VMware AirWatch Content Gateway Guide for Windows

Workspace ONE UEM v9.6

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 AirWatch Content Gateway

The VMware AirWatch Content Gateway provides a secure and effective method for end users to access internal repositories. Using the VMware AirWatch Content Gateway with VMware Content Locker 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 Content Locker. Users are granted access to their approved files and folders based on the existing access control lists defined in your internal repository. To prevent security vulnerabilities, from AirWatch Console release 9.2, Content Gateway on Linux Servers supports only SMBv2.0, and SMBv3.0. The default version is SMBv2.0.

Chapter 2:
Architecture and Security

Overview

VMware AirWatch 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 AirWatch 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

VMware AirWatch supports integration with a load balancer for improved performance and faster availability. However, 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 Robins 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 AirWatch 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 AirWatch environments support the basic and relay-endpoint deployment models. The VMware AirWatch 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 AirWatch 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.

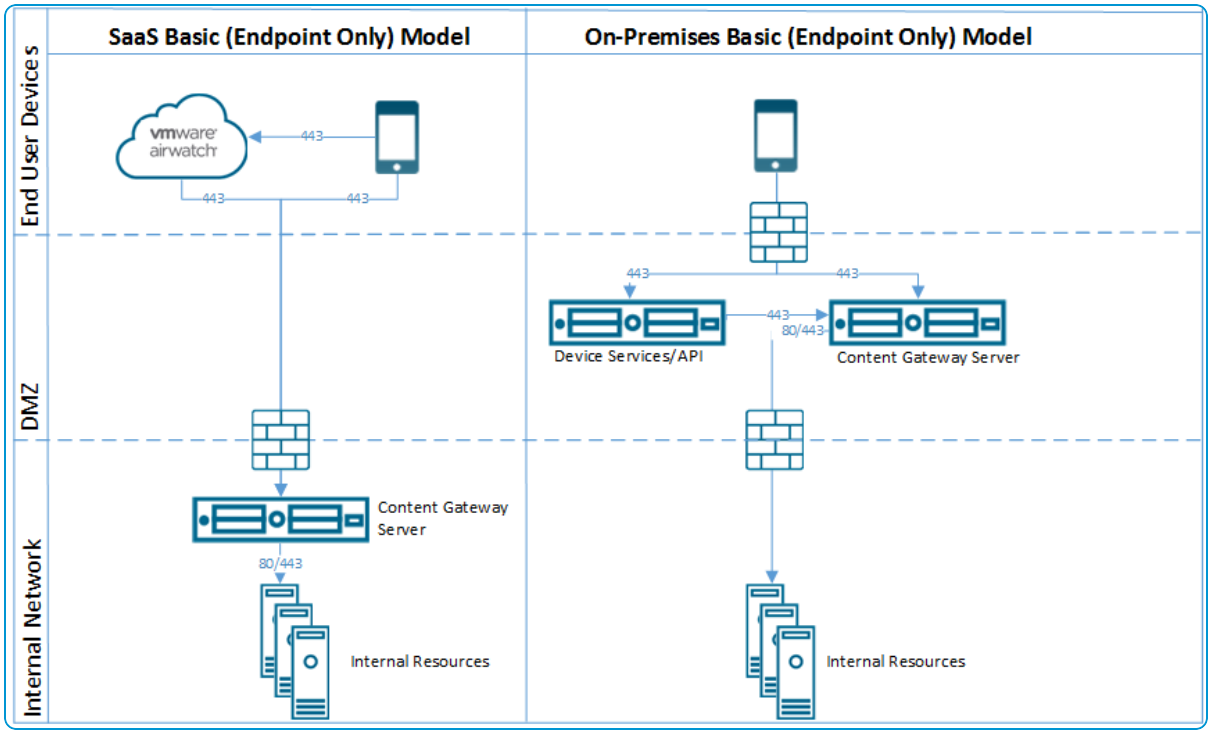
Basic (Endpoint Only) Deployment Model for Content Gateway

The basic endpoint deployment model of VMware AirWatch Content Gateway is a single instance of the product installed on a server with a publicly available DNS.

