gateway deployment in a way that best addresses your security needs and existing setup.

Consider using a load balancer in the DMZ to forward traffic on the configured ports to a Workspace ONE UEM component. Also, consider using dedicated servers to eliminate the risk of other web applications or services causing performance issues.

Content Gateway with Load Balancing

Workspace ONE UEM supports integration with a load balancer for improved performance and faster availability.

Successful integration requires some additional client-side configurations.

- Configure the proper network changes for the Content Gateway to access various internal resources over the necessary ports.
- Configure load balancers to persist a connection from a client to the same load balanced node with an algorithm of your selecting. Workspace ONE UEM supports simple algorithms such as Round Robin and more sophisticated ones such as Least Connections.
- Configure load balancers to **Send Original HTTP Headers** to avoid device connectivity problems. Content Gateway uses information in the request's HTTP header to authenticate devices.

Content Gateway Deployment Models

The VMware Content Gateway supports deploying a basic endpoint model or a relay-endpoint model. Use the deployment model that best fits your needs.

Both SaaS and on-premises Workspace ONE UEM environments support the basic and relay-endpoint deployment models. The VMware Content Gateway must have a publicly accessible endpoint for devices to connect to when making a request. Basic deployment models have a single instance of VMware Content Gateway configured with a public DNS. Alternatively, for the relay-endpoint deployment model, the public DNS is mapped to the relay server in the DMZ. This server communicates with the Device Services server. For SaaS deployments, Workspace ONE UEM hosts the API components in the cloud. For an on-premises environment, the API component is typically installed in the DMZ.

Content Gateway on Unified Access Gateway Architecture

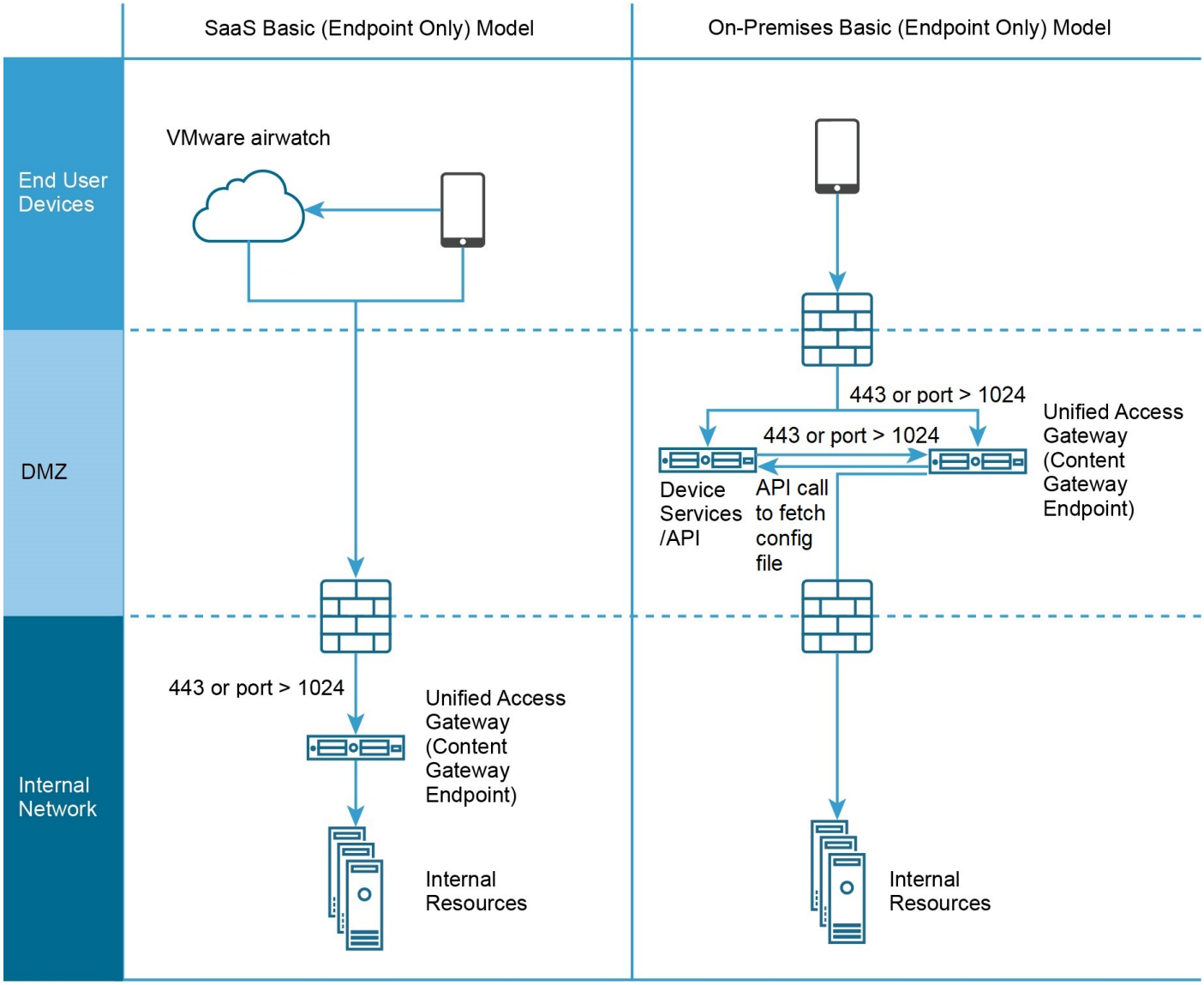
The VMware Content Gateway can be deployed using the basic endpoint model and the relay-endpoint model. These deployment models are supported on both SaaS and on-premises Workspace ONE UEM environments.

Basic Endpoint Deployment Model

The basic endpoint model has a single instance of the Content Gateway installed on the Unified Access Gateway appliance with a publicly available DNS. The Content Gateway is placed either in the internal network or DMZ. In the internal network, Content Gateway is placed behind a load balancer which is in the DMZ. The load balancer 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 API and Devices Services. Device Services connects the end-user device to the correct Content Gateway.

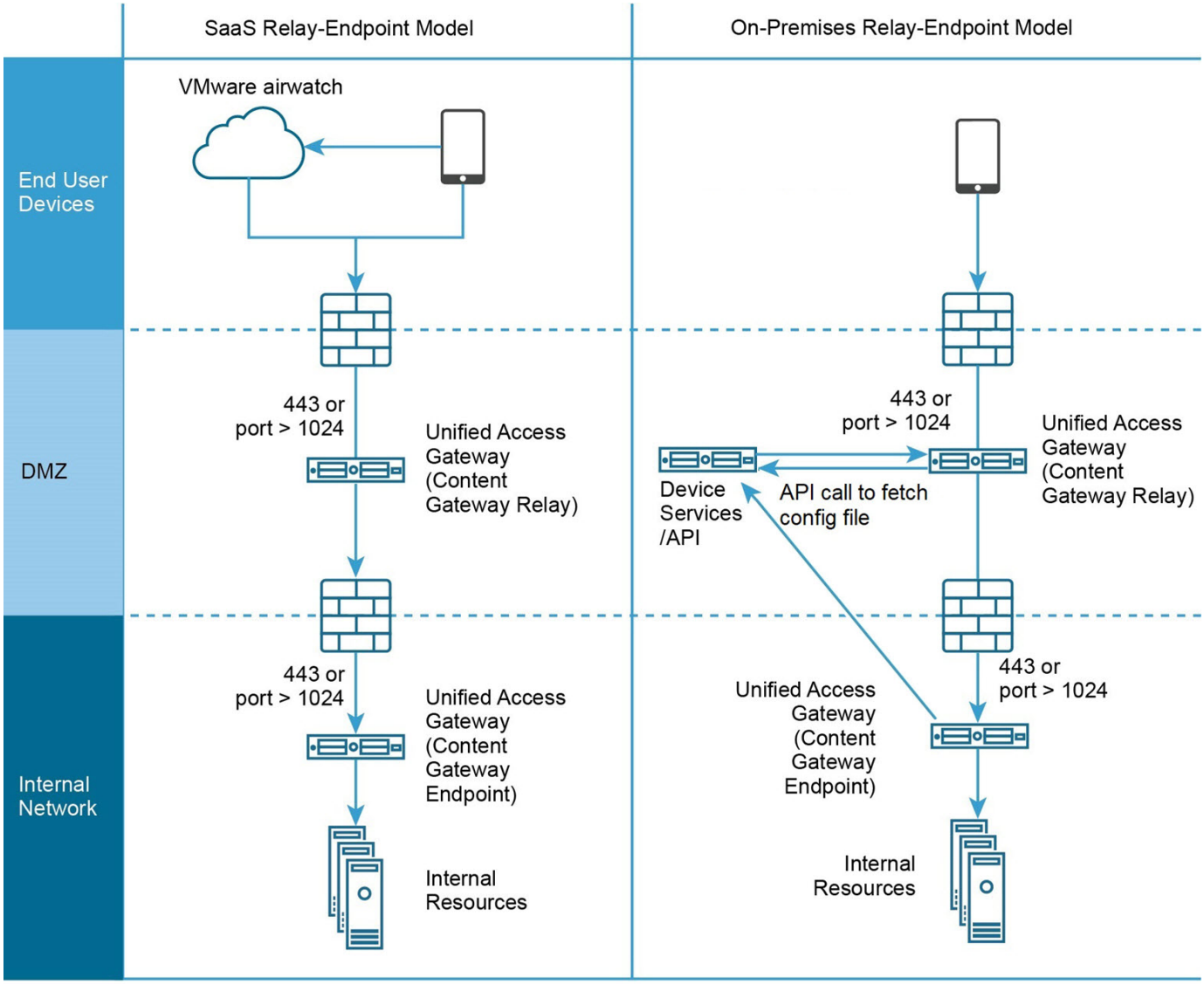
If the basic endpoint is installed in the DMZ, then proper network changes must be made for the VMware Content Gateway to access various internal resources over the necessary ports.



Relay-Endpoint Deployment Model

The relay-endpoint deployment model has 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. 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.

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.



Content Gateway Installation Preparation

Effective preparation includes evaluating the appropriateness of the Content Gateway solution for your organization, determining your deployment model, and considering the port requirements for your Content Gateway on the Unified Access Gateway.

There are no hardware or software requirements specific to Content Gateway on the Unified Access Gateway. For information about the hardware and software requirements for deploying the Unified Access Gateway, see *Unified Access Gateway System and Network Requirements* in the *Unified Access Gateway* documentation.

Port Requirements

Consider the port requirements for the basic and the relay endpoint configurations of Content Gateway when migrating to Unified Access Gateway.

Port Requirements for Content Gateway Basic Endpoint Configuration

Port	Protocol	Source	Destination	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 listens on port 10443.
443 or any port > 1024	HTTPS	Workspace ONE UEM Device Services	Unified Access Gateway Content Gateway Endpoint	If 443 is used, Content Gateway listens on port 10443.
443 or any port > 1024	HTTPS	Workspace ONE UEM console	Unified Access Gateway Content Gateway Endpoint	If 443 is used, Content Gateway listens 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

Port Requirements for Content Gateway Relay Endpoint Configuration

Port	Protocol	Source	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 listens 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 listens 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 listens on port 10443.
443 or any port > 1024	HTTPS	Workspace ONE UEM console	Unified Access Gateway Content Gateway Relay Server	If 443 is used, Content Gateway listens on port 10443.
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	

Port	Protocol	Source	Destination	Description
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

Deploy Content Gateway on Unified Access Gateway

Content Gateway deployment on Unified Access Gateway begins with providing the Unified Access Gateway (UAG) parameters to a configured node on the Workspace ONE UEM console.

