VMware AirWatch Mobile Content Management Guide

End-to-end information for configuring secure mobile access to your organization's content

Workspace ONE UEM v9.6

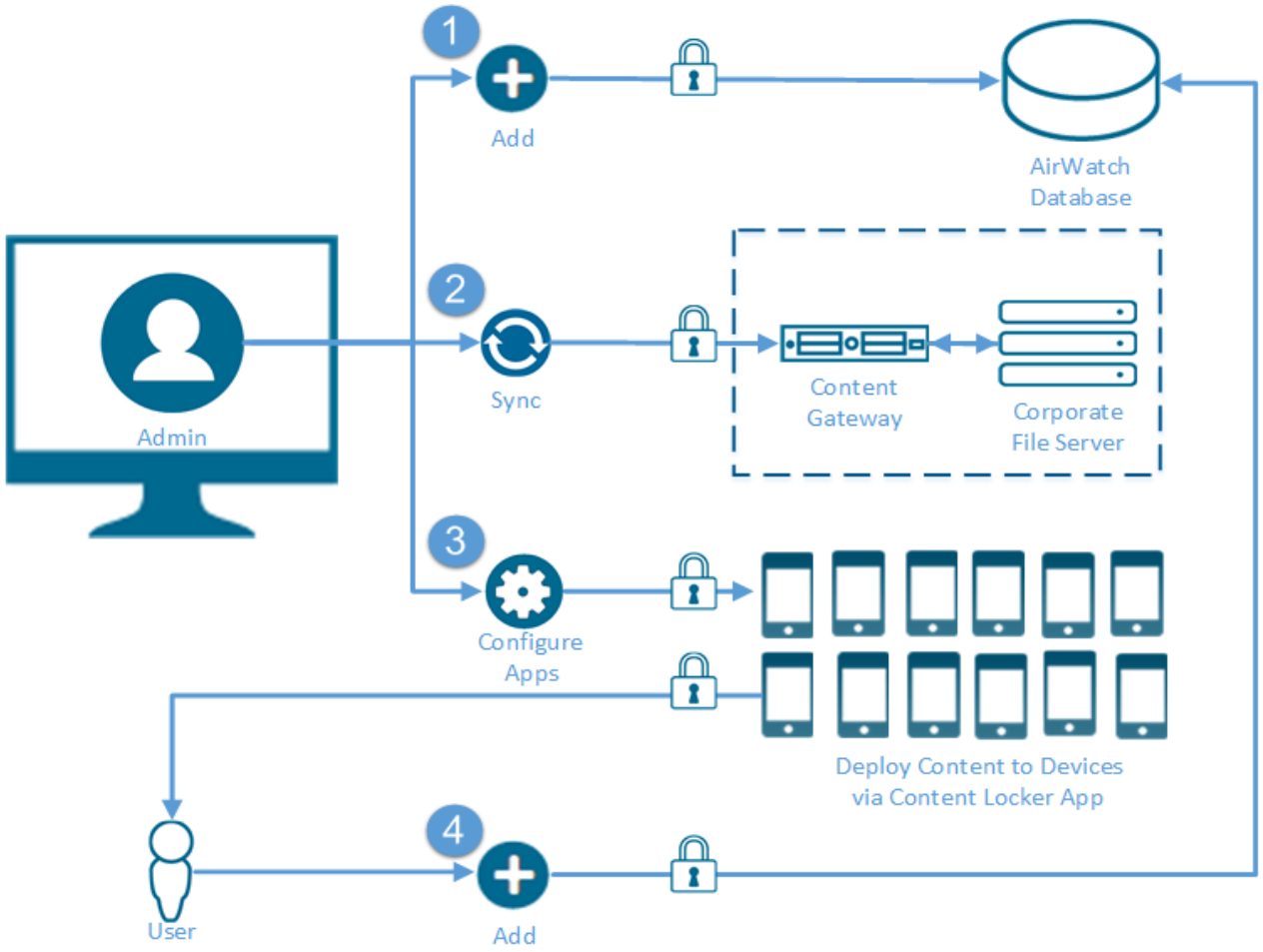
Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Table of Contents

Chapter 1:
Introduction to Mobile Content Management

The Mobile Content Management™ (MCM) solution helps your organization address the challenge of securely deploying content to a wide variety of devices using a few key actions. Use the Workspace ONE UEM console to create, sync, or enable a file store known as a repository. Once configured this content deploys to end-user devices with the VMware Content Locker.

