# VMware AirWatch Content Gateway to Unified Access Gateway Migration Guide

VMware Unified Access Gateway 3.3

**Have documentation feedback?** Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

# Table of Contents

# Chapter 1:
# Introduction to the VMware Unified Access Gateway

Use Unified Access Gateway to design VMware Horizon®, VMware Identity Manager™, and VMware 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. For more information, see Unified Access Gateway Documentation.

## 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.

## Benefits

Content Gateway is supported on the VMware 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, Horizon etc.
- 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) since there are no additional hardware and software licensing costs.
- Flexible deployment options. Unified Access Gateway is supported on VMware 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.
- Backward slash must be included in the URLs when adding network share repositories. Adding network file share with a forward slash is not currently supported for Content Gateway on Unified Access Gateway.

## 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.

# Chapter 2:
# Content Gateway Migration Requirements

To migrate from Content Gateway to Unified Access Gateway, you must first deploy and configure the Unified Access Gateway platform. Migrating from Content Gateway to Unified Access Gateway does not have any hardware or software requirement specific to your Content Gateway deployment. For more information about the types of Unified Access Gateway deployments and the related requirements, see Preparing to Deploy VMware Unified Access Gateway.

## Port Requirements

Consider the port requirements for 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 | AirWatch Device Services | Unified Access Gateway Content Gateway Endpoint | If 443 is used, Content Gateway listens on port 10443. |
| 443 or any port > 1024 | TCP | Workspace ONE UEM console | Unified Access Gateway Content Gateway Endpoint | If 443 is used, Content Gateway listens on port 10443. |
| Any port where the repository is listening to. | HTTP or HTTPS | Unified Access Gateway Content Gateway Endpoint | Web-based content repositories such as (SharePoint / WebDAV / CMIS, and so on | Any configured custom port on which the Intranet site is listening to. |
| 137–139 and 445 | CIFS or SMB | Unified Access Gateway Content Gateway Endpoint | Network Share-based repositories (Windows file shares) | Intranet Shares |

## 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 Content Gateway Endpoint | If 443 is used, Content Gateway listens on port 10443. |
| 443 or any port > 1024 | TCP | AirWatch 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. |
| 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 listens 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 |

# Chapter 3:
# Deploying Content Gateway on Unified Access Gateway

Content Gateway deployment on Unified Access Gateway begins with providing the Unified Access Gateway (UAG) parameters either to a newly configured or an existing Content Gateway 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.

## Configure a Content Gateway Node with Unified Access Gateway Parameters

To establish a node, configure 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 helps you to minimize the manual configuration and the accessibility of end users.

**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. If you have an existing active Content Gateway node, the setting will enabled.
3. Select the Configuration Type:
   a. If you want to configure a new Content Gateway Node in the Workspace ONE UEM console, select **Add**.
   b. If you want to edit an existing node, select **Edit**.

4. Complete the following fields to configure a Content Gateway node.

| Setting | Description |
|---|---|
| **Installation Type** | Select UAG as the platform. |
| **CONTENT CONFIGURATION** | |
| **Choose Configuration Type** | Select one of the following configuration types:<br>• **Basic** – Endpoint configuration with no relay component.<br>• **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. If you are editing an existing configuration, there is no requirement to update the Content Gateway Instance name. |
| **Content Gateway Relay Address** | If implementing a relay configuration, enter the Unified Access Gateway relay URL used to access the Content Gateway Relay from the Internet. |
| **Content Gateway Relay Port** | If implementing a relay configuration, enter the Unified Access Gateway relay server port. |
| **Content Gateway Endpoint Address** | Enter the Unified Access Gateway endpoint URL used to access the Content Gateway. |
| **Content Gateway Endpoint Port** | Enter the Unified Access Gateway endpoint server port for Content Gateway. |
| **Server SSL Port** | Enter the SSL port number. If there is an existing configuration, SSL port can be retained. |
| **CONTENT SSL CERTIFICATE** | |
| **Public SSL Certificate (required for Linux requirements** | If necessary, upload a PKCS12 (.pfx) certificate file with a full chain for the Content Gateway instance to bind to the port. The full chain includes a password, server certificate, intermediates, root certificate, and a private key.<br>Requirements vary by platform and SSL configuration. |

| Console Action | SSL Offloading | Server Action |
|---|---|---|
| **Upload** | No | Opt out of SSL Offloading when pro mpted during installation. |
| **Upload Optional** | Yes | Select SSL Offloading when prompt ed during installation. |
| *This field does not display when configuring Windows Content Gateway. Windows u ses IIS and does not require a Public SSL certificate. | | |

| | |
|---|---|
| **Ignore SSL Errors (not recommended)** | If using a self-signed certificate, consider enabling this feature. If enabled, Content Gateway ignores certificate trust errors and certificate name mismatches. |

| Setting | Description |
|---|---|
| **SSL Offloading** | Enable or disable SSL Offloading. If there is an existing configuration, the preconfigured selection can be retained. |

5. 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.

