Content Gateway Guide

February 10, 2026

Release Version: SaaS

Contents

Introduction to Content Gateway

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

Using the Content Gateway with 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 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: Omnissa Workspace ONE has announced the End of General Support for Content Gateway for Windows and Linux, effective October 17, 2019. Content Gateway solution on Omnissa Unified Access Gateway has been supported since 2017 as an alternative to the standalone solution offered on Windows and Linux servers.

Features, Benefits, and Limitations of Omnissa Unified Access Gateway

Before you begin migrating your Content Gateway to Unified Access Gateway (UAG), take a look at the features, benefits, and limitations of using Content Gateway with Omnissa Unified Access Gateway. Use Unified Access Gateway to design Omnissa Horizon®, Omnissa Access, and Omnissa Workspace ONE UEM deployments that need secure external access to your organization's applications. These applications can be Windows applications, software as a service (SaaS) applications, and desktops.

Features of Unified Access Gateway

- Unified Access Gateway is deployed in a demilitarized zone (DMZ).
- Unified Access Gateway directs authentication requests to the appropriate server and discards any unauthenticated request to ensure restricted resource 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.

  For more information, see Unified Access Gateway Documentation at Omnissa Product Documentation.

Benefits

Content Gateway is supported on the Unified Access Gateway platform and the number of deployments using Unified Access Gateway is increasing due to the following benefits:

- Unified Access Gateway is a secure virtual appliance.
- Unified End User Computing (EUC) gateway platform helps in easy and simple deployments. Single inbound gateway platform for multiple services like Content, Tunnel, Rev proxy, and Horizon.
- Security hardened appliance. The Unified Access Gateway platform goes through multiple internal and external security audits including pen testing and vulnerability scans to ensure security and stability.
- Certified using the highest level of security certifications like FIPS–140-2 and Common criteria.
- Lower customer Capital Expenditure (CAPEX) and Operational Expenditure (OPEX) because there are no additional hardware and software licensing costs.
- Flexible deployment options. Unified Access Gateway is supported on Hypervisors like ESXi and is also supported on Microsoft Hyper-V.
- Migrating from Content Gateway to Unified Access Gateway has few limitations that do not have a major impact on the functionality or user experience in accessing the content on Content Locker.
- Content Gateway can be easily configured on Unified Access Gateway using the admin UI.
- Trusted certificates can be imported to trust store using the admin UI.
- Details to the host file can be added using the admin UI.

Limitations

- SharePoint repositories other than Windows Authentication are supported.
- Adding network file share repositories with the forward slash is supported with Content Gateway 2.8 version. For earlier versions of the Content Gateway, you must include the backward slash in the URLs when adding network file share repositories.

Architecture and Security of Content Gateway

Understand the architecture design and security features of Content Gateway deployed as a service on the Omnissa 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 Unified Access Gateway* guide available at Omnissa Product Documentation.

Content Gateway offers basic and relay-endpoint architecture models for deployment. Both configurations support load-balancing for high-availability and SSL offloading. Configure your 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 Content Gateway can be deployed using the basic endpoint model and the 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 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 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.