To understand how the content management works, review the following outline.



1. **AirWatch Managed Content Repository** – Refers to a repository where Workspace ONE UEM administrators with the appropriate permissions have complete control over the files that get stored within it.
2. **Corporate File Server** – Refers to an existing repository that resides within an organization's internal network. Depending on an organization's structure, the Workspace ONE UEM administrator might or might not have administrator permissions for the corporate file server.
3. **VMware Content Locker** – Refers to the app that deploys to end-user devices, enabling access to content within the configured set of parameters.
4. **Personal Content** – Refers to a location where end users have complete control over the files that get stored within it.

Requirements for Mobile Content Management

Mobile Content Management (MCM) provides a flexible array of services to implement. Each service has its own unique set of requirements. Before configuring MCM, it is important to review the services you want to configure, and meet their basic requirements.

Component	Requirement & Description
Software and Hardware Requirements	
Supported Browsers	The Workspace ONE Unified Endpoint Management (UEM) console supports the latest stable builds of the following web browsers. • Chrome • Firefox • Safari • Internet Explorer 11 • Microsoft Edge **Note:** If using IE to access the UEM console, navigate to **Control Panel > Settings > Internet Options > Security** and ensure you have a security level or custom security level that includes the **Font Download** option being set to **Enabled**. If you are using a browser older than those listed above, upgrade your browser to guarantee the performance of the UEM console. Comprehensive platform testing has been performed to ensure functionality using these web browsers. The UEM console may experience minor issues if you choose to run it in a non-certified browser.

App Requirements

		Content Locker	Content Locker Sync	Outlook Add-In
Platform Requirements	iOS 7.2+	√		
	Android 3.2+	√		
	Windows 7	√*	√	√
	Windows 8	√	√	√
	Windows 10	√	√	√
	10.9 Mavericks+		√	
Framework Requirements	.NET 4.0.3+	√*		√
	.NET 4.5+		√	
	Mono		√	
Visual Studio Requirements	Visual Studio 2010 v10.0.50903	√*		√
	Visual C++ 2008		√	

Component	Requirement & Description			
Other	Link Sharing enabled			√
	Microsoft Outlook 2007+ (32-bit or 64-bit)			√
***Desktop only**				
Role Requirements				
Admin Roles	**Select a role that has *Content*, *Content Device Install*, and *Content Device Remove* enabled by default.** Grants access the content management page and control of content distribution. For more information on creating roles, read the **Roles and Added Resources Guide**.			
End-User Roles	**Enable *Manage Content* and grant *Full Access*** For more information on creating roles, read the **Roles and Added Resources Guide**.			
Repository Requirements				
AirWatch Managed Content	**Configure the category structure before uploading content** You cannot add subcategories to categories that have content in them.			
Corporate File Server Content	**Install Content Gateway** Install Content Gateway to establish a connection in instances where the Workspace ONE UEM server domain cannot access a Corporate File Server. See Support for Corporate File Servers on page 15 to review which Workspace ONE UEM supported repositories require, support, or do not support Content Gateway. For comprehensive installation instructions, read the **Content Gateway Installation Guide**.			
Personal Content	**Purchase Appropriate Bundle or Service** Not all content management packages include personal content management.			
Alternative File Storage Requirements				
Local File Storage	**Determine Appropriate Solution for Organization** For more information on available options, see Local File Storage for Workspace ONE UEM Managed Content on page 25.			
Remote File Storage	**Determine Appropriate Solution for Organization** For more information on available options, see File Storage on page 10.			

Component	Requirement & Description
Personal Content Current availability limited to content stored in the Personal Content repository. Not all content management packages include personal content management.	
Install Remote File Storage Server If using Remote File Storage as an alternative storage option for Personal Content, follow the installation instructions outlined in the **Remote File Storage Installation Guide**.	
Optional Security Component Requirements	
Content Rendering Engine	**Determine Appropriate Solution for Organization** Leverage this product to address security concerns for content shared from the Self-Service Portal.
Install Remote File Storage Server The Content Rendering Engine requires a working instance of the Remote File Server. Installation instructions are outlined in the **Remote File Storage Installation Guide**.	