## Configure Content Gateway on Unified Access Gateway

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]`<br>The destination URL must contain the protocol, host name or IP address, and port number. For example: https://load-balancer.example.com:8443.<br>Unified Access Gateway pulls Content Gateway configuration from the API server. |
| API Server Username | User name to log into the API server. |
| 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.<br>For example, **10.192.168.1 example1.com, 10.192.168.2 example2.com example-alias**. Select '**+**' to add multiple host entries.<br>**Important:** The host entries are saved only after you select **Save**. |

# Chapter 4:
# Troubleshooting Content 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.

## 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.

To verify the status the SMB connector, perform the following steps:

1. Open the Unified Access Gateway console through VMware v-Sphere.
2. To open the SMB connector folder, run the following command:

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

3. To export the SMB connector library, run the following command:

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

4. To run the SMB library, run the following command:

```
$ ./smbconnector
```

**Sample Output**

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

```
root@photon-machine [ ~ ]# cd /opt/airwatch/content-gateway/smb-connector/
root@photon-machine [ /opt/airwatch/content-gateway/smb-connector ]# export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/airwatch/content-gateway/smb-connector/lib/
root@photon-machine [ /opt/airwatch/content-gateway/smb-connector ]# ./smbconnector
Usage: smb-connector
                ## Configuration options ##
               -h, --help         - print this help information
               -v, --version      - version
               -l, --log_file     - set log file path (default: /var/log/airwatch/content-gateway/smb-connector/smbconnector.log)
               -g, --log_level    - set logging level, supported values are from 1 to 6 (default: 0)
               -m, --mode         - smbconnector should run as server or client (default:server)

        ## Server mode options ##
               -s, --socket_name  - unix-domain socket to listen on
               -i, --idle_timeout - wait in seconds for request before application exit (default: 300 seconds)
               -c, --smb_conf     - set path for smb configuration file (default: /opt/airwatch/content-gateway/smb-connector/smb.conf)

        ## Client mode options ##
               -s, --socket_name  - unix-domain socket to connect to
               -o, --op_code      - operation to be performed 1(list directory), 2(download), 3(upload),
                                    4(add-folder) 5(delete file/folder) 6(test-connection)
               -u, --url          - url to SMB server with file path appended
               -n, --user         - user-name
               -p, --password     - password
               -w, --workgroup    - workgroup
               -f, --show_folder  - should show only folders during list-dir operation
               -d, --show_hidden  - should show hidden folders as well during list-dir operation
               -a, --page_size    - number of entries to be sent for list-directory operation (default: 5)
               -t, --start_offset - start offset for range file download (default: 0 )
               -e, --end_offset   - end offset for range file download (default: File size)
               -q, --out_file     - output file to wrote download data for download operation
               -b, --buff_size    - buffer queue size for upload/download operation (default: 10)
root@photon-machine [ /opt/airwatch/content-gateway/smb-connector ]#
```

## Verify Content Gateway Traffic

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

1. To install the tcpdump & ethtool, run the following command:

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

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

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

To verify the traffic, perform the test connection of Content Gateway on the Workspace ONE UEM console. The .pcap file can be opened using any supported library or packet analyzer, for example Wireshark.

## 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.

## Content Gateway Domain Join Configuration

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

### Multiple Repositories and 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.

To add the domain in smb.conf:

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
```

## DNS Configuration for Host Name Resolution

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

**Adding DNS Server**

1. Navigate to **/etc/resolv.conf** and open the **resolv.conf** file.
2. 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.

**Adding Fully Qualified Domain Name (FDQN) to Search**

If shares are not provided or configured as FQDN, and DNS servers do not resolve them properly, perform the following steps:

1. Navigate to **/etc/resolv.conf** and open the **resolv.conf** file.
2. 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.

## 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. By adding local configurations in the Hosts file, domains can be resolved to the specified IP addresses.

1. Navigate to in **/etc/hosts** file.
2. Map the IP address to the respective hostname. Unified Access Gateway provides options in the Unified Access Gateway console to add host entries.
   The following image displays a list of sample IP addresses mapped to the respective hostname: