

# Content Gateway for Windows

VMware Workspace ONE UEM 1907



vmware®

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

<https://docs.vmware.com/>

If you have comments about this documentation, submit your feedback to

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2019 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

<b>1</b>	<b>Introduction to the VMware Content Gateway</b>	<b>4</b>
<b>2</b>	<b>Architecture and Security</b>	<b>5</b>
	Content Gateway with Load Balancing	5
	Content Gateway Deployment Models	5
	Basic (Endpoint Only) Deployment Model for Content Gateway	6
	Relay-Endpoint Deployment Model for Content Gateway	7
<b>3</b>	<b>Content Gateway Installation Preparation</b>	<b>8</b>
	Support for Corporate File Servers	8
	Disable SMBv1 Protocol	10
	Content Gateway Requirements for Windows	10
<b>4</b>	<b>Content Gateway Configuration</b>	<b>14</b>
	Content Gateway Compatibility Matrix	15
	Download the Content Gateway Installer	16
	Considerations for Content Gateway Configuration	16
	Content Gateway Robustness	17
<b>5</b>	<b>Content Gateway Installation</b>	<b>18</b>
	Install a Content Gateway Relay Server	18
	Install a Content Gateway Endpoint Server	19
	Verify Content Gateway Connection	19
<b>6</b>	<b>Content Gateway Management</b>	<b>21</b>
	Content Gateway Troubleshooting	21

# Introduction to the VMware Content Gateway

1

The Workspace ONE UEM powered by AirWatch provides VMware Content Gateway as 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.

By default, Content Gateway on Window Servers supports SMB2 through SMB3 versions. Due to security vulnerabilities, SMB1 is not supported by default but if necessary can be customized to support SMB1.

This documentation provides information about installing the Content Gateway on a physical appliance using a standalone installer.

# Architecture and Security

Understand the architecture design and security features of VMware Content Gateway.

## Overview

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.

This chapter includes the following topics:

- [Content Gateway with Load Balancing](#)
- [Content Gateway Deployment Models](#)
- [Basic \(Endpoint Only\) Deployment Model for Content Gateway](#)
- [Relay-Endpoint Deployment Model for Content Gateway](#)

## 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 your API servers. 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.

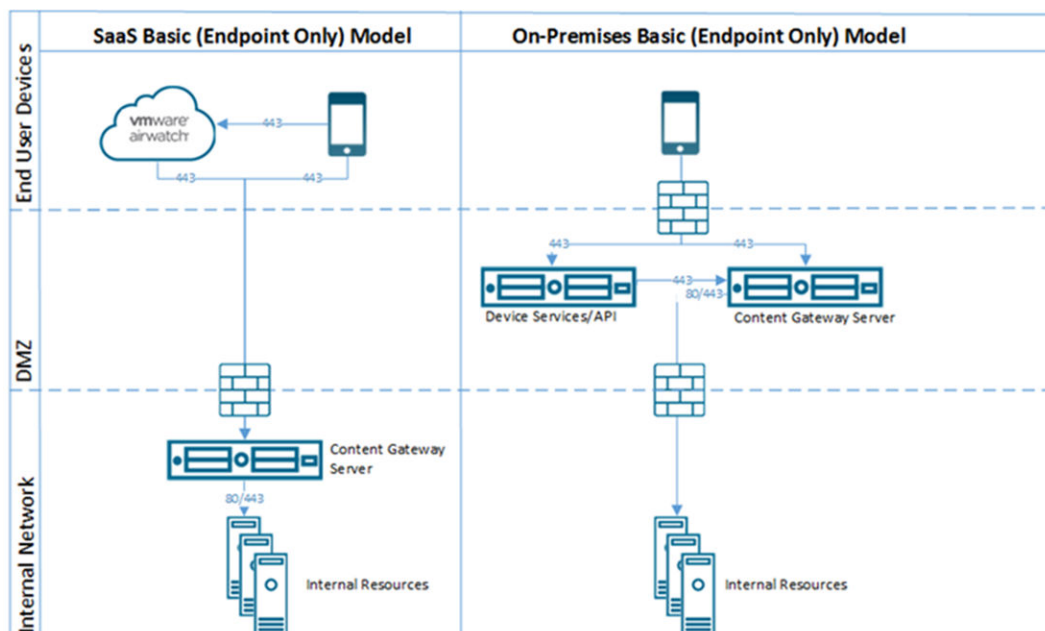
## Basic (Endpoint Only) Deployment Model for Content Gateway