Component	Requirement & Description
Install Content Rendering Engine Follow the installation instructions outlined in the **Content Rendering Engine Installation Guide**.	
Onboarding	**Meet minimum app and OS requirements** • iOS VMware Content Locker v2.4+ • iOS 7+ device

Chapter 2:
File Storage

Overview of Storage Options by Content Type

Various content types are available for configuration in the Workspace ONE UEM console that can be deployed to the VMware Content Locker app on end-user devices. Although the content type does not impact the deployment location, back end storage varies by content type.

To gain insight about the storage options available for each content type, review the following chart. Learn about the additional configuration and components requirements for each storage option.

	Configurations	Components	Notes
Workspace ONE UEM Managed Content			
Workspace ONE UEM Database	X	X	
Local File Storage	√	√	Modify at a Global level Organization Group on-premises only
Corporate File Servers			
Workspace ONE UEM Database	X	X	Synced content only stores metadata on the Workspace ONE UEM Database
Network Repositories	√	√/X	Some repositories require Content Gateway. Requirements vary by repository type.
Personal Content			
Workspace ONE UEM Database	X	X	
Local File Storage	√	√	Modify at a Global level Organization Group on-premises only
Remote File Storage	√	√	Personal Content only

Content Management Enterprise Integration Solution

Overview

The Content Management solution provides a suite of enterprise integration components designed to address the unique challenge of securing the content on mobile devices. The available Content Management components include Content Gateway, Remote File Storage (RFS), and Content Rendering Engine (CRE).

Content Gateway

The Content Gateway, together with VMware Content Locker, lets your end users securely access content from an internal repository. This means that your users can remotely access their documentation, financial documents, board books, and more directly from content repositories or internal file shares. As files are added or updated within your existing content repository, the changes will immediately be reflected in VMware Content Locker, and users will only be granted access to their approved files and folders based on the existing access control lists defined in your internal repository. Using the Content Gateway with VMware Content Locker allows you to provide unmatched levels of access to your corporate content without sacrificing security.

Remote File Storage

Remote File Storage provides an on-premises storage alternative for Personal Content. Personal Content refers to a repository consisting of files uploaded and managed by end users. End users add files on their devices with VMware Content Locker, from any supported web browser with the Self-Service Portal, and from their personal computer with Content Locker Sync. By default, this content is stored in the Workspace ONE UEM database. For SaaS customers, that means Personal Content stores in the cloud by default. In some use cases, storing certain types of content in the cloud poses a security risk. Use Remote File Storage (RFS) to store Personal Content in a dedicated on-premises location.

Content Rendering Engine

The Content Rendering Engine (CRE) integrates with Remote File Storage to secure shared Personal Content. When an end user shares Personal Content from the Self-Service Portal, CRE converts the shared content into a rendered image of the source file. These shared images eliminate the need to download shared content, and enforce read-only permissions.

CRE enforces read-only permissions for the following file types.

- Word (doc, docx)
- Power Point (ppt, pptx)
- Excel (xls, xlsx)
- JPEG, JPG
- BMP
- PNG
- PDF
- Text

Set Content Storage Capacity

Storage capacity refers to the amount of space allocated for managed and personal content in an Organization Group and its child groups.

To set storage capacity:

1. Navigate to **Groups & Settings > All Settings > Admin > Storage** at a *Customer* or *Global* organization group level.
2. Select **Content** from the **Type** drop-down menu.

3. Select the **Edit** icon. Complete the settings.

Setting	Description
Organization Group Name	Specify the group to which you want to apply content storage restrictions.
Capacity	Set maximum storage space in MB allocated to content stored in the Workspace ONE UEM database. The default storage for Content Locker provided by VMware AirWatch to SaaS customers is 5 GB.
Overage Allowed	Enter the amount of overage you want to allow, if any. For SaaS customers, this value is not configurable.
Max File Size	Use the default value of 200 MB as the maximum size for uploads. If operating against this recommendation, 2 GB is the upper limit.
Encryption	Encrypt the content with AES - 256 file level encryption. Enabling encryption triggers the File Encryption Migration scheduler to begin migrating any unencrypted data it finds.

4. Select **Save**.

Restrict File Extensions

Specify file type permissions by creating a whitelist or blacklist for Managed, Corporate File Server, and Personal content. This restriction hides blocked file types based on their extension from being visible in the UEM console or within Content Locker and so prevents them from being downloaded or uploaded to Content Repositories.