In the Basic deployment model, VMware AirWatch 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 AirWatch Content Gateway. VMware AirWatch 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, the proper network changes must be made for the VMware AirWatch 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 AirWatch Content Gateway. It provides a layer of security because the public DNS is not pointed directly to the server that hosts the VMware AirWatch Content Gateway.



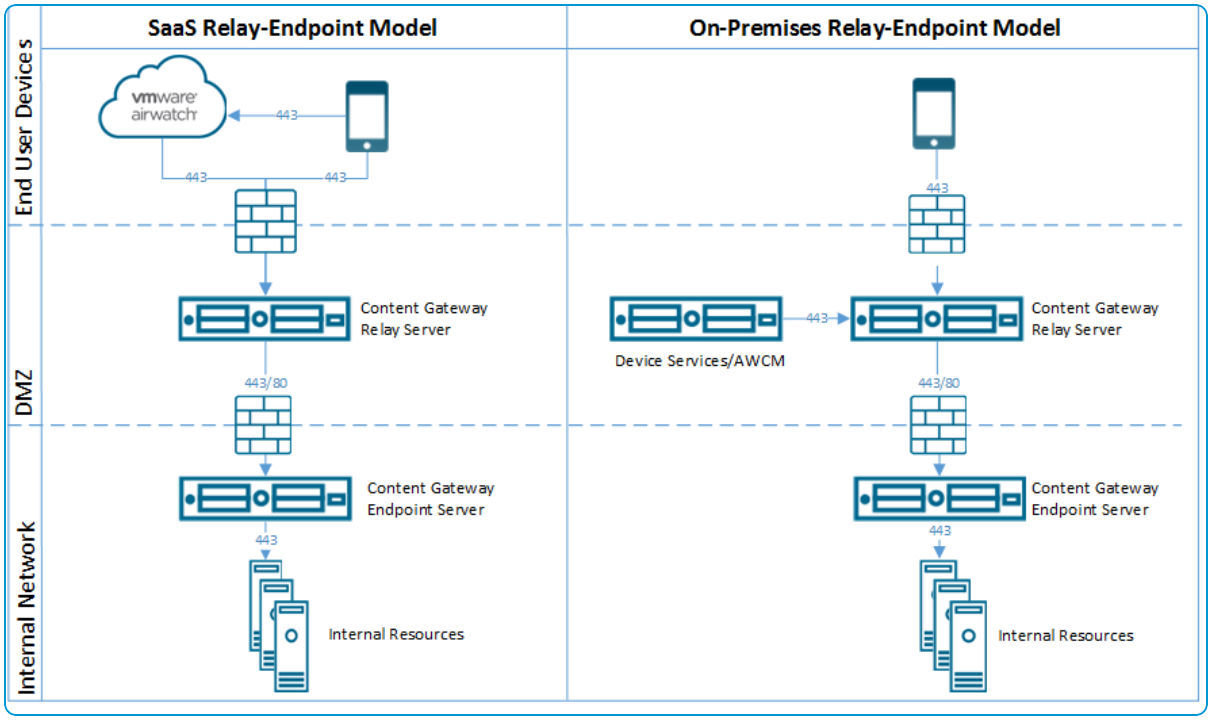
Relay-Endpoint Deployment Model for Content Gateway

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



Chapter 3:
Content Gateway Installation Preparation

Overview

Prepare for the Content Gateway installation to ensure that the procedure runs as smoothly as possible. 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.

Deploying Content Gateway on Unified Access Gateway

If you are 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.