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

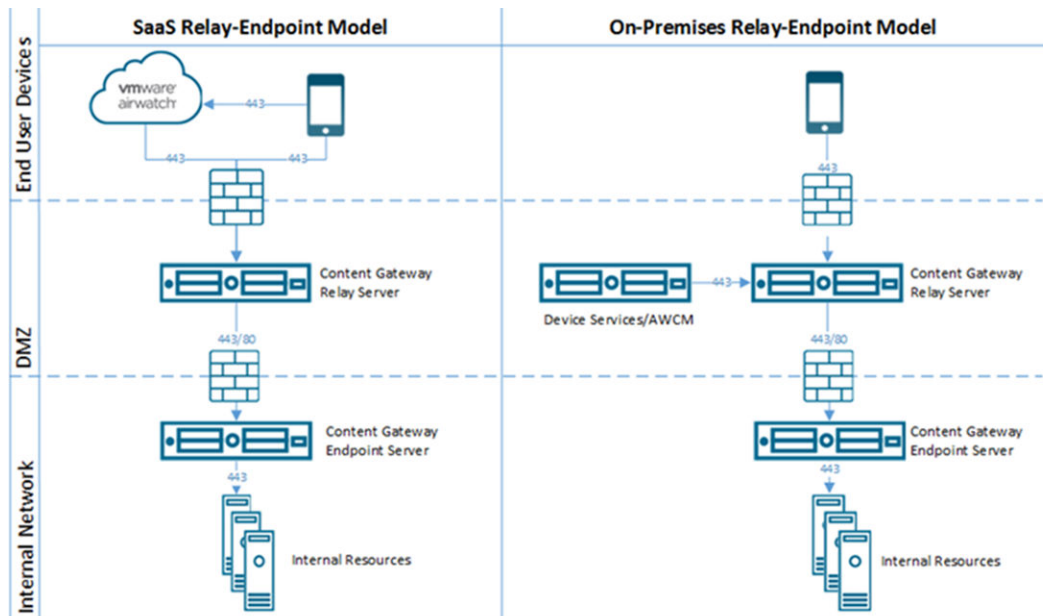
The relay-endpoint deployment model architecture includes two instances of the VMware Content Gateway with separate roles.

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.



# Content Gateway Installation Preparation

## 3

Effective preparation includes evaluating the appropriateness of the Content Gateway solution for your organization, determining your deployment model, and meeting the hardware, software, and network requirements.

This chapter includes the following topics:

- [Support for Corporate File Servers](#)
- [Content Gateway Requirements for Windows](#)

## Support for Corporate File Servers

Workspace ONE UEM supports integration with various corporate file servers. The syncing method support and requirement of the Content Gateway component vary by repository type.

### Available Sync Methods

Review the available syncing methods for repositories:

- **Admin** – Refers to a repository that gets fully configured and synced by an administrator in the UEM console. Each assigned user receives the same static link to the file repository.
- **Automatic** – Refers to a repository that gets configured by an administrator in the UEM console but allows the admin to use dynamic lookup values. The repository gets synced by end users on their devices. Each assigned user receives a unique or semi-unique link to a file repository. This is a useful option for link to users' home directories.
- **Manual** – Refers to a repository that gets configured in the UEM console, but allows the admin to set a static and wildcard portion of a link. Each end user can manually add the repository link that complies with the format set by the admin and sync the repository on their device.