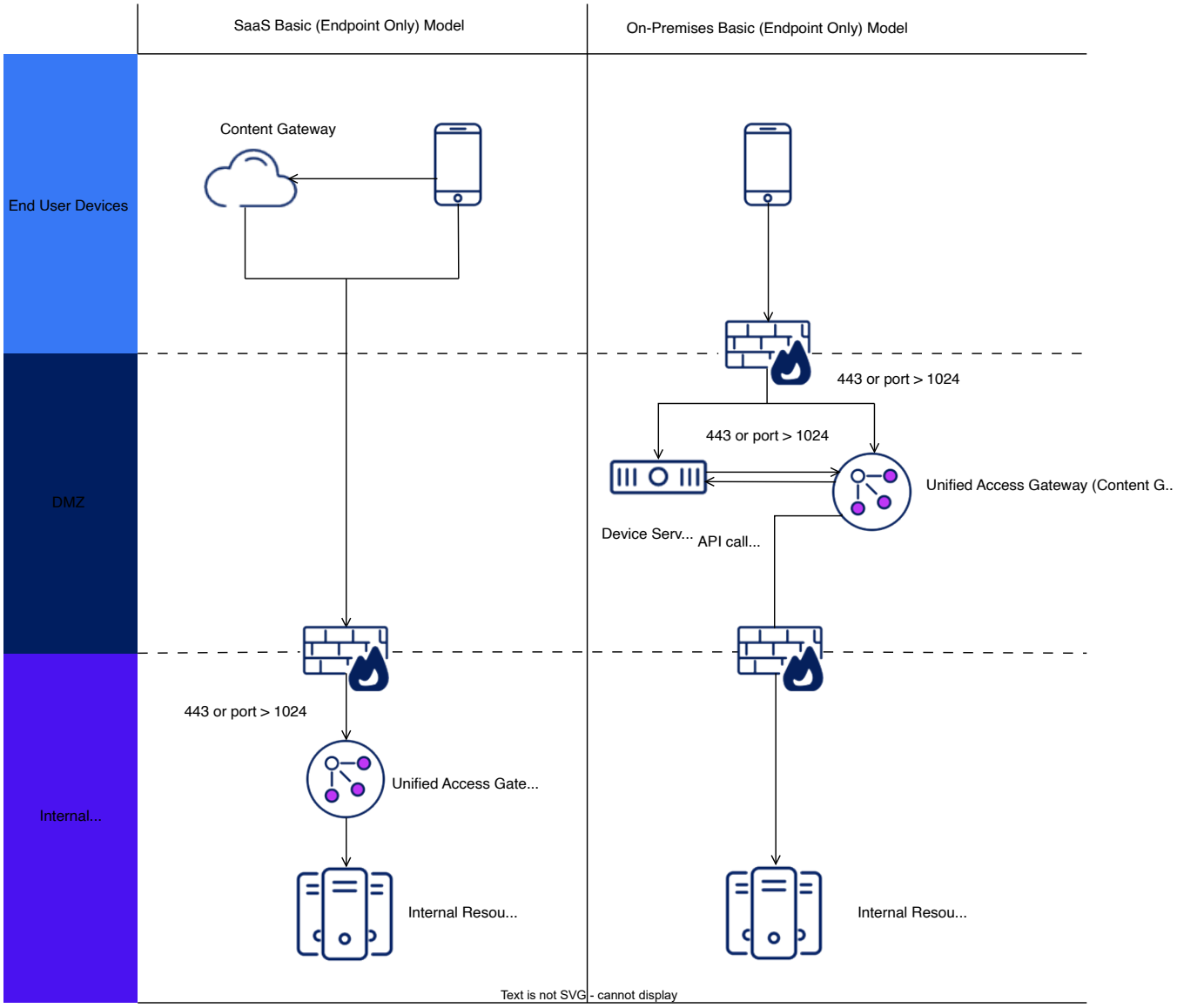
Basic Endpoint Deployment Model

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 Content Gateway. 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.

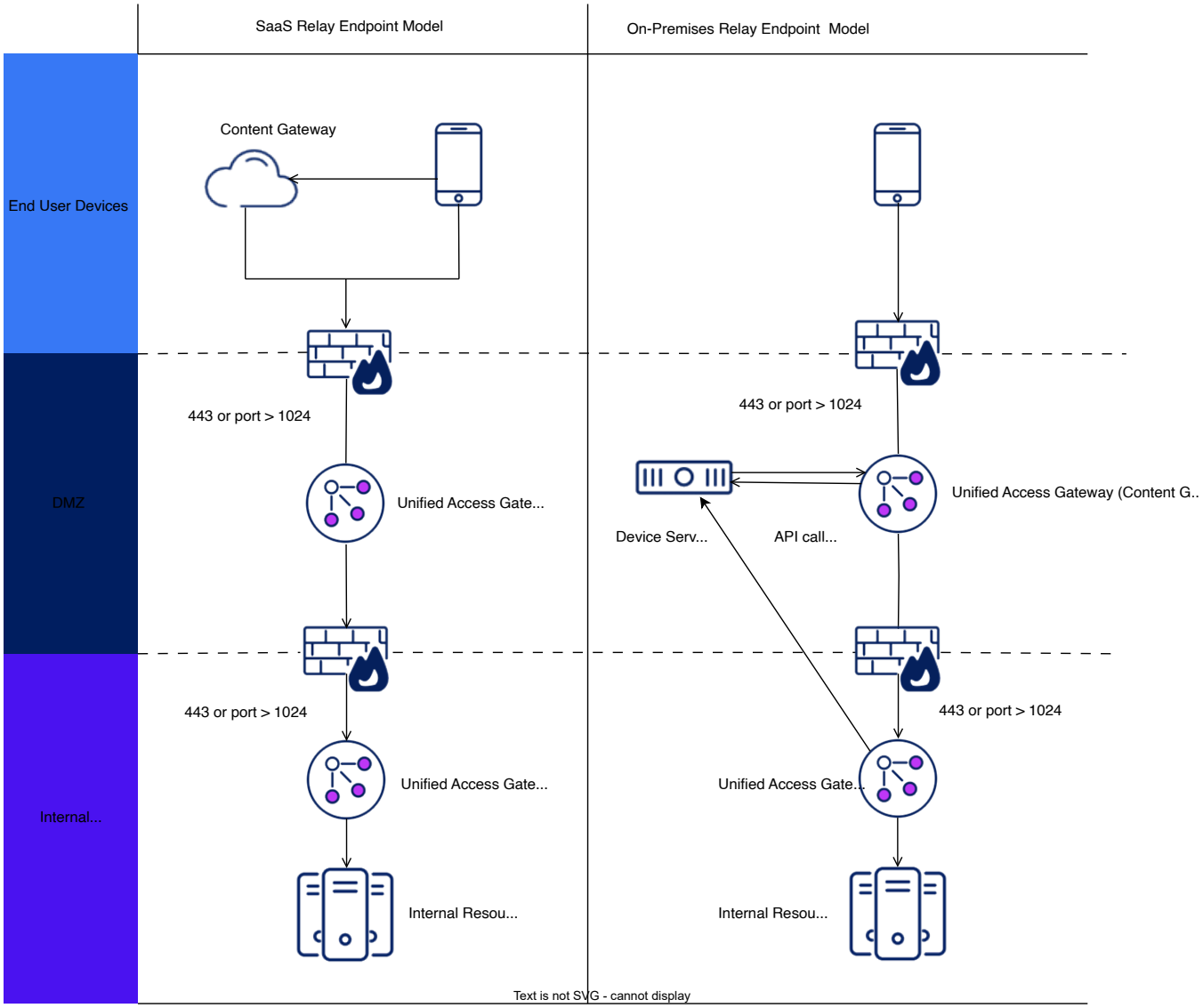
If the basic endpoint is installed in the DMZ, then proper network changes must be made for the Content Gateway to access various internal resources over the necessary ports.



Relay-Endpoint Deployment Model

The relay-endpoint deployment model has two instances of the Content Gateway with separate roles. The Content Gateway relay server resides in the DMZ and can be accessed from public DNS over the configured ports. The 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 Omnissa 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 *Deploying and Configuring Omnissa Unified Access Gateway* guide available at Omnissa Product Documentation.

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

Note: For SSL offloading configurations of Content Gateway on UAG, the Content Gateway server will listen for HTTP traffic on port 10080.

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	HTTPS	Devices (from Internet	Unified Access Gateway Relay	If 443 is used, Content

Port	Protocol	Source	Destination	Description
> 1024		and Wi-Fi)	Server (Content Gateway Relay)	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	
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 Omnissa Unified Access Gateway

Content Gateway deployment on Omnissa 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* at Omnissa Product Documentation.

Configure a Content Gateway Node with Unified Access Gateway Parameters

To establish a Content Gateway node, configure the Content Gateway settings in the Workspace ONE UEM console. Configuration includes selecting the platform, configuration model, associated ports, and if necessary, uploading an SSL certificate.

You can either add a new node and configure the Unified Access Gateway settings or edit an existing configuration and provide the Unified Access Gateway parameters. When you edit an existing configuration, the updated settings are applied on the active repositories and help you to minimize the manual configuration and the accessibility of end users.

After you edit and save the existing configuration of your standalone Content Gateway instance, you cannot revert to the previously configured values. If you revert to the previously configured values on the console, you must reinstall the Content Gateway.

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. If you have an existing active Content Gateway node, the setting is enabled.
3. Select the Configuration Type.
   - If you want to configure a new Content Gateway Node in the Workspace ONE UEM console, select **Add**.
   - If you want to edit an existing node, select **Edit**.
4. To configure a Content Gateway node, complete the following fields.
   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.

Note: Ensure that a full chain SSL certificate is uploaded on the Content Gateway configuration. SSL connections might fail if a full chain certificate is not uploaded.

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.

Public SSL Certificate Upload for Linux

Console Action	SSL Offloading	Server Action
Upload	No	Opt out of SSL Offloading when prompted during installation.
Upload Optional	Yes	Select SSL Offloading when prompted during installation.

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 and NFS repositories from their devices. **Note**: In case of a Network Share repository, ensure that the configuration keys `jcifs` must be set to `false` and `jcifsng` must be set to `true`.
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.

Setting	Description
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 does not require manual updates to the configuration files each time the UAG is upgraded. 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 Internet Content Adaptation Protocol (ICAP) Proxy with Workspace ONE (2960835).

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

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.

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	true	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
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,	Comma separates list of allowed	UAG 3.9 (CG 2.11.0) and later

Keys	Type	Value	Description	Supported UAG and CG version
		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	ciphers.	
aw.http.protocols	String	TLSv1, TLSv1.1, TLSv1.2	Values can be separated by comma.	UAG 3.10 (CG 2.11.0) and later
aw.server.fixed-headers	String	`X-Frame-Options: DENY## X-XSS-Protection: 1; mode=block##Expect-CT: max-age=86400, enforce##X-Content-Type-Options: nosniff`	Double hash (#) separated headers. Header name and value separated by a colon (:). **Caution**: Use this KVP only when you want to mitigate any threat detection for the missing headers from Content Gateway requests.	UAG 3.10 (CG 2.11.0) 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.`*`company_name`*	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. For more information, see *Configure Content Gateway on Unified Access*

Gateway in the *Deploying and Configuring Unified Access Gateway* Guide at Omnissa Product Documentation.

Verify Content Gateway Connectivity

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

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

Content Gateway Sizing Infrastructure for NFS Repository Sync

Using Content Gateway as a secure and effective medium, network share repositories like NetApp, SMB, and Network File Share () provide content access for end users. The performance of the Content Gateway depends on the number of users syncing and accessing the content.

To help you provide the best experience to your end user, we have tested the NFS repository sync performance at Omnissa Workspace ONE UEM by configuring NFS with Content Gateway on Omnissa Unified Access Gateway.

The details provided in this topic helps you to estimate the load Content Gateway can handle with the available resources and helps you to provide seamless access to the end-user documents.

NFS Testing Requirements

The infrastructure that we have used for testing the NFS repository with Content Gateway configured on the Unified Access Gateway appliance is listed in this section. The requirements and details specified in this section can be used for reference purposes. The requirements can change as per your need and supporting infrastructure.

High-Level Infrastructure

- A single instance of Content Gateway on Unified Access Gateway configured in the cascade mode on vSphere, with a Windows share configured on the same domain.
- No load balancers are used.

Hardware Specifications

Content Gateway

CPU Core	RAM	Disk Space	Notes
2	4 GB	20 GB	The requirements provided in the table are for supporting a basic data query. Large-scale UEM deployment has 4 cores of CPU and 16 GB of RAM to provide higher performance.

Windows NFS

CPU Core	RAM	Disk Space	Notes
16	4 GB	100 GB	The requirements provided in the table are used for conducting performance tests on NFS. The results can vary with varying specifications.

Sync Recommendations

The following data is derived from the NFS repository sync performance tested using Workspace ONE UEM. The sync test results can vary if the NFS or Content Gateway specifications are changed. Use the results as reference when using Content Gateway with the NFS repository.

Consider the number of sync requests as device requests with the assumption that each device makes one request.

Number of Files in NFS Repository	Number of Sync Requests	
	In 5 Minutes	In 1 Hour
500	7000–8000	85000–87000
1000	5000–6000	55000–60000
5000	2000–3000	20000–23000

Troubleshooting Content Gateway

Understand the common errors that can occur after the Content Gateway configuration on Omnissa 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* available at Omnissa Product Documentation.

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 200 on the browser. You must mention the port if Content Gateway is configured using any port other than 200 on Unified Access Gateway.

Note

Ensure to turn off the **JCIFS** flag as it is outdated. However, **JCIFS-ng** flag can be turned on only for CBA enabled repos.

Identify Network File Share Errors

Verify the status of the SMB connector on the Unified Access Gateway where Content Gateway is configured. The status of the SMB connector helps to identify Network File Share related errors like test connection errors, synchronization, upload, or download errors on the device.

1. Open the Unified Access Gateway console through vSphere.
2. To open the SMB connector folder, run the required command.

```
$ cd /opt/airwatch/content-gateway/smb-connector/
```