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.
- **Automatic** – Refers to a repository that gets configured by an administrator in the UEM console, but gets synced by end users on their devices.
- **Manual** – Refers to a repository that gets configured in the UEM console, but relies on the end user to add the link manually 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	✓	✓	✓
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	✓	–	–

	Admin	Automatic	Manual
SharePoint Windows Auth	✓	✓	✓
WebDAV	✓	✓	✓
Document Extensions			
Box	✓	✓	✓
CMIS	✓	✓	✓
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	✓ *	✓ *	✓ *

Legend:

¥ =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

✓ * = Supported, with limitations. Access limited to files from repositories previously opened in the Content Locker.

✓ ** = Supported, with limitations. Access limited to files previously downloaded in the Content Locker.

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 following 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 following command:
   a. Run **Set-SmbServerConfiguration -EnableSMB2Protocol $true**.
   b. Select **Y** to confirm.

Content Gateway Requirements for Windows

To deploy VMware AirWatch Content Gateway for Windows, ensure that your system meets the requirements.

Hardware Requirements

Use the following requirements as a basis for creating your VMware AirWatch 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.
Sizing Recommendations				
Number of Devices	**Up to 5,000**	**5,000 to 10,000**	**10,000 to 40,000**	**40,000 to 100,000**
CPU Cores	1 server with 2 CPU Cores*	2 load-balanced servers with 2 CPU Cores each	2 load-balanced servers with 4 CPU Cores each	4 load-balanced servers with 4 CPU Cores each
RAM (GB)	4	4 each	8 each	16 each
Hard Disk Space (GB)	400 MB for installer ~10 GB for log file space**			

*It is possible to deploy only a single AirWatch 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 AirWatch 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: • **Endpoint-Only Configuration Model** – Register the endpoint server. • **Relay-Endpoint Configuration Model** – Register the relay server.

Requirements	Notes
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: • Android does not natively trust all Comodo certificates. • PKCS12 (.pfx) format includes the server certificate, private key, root chain, and password protection.

Windows Software Requirements

Ensure your VMware AirWatch 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	VMware AirWatch recommends setting up Remote Desktop Connection Manager. Download the installer from: https://www.microsoft.com/en-us/download/details.aspx?id=44989
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)	VMware AirWatch recommends setting up Notepad++. Download the installer from: http://download.tuxfamily.org/notepadplus/6.5.1/npp.6.5.1.Installer.exe
IIS 443 bound with SSL certificate	Validate that you can connect to the server over HTTPS (https://<yourAirWatchDomain>.com). At this point, you should see the IIS splash page.
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 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*	5
UEM Console	Content Gateway Endpoint	HTTPS	443*	6

Source Component	Destination Component	Protocol	Port	Note
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	7
Content Gateway Endpoint	CRL: http://csc3-2010-crl.verisign.com/CSC3-2010.crl	HTTP	80	8
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*	5
UEM Console	Content Gateway Relay	HTTPS	443*	6
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*	4
Content Gateway Relay	CRL: http://csc3-2010-crl.verisign.com/CSC3-2010.crl	HTTP	80	8
Content Gateway Endpoint	Network Share-based repositories (Windows file shares)	CIFS or SMB	137-139 and 445	7
* 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 Content Locker to access internal content from websites, such as SharePoint.
3. For applications communicating with internal systems.

   If a firewall resides between the Content Gateway Endpoint and an internal system you are trying to reach, then you will have to open the corresponding port depending on the traffic. For example, Windows Network Files Shares require ports 135 through 139 and 445 to be open in order to access content on Windows file shares.
4. For Content Gateway Relay topologies to forward device requests to the internal Content Gateway endpoint only.
5. For the Device Services server to enumerate the repositories through the content relay and convert them into a format devices can use.
6. For the console server to enumerate the repositories through the content relay for viewing in the UEM console.
7. For devices with the VMware Content Locker to access internal content from Network Shares.
8. For various services to function properly.

Chapter 4:
Content Gateway Configuration

Configure a Content Gateway Node

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, Unified Access Gateway (UAG) is provided as an 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 Windows or Content Gateway to Unified Access Gateway.