## Corporate File Server Matrix

Use the matrix to determine the supported syncing methods and Content Gateway requirements by repository type:

	Admin	Automatic	Manual
Available Repositories			
Box	✓	✓	✓
CMIS	✓	✓	✓

	Admin	Automatic	Manual
Google Drive	✓	–	–
Network Share	✓	✓	✓
OneDrive	✓	–	–
OneDrive for Business	✓	–	–
OneDrive for Business ADFS	✓	–	–
OneDrive for Business OAuth	✓	–	–
SharePoint	✓	✓	✓
SharePoint ADFS	✓	✓	✓
SharePoint O365	✓	✓	✓
SharePoint O365 ADFS	✓	✓	✓
SharePoint O365 OAuth	✓	–	–
SharePoint - Personal (My Sites)	✓	–	–
SharePoint WebDAV	✓	–	–
SharePoint Windows Auth	✓	✓	✓
WebDAV	✓	✓	✓
Access through Content Gateway			
Box	–	–	–
CMIS	✓+	✓+	✓+
Google Drive	–	–	–
Network Share	✓+	✓+	✓+
OneDrive	–	–	–
OneDrive for Business	✓	–	–
OneDrive for Business ADFS	✓	–	–
SharePoint	✓	✓	✓
SharePoint ADFS	✓	✓	✓
SharePoint O365	✓	✓	✓
SharePoint O365 ADFS	✓	✓	✓
SharePoint - Personal (My Sites)	✓	–	–
SharePoint WebDAV	✓	–	–
SharePoint Windows Auth (Content Gateway for Linux)	–	–	–
SharePoint Windows Auth (Content Gateway for Windows)	✓	✓	✓
WebDAV	✓	✓	✓

	Admin	Automatic	Manual
<b>Legend:</b>			
¥ = The VMware Content Gateway on Linux servers supports only SMB v2.0 and SMB v3.0. The default supported version is SMB v2.0.			
✓+ = Required			
✓ = Supported			
– = Not Supported			

## Disable SMBv1 Protocol

AirWatch Content Gateway does not support the SMBv1 protocol because of security vulnerabilities.

For using Network Share with maximum security, disable SMBv1 and enable the SMBv2 protocol.

### Procedure

- 1 Navigate to your Network Share server.
- 2 Start **PowerShell** with administrator privileges.
- 3 Run **Get-SmbServerConfiguration | Select EnableSMB1Protocol, EnableSMB2Protocol** to verify the status of the SMB protocols in use.
- 4 If you have the SMBv1 protocol enabled, disable it by running the required command.

- a Run

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

- b Select **Y** to confirm.

- 5 If you have the SMBv2 protocol disabled, enable it by running the required command.

- a Run

```
Set-SmbServerConfiguration -EnableSMB2Protocol $true
```

- b Select **Y** to confirm.

## Content Gateway Requirements for Windows

To deploy VMware Content Gateway for Windows, ensure that your system meets the specified hardware, software, network, and general requirements.

### Hardware Requirements

Use the following requirements as a basis for creating your VMware Content Gateway server.

Requirement	CPU Cores	RAM (GB)	Disk Space	Notes
VM or Physical Server (64-bit)	2 CPU Core (2.0+ GHz)* *An Intel processor is required.	2 GB+	5 GB	The requirements listed here support basic data query. You may require additional server space if your use case involves the transmission of large encrypted files from a content repository.
Hard Disk Space (GB)	400 MB for installer ~10 GB for log file space**			

\*It is possible to deploy only a single Content Gateway server as part of a smaller deployment. However, consider deploying at least 2 load-balanced servers with 2 CPU Cores each regardless of number of devices for uptime and performance purposes.

\*\*About 10 GB is for a typical deployment. Log file size should be scaled based on your log usage and requirements for storing logs.

## General Requirements

Ensure your VMware Content Gateway is set up with the following general requirements to ensure a successful installation.

Requirements	Notes
Internally registered DNS record	Register the Endpoint server.
Externally registered DNS record	Identify the appropriate configuration model to determine which server to register: <ul style="list-style-type: none"> <li>■ Endpoint-Only Configuration Model – Register the endpoint server.</li> <li>■ Relay-Endpoint Configuration Model – Register the relay server.</li> </ul>
SSL Certificate from trusted third party with subject name of server hostname	Requires a PKCS12 (.pfx) format and the trust of all device types in use. Keep in mind: <ul style="list-style-type: none"> <li>■ Android does not natively trust all Comodo certificates.</li> <li>■ PKCS12 (.pfx) format includes the server certificate, private key, root chain, and password protection.</li> </ul>

## Windows Software Requirements

Ensure your VMware Content Gateway server meets all the following software requirements.

Requirements	Notes
Windows Server 2008 R2, 2012 or 2012 R2; 64-bit, 2016	Basic infrastructure type recommended.
Remote access to Windows servers	Set up the Remote Desktop Connection Manager. Download the installer from: <a href="https://www.microsoft.com/en-us/download/details.aspx?id=44989">https://www.microsoft.com/en-us/download/details.aspx?id=44989</a>
Admin Privileges	Ensure your admin permissions allow you to run the installer, create services, manage services, install features, create folders, and run processes.
Notepad++ (Recommended)	Set up Notepad++.
IIS 443 bound with SSL certificate	Validate that you can connect to the server over HTTPS ( <a href="https://&lt;yourAirWatchDomain&gt;.com">https://&lt;yourAirWatchDomain&gt;.com</a> ). At this point, you should see the IIS splash page.

Requirements	Notes
Role from Server Manager installed	IIS 7.0 (Server 2008 R2) IIS 8.0 (Server 2012 or Server 2012 R2) IIS 8.5 (Server 2012 R2 only)
.NET Framework 4.6.2	The installer will install this version of .NET provided the server has Internet access. Otherwise, download and manually install it.

## Network Requirements

For configuring the ports listed below, all the traffic is uni-directional (outbound) from the source component to the destination component.

Source Component	Destination Component	Protocol	Port	Note
Content Gateway – Basic-Endpoint Configuration				
Devices (from Internet and Wi-Fi)	Content Gateway Endpoint	HTTPS	443*	1
AirWatch Device Services	Content Gateway Endpoint	HTTPS	443*	4
UEM Console	Content Gateway Endpoint	HTTPS	443*	5
Content Gateway Endpoint	Web-based content repositories (SharePoint / WebDAV / CMIS / etc.)	HTTP or HTTPS	80 or 443	2
Content Gateway Endpoint	Network Share-based repositories (Windows file shares)	CIFS or SMB	137-139 and 445	6
Content Gateway Endpoint	CRL	HTTP	80	7
Content Gateway – Relay-Endpoint Configuration				
Devices (from Internet and Wi-Fi)	Content Gateway Relay	HTTPS	443*	1
AirWatch Device Services	Content Gateway Relay	HTTPS	443*	4
UEM Console	Content Gateway Relay	HTTPS	443*	5
Content Gateway Endpoint	Web-based content repositories (SharePoint / WebDAV / CMIS / etc.)	HTTP or HTTPS	80 or 443	2
Content Gateway Relay	Content Gateway Endpoint	HTTPS	443*	3
Content Gateway Relay	CRL	HTTP	80	7
Content Gateway Endpoint	Network Share-based repositories (Windows file shares)	CIFS or SMB	137-139 and 445	6

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

- 1 For devices attempting to access internal resources.
- 2 For devices with the VMware Workspace ONE Content to access internal content from websites, such as SharePoint.
- 3 For Content Gateway Relay topologies to forward device requests to the internal Content Gateway endpoint only.

- 4 For the Device Services server to enumerate the repositories through the content relay and convert them into a format devices can use.
- 5 For the console server to enumerate the repositories through the content relay for viewing in the UEM console.
- 6 For devices with the VMware Workspace ONE Content to access internal content from Network Shares.
- 7 For the Content Gateway server to perform certificate validation and ensure it does not accept a revoked certificate.

# Content Gateway Configuration

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

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

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

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

## Procedure

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

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

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

- 3 Click **Add**.

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

##### a Configure the **Installation Type**.

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

##### b Configure the **Content Configuration** settings.

Setting	Description
Configuration Type	<ul style="list-style-type: none"> <li>■ <b>Basic</b> – Endpoint configuration with no relay component.</li> <li>■ <b>Relay</b> – Endpoint configuration with a relay component.</li> </ul>
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 using a self-signed certificate, consider enabling this feature. If enabled, Content Gateway ignores certificate trust errors and certificate name mismatches.