Prerequisites

You must have an active deployment of the Unified Access Gateway either as an Appliance or using PowerShell to configure Content Gateway. For more information, see *Deploying Unified Access Gateway Appliance* and *Using PowerShell to Deploy Unified Access Gateway* in the *Unified Access Gateway* documentation.

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

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.

Custom Values for Content Gateway

The custom configuration values for the Content Gateway on Unified Access Gateway (UAG) can be set on the Workspace ONE UEM console. These custom values when fetched by the UAG server are automatically updated into the Content Gateway configuration files. The automatic updates eliminate the manual effort of updating the configuration files every time the UAG server undergoes an upgrade.

Custom values available on the Workspace ONE UEM console

The tabulated list contains the keys that are available on the UEM console.

Keys	Type	Value	Description	Supported UAG and CG version
aw.server.security-headers.hsts.enabled	Boolean	False	Allows HSTS support in CG.	UAG 3.9 (CG 2.11.0) and later
aw.fileshare.client.domain	String		Default domain with which the users are associated while accessing fileshare repositories.	UAG 3.9 (CG 2.11.0) and later

Keys	Type	Value	Description	Supported UAG and CG version
aw.http.cipher-suites	String	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA256	Comma separates list of allowed ciphers.	UAG 3.9 (CG 2.11.0) and later
aw.http.protocols	String	SSLv2Hello, SSLv2, SSLv3, TLSv1, TLSv1.1, TLSv1.2	Values can be separated by comma.	UAG 3.10 (CG 2.12.0) and later

Note The changes made after starting the Content Gateway service requires resaving of the service configuration on UAG.

Modifying the SMB Configurations

The SMB configurations are stored in `smb.conf` and `smb-connector.conf` files under the smb-connector directory at the Content Gateway installation path. To define precisely the custom values for these configuration files, you must obtain the current files from the UAG's log export functionality. A definite sequence is not followed when adding a new custom value to these configuration files. The new value when added appears at the end following all the existing values in the file.

Custom values can be provided in the UEM console using the following syntax:

```
extconf##FILE_NAME##CHANGE_TYPE[##EXISTING_LINE]=LINE_VALUE
```

- FILE_NAME = Name of the file; smb or smb-connector
- CHANGE_TYPE = ADD, REMOVE, or UPDATE
- EXISTING_LINE = The current content of the line that needs the required change. If the line is not found in the file, this entry in the Key Value Pair (KVP) is ignored and does not have any impact on the file. It is applicable if there is UPDATE or REMOVE.
- LINE_VALUE = Value of the line to be inserted or updated. It is ignored if there is REMOVE.

Listed are few examples of modifying the custom values in the SMB configuration files.

Example 1: An environment requires updating minimum smb protocol version from SMB2_02 to SMB3.

Key	Type	Value	Description
extconf##smb##UPDATE## client min protocol = SMB2_02	String	client min protocol = SMB3	Update the line in the smb.conf file that equals that client min protocol = SMB2_02 with client min protocol = SMB3

Example 2: Updating the smb-connector logs to debug mode. Default is 1 (error) and allowed values are: 0: Off, 1: Error, 2: Warning, 3: Info, 4: Debug

Key	Type	Value	Description
extconf##smb-connector##UPDATE##log_level 1	String	log_level 4	Update the line in the smb-connector.conf file that equals that “log_level 1” with “log_level 4”

Note All custom values must be provided as a String when inserting or updating the configuration and as Null when removing the configuration.

Modifying Application Log Levels

To update the application logging level to debug, the below KVP entry can be used. Info is the default level and the permitted values include Error, Warn, Info, Debug, and Trace.

Key	Type	Value	Description
extconf##logback##level##com.vmware	String	debug	Update the application logging level to debug.

Configure Content Gateway on Unified Access Gateway

Enable the Content Gateway settings and provide the configuration details required for configuring Content Gateway on Unified Access Gateway.