1. Navigate to **Content > Settings > Advanced > File Extensions**.

2. Set the **Allowed File Extensions**.

Setting	Description
Whitelist	Enter the file extensions you want to include. Separate extensions using a new line, a comma, or a space.
Blacklist	Enter the file extensions you want to exclude. Separate extensions with a line break, a comma, or a space.
All	Select to allow any file type for upload or sync.

3. Select **Save** to apply the configuration.

   Once restrictions are applied, you can anticipate the following responses.

Response	Who	What	Where	Repository
Error Message	Administrator	Manually adds a restricted file to the content repository	Console	AirWatch Managed
Error Message	End User	Manually adds a restricted file	Device	Personal Content

Silent interaction	Administrator	Syncs with a corporate file server that contains a restricted file	Console	Corporate File Server
Silent interaction	End User	Syncs with a corporate file server that contains a restricted file	Device (through Content Locker)	Corporate File Server

Chapter 3:
Corporate File Servers

Overview

The Content Management solution supports integration with your Corporate File Servers (CFS). Corporate File Servers refer to existing repositories that reside within an organization's internal network.

Features

Corporate File Server integration supports the following features:

- Secure integration
- Protect access to organization's internal network
- Advanced integration options using Content Gateway and Remote File Storage

Security

The Content Management solution provides the following security options:

- SSL encryption for data transit
- Control access and download rights of Workspace ONE UEM administrators
- Content stored within organization's network
- Only metadata stored in Workspace ONE UEM database. Support for review and management of the stored metadata.

Deployment

Depending on an organization's structure, the Workspace ONE UEM administrator might or might not have administrative permissions for a CFS. After the Content Management solution is integrated with CFS, the end-user devices can sync the content from the servers using VMware Content Locker.

Enable End-User Access to Corporate File Server Content

Sync your network's existing corporate file servers with Workspace ONE UEM by configuring an Admin Repository, an Automatic User-Added Repository, or a Manual User-Added repository. The available configurations impact the "trigger" that initiates the syncing of content to devices.

Use this macro-level configuration overview to gain insight into the start-to-finish process of enabling end-users access to the Corporate File Server content.

1. Configure a repository in the UEM console.
2. Download the configured Content Gateway installer.
3. Run the Content Gateway installer.
4. Verify connectivity between the UEM console and Content Gateway.
5. Evaluate your organization's need for multiple Content Gateway nodes. Global organizations with concerns about latencies caused by geographical separations can use this functionality.
6. Configure an Admin repository or sync Corporate File Servers (CFS) in the UEM console.

   If configuring an Admin Repository, select **Test Connection** to ensure connectivity.
7. Configure VMware Content Locker in the UEM console.
8. Deploy Workspace ONE UEM Applications to your device fleet.

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	✓	✓	✓

	Admin	Automatic	Manual
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	✓	–	–
SharePoint Windows Auth	✓	✓	✓

	Admin	Automatic	Manual
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.

Configure an Admin Repository

Configure an Admin Repository to sync your network's existing corporate file servers with Workspace ONE UEM. After the sync, end users can access the Corporate File Server content from their devices.

To configure an Admin Repository:

1. Navigate to **Content > Repositories > Admin Repositories** in the UEM console.
2. Select **Add**.
3. Configure the settings that appear:

Setting	Description
Name	Label the content directory.
Type	Select a Corporate File Server from the drop-down menu.
Link	Provide the full path to the directory location rather than the root domain. **Example:** http://SharePoint/Corporate/Documents A URL copied directly from a web browser might not have permission to access a server for certain repository types.
Organization Group	Assign Corporate File Server access to a selected group of users.
Authentication Type	Select the access level admins have to Corporate File Servers from the UEM console. • **None** – Prevent administrators from viewing and downloading Corporate File Server content from the UEM console. • **User** – Permit browsing of the repository file structure within the UEM console. Enter credentials into the **Username**and**Password** text boxes that appear.
Access via Content Gateway	Use the Content Gateway if the Workspace ONE UEM server's domain cannot access the Corporate File Server.
Content Gateway	Identify the unique name of the appropriate Content Gateway node from the drop-down menu.
Allow Inheritance	Permit child organization groups to inherit the same access permissions as their parent organization group.
Allow Write	Permit end users to create and upload files and folders, edit documents, and check in or check out files to external repositories on their devices.
Allow Delete	Permits remote content delete for the Network Share repository. With this feature, the end user can delete their content permanently from the Network Share repository using the Content Locker.

4. Select **Test Connection** to verify connectivity. A successful test result indicates the corporate file server integrated successfully.
5. Enter the values in the remaining text boxes under the Security, Assignment, and Deployment tabs. Select**Save**.

Link Configuration Best Practices

This specific rule applies to SharePoint 2013, Office 365, and the later versions. Some URLs cannot be accessed using applications and services, and can only be accessed using a web browser. If a 'browser only' URL gets entered as the link when configuring Content Gateway, the connection fails.

To ensure that Content Gateway gets configured with the correct link, follow the procedure:

1. Enter the URL in the browser.
2. Navigate to **PAGE > Edit Properties > View Properties**.
3. Right click and copy link address.
4. Paste the address into the **Link** text box in the UEM console.

Enable Users to Sync Corporate File Servers

Integrate Workspace ONE UEM with existing content repositories by configuring an Automatic or Manual Template that end users sync to from their devices. After the sync, end users access the Corporate File Server content from their devices.

The steps can vary when configuring an Automatic or Manual Template. The differences are marked in *italics*.

1. Navigate to the appropriate page in the UEM console:

Corporate File Server Type	Location
Automatic Template	**Content > Repositories > Templates > Automatic**
Manual Template	**Content > Repositories > Templates > Manual**

2. Select **Add**.
3. Complete the text boxes that appear. The text boxes can change when configuring an Admin Repository, an Automatic Template, or a Manual Template. The differences are marked in *italics*.

Setting	Description
Name	Label the content directory.
User Repository Name *(auto template only)*	Use look-up values to name the repository after the end user within the VMware Content Locker.
Type	Select a Corporate File Server from the drop-down menu.
Link	A URL copied directly from a web browser might not have permission to access a server for certain repository types.
Link*(auto template only)*	Use look-up values to create a repository when an end user accesses the VMware Content Locker. **Example:** https://sharepoint.acme.com/share/{EnrollmentUser}
Link*(manual template only)*	Provide the path to the directory location using * as a wildcard for a domain link. **Example:** http://*.sharepoint.com
Organization Group	Assign Corporate File Server access to a specified group of users.
Access via Content Gateway	Use the Content Gateway if the Workspace ONE UEM server's domain cannot access the Corporate File Server.
Allow Inheritance	Allow child organization groups to inherit the same access permissions as their parent organization group.

Setting	Description
Allow Write	Allow end users to create and upload files and folders, edit documents, and check in or check out files to external repositories on their devices.

4. Complete the remaining Security, Assignment, and Deployment tabs and select **Save**.
5. *If configuring a **Manual Template***, direct end users to the Self Service Portal where they can manually add and access their repository.

Configure Repository Details

Configure the Security, Assignment, and Deployment details to ensure the content in the Managed and the Corporate File Server repositories remain secure.

1. On the Security tab, complete the text boxes to control how the end users share and move sensitive documents outside of corporate mediums. The Force Encryption setting has been removed since Workspace ONE UEM console version 9.5. The VMware Content Locker app encrypts all the files by default, whether the setting is available or not.

Setting	Description
Document Sharing	Disable the sharing settings for maximum security. You can enable them for configuring end-user collaboration.
Access Control	Set to **Allow Offline Viewing** to give end users the most viewing freedom for their document. Configure **Allow Online Viewing Only** to ensure that all devices accessing content are compliant, as Workspace ONE UEM cannot scan offline devices for compliance.
Allow Open in Email	Allow the content to open in emails.
Allow Open in Third Party Apps	Give the permission to open this content in other applications. You can set a list of approved apps in the SDK Profile.
Allow Saving to Other Repositories	Select to allow your end users to save this file to their Personal Content.
Enable Watermark	Select to add a watermark overlay to the file. Configure the Overlay Text for the watermark as part of an SDK profile.
Allow Printing	Give the end users the permission to print PDF documents from the iOS VMware Content Locker using AirPrint server. Once printed, content falls out of the control of the Workspace ONE UEM administrator.
Allow Edit	This setting only applies to write-enabled repositories.