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

#### 5 Select **Add**.

#### 6 Select **Save**.

#### What to do next

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

## Content Gateway Compatibility Matrix

The following table provides information about the compatibility of Content Gateway with the current and previous versions of the UEM console and Remote File Storage (RFS).

## Content Gateway for Windows

Console Version	Content Gateway Version	RFS for Windows Version
1907	9.2.3	9.2.3
1905	9.2.3	9.2.3

## Download the Content Gateway Installer

After you configure the Content Gateway node on the UEM console, install the Content Gateway using the VMware Content Gateway installer. The VMware Content Gateway installer is available for download on the My Workspace ONE portal.

### Procedure

- 1 From UEM console, navigate to **Groups & Settings > All Settings > Systems > Enterprise Integration > Content Gateway** in an Organization Group with at least one configured and saved Content Gateway node.
- 2 To retrieve the existing Content Gateway instance configuration as XML file, select the configuration using the radio button and then select **Download Configuration**.
- 3 Enter and confirm a **password** for the certificate.  
The password must contain a minimum of six characters.
- 4 From the More Actions menu, select **Download Installer** to configure Content Gateway using Content Gateway installer.  
You are redirected to the My Workspace ONE portal to download the Content Gateway installer files.
- 5 Log in to the My Workspace ONE portal and then select the required platform, app, and Console version for Content Gateway.
- 6 Select **Installs And Upgrades** and then select the Content Gateway installer file to begin the download.

## Considerations for Content Gateway Configuration

- 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.
- When connecting to network file shares using the Content Gateway for Windows, the endpoint server and NFS must be on the same domain. Otherwise, if the Content Gateway is on a different domain, it must have domain trust with the domain of NFS.

- Security focused implementations of Content Gateway for Windows might prevent Content Gateway from impersonating the calling user. If Content Gateway cannot check user access to shared network folders, end user attempts to access a repository using credentials return an **Impersonation Failed** message. To resolve this issue:
  - Navigate to **Security Settings > Local Policies > User Rights Assignment > "Allow log on locally"** in the Local Security Policies on the Content Gateway server.
  - Add **Allow log on locally**, **Log on as a service** and **Access this computer from the network** permissions to each user accessing content - successfully invoking user impersonation from the Content Gateway Windows Server to the Windows Network File Share.

## 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.

# Content Gateway Installation

Workspace ONE UEM helps you install Content Gateway on Windows and Linux servers. Workspace ONE UEM supports Content Gateway installation on relay and endpoint servers.

Log in to the My Workspace ONE portal to download the Content Gateway Installer and configure it based on your requirements. You can also verify your installation and configuration using the verification options available in the UEM console.

This chapter includes the following topics:

- [Install a Content Gateway Relay Server](#)
- [Install a Content Gateway Endpoint Server](#)
- [Verify Content Gateway Connection](#)

## Install a Content Gateway Relay Server

For a relay-endpoint configuration, you must set up a Content Gateway relay server.

### Prerequisites

After ensuring that your servers meets all the proper requirements, configuring settings in the UEM console, and downloading the installer, run the installer to enable the service.

### Procedure

- 1 Open the installer executable on the Relay Content Gateway server and then select **Next**.
- 2 Accept the End User License Agreement and then select **Next**.
- 3 Specify the destination for the downloaded Content Gateway installation files and then select **Next**.
- 4 Configure the **Content Gateway Setup** screen.

Setting	Description
Relay	Select to first install Content Gateway on the Relay server.
Is this server SSL Offloaded?	Select if the SSL connection terminates using a reverse proxy prior to reaching the Relay server

- 5 Enter the Certificate Password created when downloading the installer. Click **Next**.
- 6 Use the drop-down menu to select the Target Site in IIS to install the Workspace ONE UEM application in. Click **Next**.
- 7 Verify the Windows Firewall settings allow the Content Gateway ports and Default IIS website port.