Procedure

1. Open the Unified Access Gateway Admin UI and navigate to **General Settings > Edge Service Settings > Content Gateway Settings** and click the gearbox icon.
2. Select **YES** to enable Content Gateway settings.
3. Configure the following settings and click **Save**.

Option	Description
Identifier	Indicates that this service is enabled.
API Server URL	The AirWatch API Server URL `[http[s]://]hostname[:port]` The destination URL must contain the protocol, host name or IP address, and port number. For example: https://load-balancer.example.com:8443. Unified Access Gateway pulls Content Gateway configuration from the API server.
API Server Username	User name to log into the API server. You must assign the Content Gateway role to the admin account.
API Server Password	Password to log into the API server.
Content Gateway Hostname	Host name used to configure edge settings.
Content Gateway Configuration GUID	VMware 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 Workspace ONE UEM console under **Settings > Content > Content Gateway**.
Outbound Proxy Host	The host where the outbound proxy is installed. If configured, the Unified Access Gateway makes a connection to API Server through an outbound proxy.
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.

Option	Description
Trusted Certificates	Add a trusted certificate to this edge service. Select '**+**' to select a certificate in the PEM format and add to the trust store. Select '**-**' to remove a certificate from 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.
Host Entries	Enter the details to be added in the /etc/hosts file. Each entry includes an IP, a hostname, and an optional hostname alias in that order, separated by a space. For example, **10.192.168.1 example1.com, 10.192.168.2 example2.com example-alias**. Select '**+**' to add multiple host entries. **Important** The host entries are saved only after you select **Save**.

Verify Content Gateway Connectivity

Post-installation, test the Content Gateway's connection in the UEM console to verify if the installation is completed successfully.

Procedure

1. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Content Gateway** in the UEM console.
2. Select **Test Connection** to verify the connectivity.

Considerations for Content Gateway Configuration

Consider the sync behavior of the repository content when the repository access is set up using the Content Gateway.

When setting up repository access using the Content Gateway, repository content only syncs up to two folder levels. Other subfolders sync as the UEM console or devices request them. On the console, the sync occurs when performing a manual sync action inside a subfolder. On the device, the sync occurs when an end user navigates to a subfolder.

Content Gateway Robustness

Understand how to address performance issues caused by the geographical separations between Content Gateway and Corporate File Servers.

Geographical separations in content infrastructure can lead to latencies that impact performance. Global organizations might encounter issues when syncing content from Corporate File Servers dispersed across the globe through a single Content Gateway connector.

To address the performance issues caused by geographical separations between Content Gateway and the local Corporate File Servers, configure multiple Content Gateway instances at the same Organization Group. It also splits the load for large deployments.

Evaluate your organization's need for multiple Content Gateway nodes. Global organizations with concerns about latencies caused by geographical separations benefit the most from this configuration option.

Troubleshooting Content Gateway

Understand the common errors that can occur after the Content Gateway configuration on Unified Access Gateway.

Content Gateway does not have specific error codes or messages to communicate the errors. You can identify the errors in the Content Gateway instance using the standard HTTP status codes. To troubleshoot errors on Unified Access Gateway, see Troubleshooting Unified Access Gateway Deployment.

Connection and Repository Error Logs

Log files on Content Gateway test connection failures, repository-related errors when accessed through Content Gateway, upload or download related issues from the device can be obtained from the Unified Access Gateway log archive. You can download the UAG-log-archive.zip file from the Support Settings section in the Unified Access Gateway Admin UI. For more information on log files, see Collecting Logs from the Unified Access Gateway Appliance.

Verify Packet Install Status

To check information about a specific package installed on the Unified Access Gateway Photon Machine, use the following command:

```
$ tdnf info <packagename>
```

Verify Content Gateway Connectivity

To check the health API endpoint connectivity, use the following URL on your browser.

```
https://<UAG_Content_Gateway_URL>:<port>/content/awhealth
```

The URL returns the HTTP status as 403 on the browser. You must mention the port if Content Gateway is configured using any port other than 443 on Unified Access Gateway.