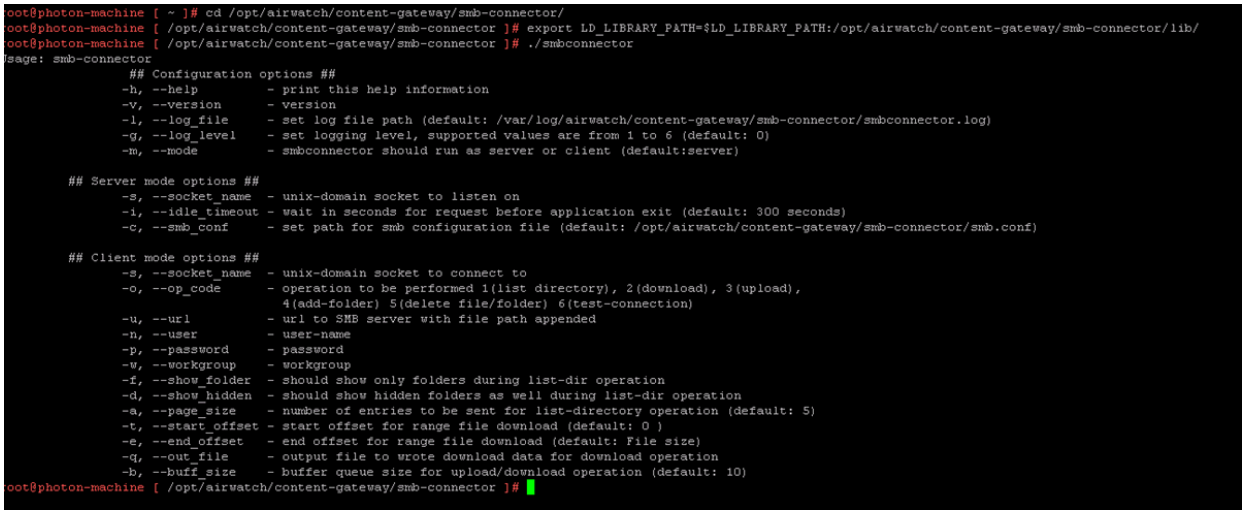
3. To export the SMB connector library, run the required command.

```
$ export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/airwatch/content-gateway/smb-connector/lib/
```

4. To run the SMB library, run the required command.

```
$  ./smbconnector
```

To ensure that there are no SMB connector errors on the Unified Access Gateway Photon Machine, verify the SMB output.



Verify Content Gateway Traffic

Verify that the Content Gateway configured on port 443 (standard port) internally reroutes the traffic on port 10443.

1. Run the following command to install debug packages.

```
$ "advancedDebugPackages install"
```

2. To verify the traffic flow on a specified port, run the required command.

```
$  tcpdump -i any -n -v tcp port 10443 -w <filename.pcap>
```

3. To verify the traffic, perform the test connection of Content Gateway on the Workspace ONE UEM console.

Content Gateway Domain Join Configuration

This section provides information about the different domain join configurations for the SMB connector.

DNS Resolution Using the Hosts File

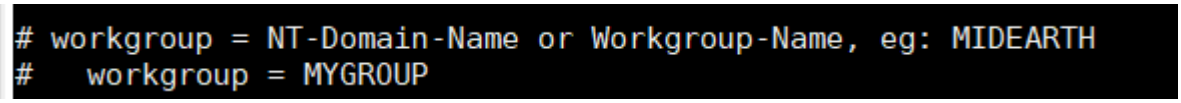
If the environment does not have any DNS servers or they are unreachable, add local configurations in the hosts file. You can add host entries to the host file using the Host Entries parameter available on the Unified Access Gateway Admin UI.

Configure Multiple Repositories and the Same Domain

If all users on the same domain are accessing multiple file share repositories through Content Gateway, the domain can be added into smb.conf for a quicker resolution. Adding the domain to smb.conf helps the users to avoid entering domain names while providing login credentials.

1. Navigate to **/opt/airwatch/content-gateway/smb-connector/smb.conf** and uncomment the workgroup section.
2. Add the user domain to the smb.conf file.

   The following image displays a domain that is added to the smb.conf file:

   
   ```
   # workgroup = NT-Domain-Name or Workgroup-Name, eg: MIDEARTH
   #   workgroup = MYGROUP
   ```

Configure DNS for Host Name Resolution

If short names are used or if host names of target shares are not resolved, perform the following configurations.

1. Add the DNS Server.
   a. Navigate to **/etc/resolv.conf** and open the **resolv.conf** file.
   b. Add DNS server IPs in the resolv.conf file.

      Adding server IPs directs the queries to the appropriate DNS server. Add multiple servers in multiple lines.
2. If shares are not provided or configured as FQDN, and DNS servers do not resolve them properly, add Fully Qualified Domain Name () to Search.
   a. Navigate to **/etc/resolv.conf** and open the **resolv.conf** file.
   b. Add the search parameter and provide the FQDNs that you want to be queried.

      Multiple entries can be added by separating the entries with space.