- 8 Click **Install** to begin Content Gateway installation on the server.
- 9 Click **Finish** to close the Content Gateway installer.
- 10 Close the installer.

## Install a Content Gateway Endpoint Server

For a relay-endpoint or basic endpoint configuration, you must set up a Content Gateway endpoint server.

In Relay-Endpoint configurations, you install the endpoint server after installing the relay server. If you have not already, install the relay server. See [Install a Content Gateway Relay Server](#).

### Prerequisites

After ensuring that your servers meets all the proper requirements, configuring settings in the UEM console, and downloading the installer, run the installer to enable the service.

### Procedure

- 1 Open the installer executable on the Endpoint Content Gateway server and then select **Next**.
- 2 Accept the End User License Agreement and then select **Next**.
- 3 Specify the destination for the downloaded Content Gateway installation files and then select **Next**.
- 4 Select the **Endpoint** button to install Content Gateway on the Endpoint server.
- 5 Enter the Certificate Password created when downloading the installer. Click **Next**.
- 6 Use the drop-down menu to select the Target Site in IIS to install the Workspace ONE UEM application in. Click **Next**.
- 7 Verify the Windows Firewall settings allow the Content Gateway ports and Default IIS website port.
- 8 Click **Install** to begin Content Gateway installation on the server.
- 9 Click **Finish** to close the Content Gateway installer.
- 10 Close the installer.

### What to do next

Verify Content Gateway's connectivity in the Workspace ONE UEM Admin console to ensure that the installation is completed successfully. See [Verify Content Gateway Connectivity](#).

## Verify Content Gateway Connection

After installing the relay-endpoint or basic endpoint configuration, test the Content Gateway's connection in the Workspace ONE UEM console to verify that the installation completed successfully.

### Procedure

- 1 Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Content Gateway** in the UEM console.

- 2 Select the radio button next to the Content Gateway node and then select the **Test Connection** option to verify the connectivity.

The **Test Connection** option is also available in the Content Gateway Configuration screen. The edit icon next to the content gateway node when selected displays the Content Gateway Configuration screen.

# Content Gateway Management

To access the latest iteration, upgrade the Content Gateway. Any custom changes you make to the configuration files after the original installation is lost, so you can create backups of these files to reference later.

## Procedure

- 1 Navigate to **Groups & Settings > All Settings > System > Enterprise Integrations > Content Gateway**.
- 2 To retrieve the existing Content Gateway instance configuration as XML file, select the configuration using the radio button and then select **Download Configuration**.
- 3 Enter and confirm a **password** for the certificate. The password must contain a minimum of six characters.
- 4 From the More Actions menu, select **Download Installer** to configure Content Gateway using Content Gateway installer.

Downloading the installer removes Content Gateway v8.3 functionality. Only download the installer if prepared to immediately follow-through with installation.

You are redirected to the My Workspace ONE portal to download the Content Gateway installer files.

- 5 On the My Workspace ONE portal page for Content Gateway, select the required platform, app, and Console version.
- 6 Select **Installs And Upgrades** and then select the Content Gateway installer file to begin the download.

## What to do next

After the download, continue with the steps for Installing the Content Gateway – Basic or Installing the Content Gateway – Relay-Endpoint.

## Content Gateway Troubleshooting

Use the available logs and commands or monitoring URL to diagnose and troubleshoot intermittent issues that you might experience with the Content Gateway.

### Windows Logs

- Logs are located at AirWatch/Logs/ContentGateway/CGContent.log

- To change log levels, navigate to AirWatch\AirWatch.EnterpriseIntegration.Content\ and open the Web.config file. Locate the loggingConfiguration entry and change level="Error" to level="Verbose". Restarting the Content Gateway service or performing an IIS reset might be necessary.

## Windows Monitoring URL

URL	Return	Notes
https://<Content_Gateway_URL > /content/systeminfo	403 Forbidden	Enable the <add key="enableSystemInfo" value="true" / > flag in the Web.config file

**Note** The Content Gateway does not have specific error codes or messages through which it communicates the errors. Content Gateway communicates errors through the standard HTTP status codes. For more information, see [HTTP status codes](#).