Procedure:

1. Navigate to **Groups & Settings > All Settings > 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.

Setting	Description
Installation Type	Select the Operating System for the Content Gateway server.
CONTENT CONFIGURATION	
Choose Configuration Type	Select one of the following configuration types: • **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.

Setting	Description
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.
Server SSL Port	Enter the SSL port number.
CONTENT 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.
SSL Offloading	Enable or disable SSL Offloading.

For more information about configuring ICAP Proxy, see https://support.air-watch.com/articles/115001675368.

5. Select **Save**.

Next Steps

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
9.6	9.2.3	9.2.3
9.5	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 AirWatch Content Gateway installer. The VMware AirWatch Content Gateway installer is available for download on the

AirWatch Resource Portal.

Procedure:

1. From UEM console, navigate to **Groups & Settings > All Settings > Content > 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 **Download Configuration** from UEM console.
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 AirWatch Resource Portal page to download the Content Gateway installer files.
5. Select **Download**.

Deployment Methods

To start the Content Gateway's services, run the downloaded installer. Use the platform and configuration model to determine which server type to install.

- If using the relay-endpoint configuration model for Windows Content Gateway, install the relay server.
- If using the endpoint-only configuration model for Windows Content Gateway, install the endpoint server.

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

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.

Chapter 5:
Content Gateway Installation

Install a Content Gateway Relay Server on Windows

When deploying the Content Gateway using the relay-endpoint model, you must install two instances of the Content Gateway on separate Windows servers. One of the servers on which one instance must be installed is the relay server.

Procedure:

1. Open the installer file on the Endpoint Content Gateway server and then select **Next**.
2. Accept the End User License Agreement and then select **Next**.
3. Select the destination for the downloaded Content Gateway installation files and then select **Next**.
4. Select the path to the downloaded Content Gateway configuration file (XML).
5. Configure the **Content Gateway Setup** screen.
   - **Relay** – Select to first install Content Gateway on the Relay server.
   - **Is this server SSL Offloaded?** – Select if you configured the SSL connection to end before reaching this server.
6. Enter the Certificate Password created when downloading the installer. Click **Next**.
7. Use the drop-down menu to select the Target Site in IIS to install the Workspace ONE UEM application in. Click **Next**.
8. Verify that the Windows Firewall settings allow the following ports.
   - Content Gateway ports
   - Default IIS website port
9. Click **Install** to begin the Content Gateway installation on the server.
10. Click **Finish** to close the Content Gateway installer.
11. Close the installer and verify connectivity to AirWatch. For information about testing the Content Gateway connectivity, see Verify Content Gateway Connectivity on page 19.

Install a Content Gateway Endpoint Server on Windows

When deploying the Content Gateway using the relay-endpoint model, you must install two instances of the Content Gateway on separate Windows servers. Out of the two instances where one instance is installed on the relay server, the other instance must be installed on the endpoint server.

Procedure:

1. Open the installer file on the Endpoint Content Gateway server and then select **Next**.
2. Accept the End User License Agreement and then select **Next**.
3. Select the destination for the downloaded Content Gateway installation files and then select **Next**.
4. Select the path to the downloaded Content Gateway configuration file (XML).
5. Configure the **Content Gateway Setup** screen.
   - **Endpoint** – Select the 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 that the Windows Firewall settings allow the following ports.
   - Content Gateway ports
   - Default IIS website port
8. Click **Install** to begin the Content Gateway installation on the server.
9. Click **Finish** to close the Content Gateway installer.
10. Close the installer and verify connectivity to AirWatch. For information about testing the Content Gateway connectivity, see Verify Content Gateway Connectivity on page 19.

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 > Content > Content Gateway** in the UEM console.
2. Select **Test Connection** to verify the connectivity.

Chapter 6:
Content Gateway Management

Upgrade Content Gateway

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 > Content > Content Gateway**.
2. Select the installer link for the appropriate operating system.
3. Enter and confirm an installer password with a minimum of six characters and select **Download**.

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

4. 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.

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 the HTTP status codes.

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.