2. Configure the **Assignment** settings to control which users have access to content. This function ensures that only authorized employees have access to confidential or sensitive material and allows you to set up a tiered hierarchy of content access.

Setting	Description
Device Ownership	Define as **Any**, **Corporate-Dedicated**, **Corporate-Shared**, **Employee Owned** or **Undefined**.
Organization Groups	To assign the content to a new group, start typing in the text box.
User Groups	Designate groups if you are integrating with Directory Services or custom user groups.

3. Use the **Deployment** settings to control how and when your end users access content.

Setting	Description
Transfer Method	Specify **Any** method or **Wi-Fi Only** from the drop-down menu. Restricting transfers to Wi-Fi forces devices to check in with Workspace ONE UEM to ensure compliance.
Download While Roaming	Enable to allow your end users to download the content while roaming.
Download Type	Set to deploy content one of two ways: • **Automatically** – Installs on devices when content becomes available. • **On Demand** – Installs on devices only at the end user's request.
Download Priority	Define to let your end users know if the content download is **Normal**, **High**, or **Low** priority.
Required	Select to flag the content as required in the VMware Content Locker. End users must download and review the required content in order for their devices to maintain compliance with Workspace ONE UEM.
Effective Date	Specify to configure a limited range of content availability.
Expiration Date	Specify to configure a limited range of content availability.

4. Select **Save**.

Chapter 4:
AirWatch Managed Content Repository

Overview

The Workspace ONE UEM Managed Content repository refers to a location where administrators with the appropriate permissions have complete control over the files that gets stored within it. The end users can access the added content using VMware Content Locker in the repository labeled AirWatch Managed.

Features

Managed Content repository provides the following features:

- Uploading of files manually
- Options to configure and provide permissions for individual files
- Sync options to control content accessed on end-user devices
- List View for advanced file management options

Security

To protect the content that is stored and synced from the repository to end-user devices, the following security features are available:

- SSL encryption secures data during transit between the UEM console and end-user devices
- Roles with the security pin for controlled access to the content

Deployment

The Managed repository content is stored in the Workspace ONE UEM database. You can choose to host the database in the Workspace ONE UEM cloud or on-premises, depending on your deployment model. For more information, seeConfigure the AirWatch Managed Content Category Structure on page 23.

Configure the AirWatch Managed Content Category Structure

Content categories help keep the AirWatch Managed repository content organized in the UEM console and the Content Locker. Configure the category structure for the Workspace ONE UEM Managed content before uploading content to the UEM console.

To add a category:

1. Navigate to **Content > Categories** > **Add Category**.
2. Configure the settings that appear and **Save**.

Setting	Description
Managed By	Select the organization group or groups you want to apply the category.
Name	Enter a name that is easily recognizable and applies to a clear set of content.
Description	Provide a brief description of the category.

To add a subcategory to your category structure:

1. Select **Add**  from the **Action Menu**.
2. Configure the settings that appear and **Save**.

Setting	Description
Managed By	Review the organization group of the parent category that populates by default.
Name	Enter a name that is easily recognizable and applies to a clear set of content.
Description	Provide a brief description of the subcategory.

Upload Content to the AirWatch Managed Repository

Add files to the Managed Content repository by manually uploading and configuring them in the UEM console. The repository stores its content in the Workspace ONE UEM database by default, and syncs with the VMware Content Locker app, delivering content to end users' devices.

To upload files:

1. Navigate to **Content > List View**.
2. Select **Add Content** and choose **Select Files**.
3. Select an individual file for the upload from the dialog box.
4. Configure content **Info** settings.

Setting	Description
Name	Review the filename that automatically populates in this text box.

Setting	Description
Organization Group	Review the organization group to which this content deploys.
File	Review the file that populates in this text box.
Storage Type	Ensure that the text box displays AirWatch Managed.
Version	Ensure that the version number is 1.0 as you are adding this content to the UEM console for the first time. You can upload new versions from the Action menu in the AirWatch Managed List View.
Description	Provide a description of the files you upload.
Importance	Set the content importance as **High**, **Normal**, or **Low**.
Category	Map the uploaded content to a configured Category.

5. Provide additional metadata about the content in the **Details** settings.

Setting	Description
Author	Name the author of the file.
Notes	Provide notes on the file.
Subject	Provide a subject.
Keywords	List keywords and topics that this file covers.

6. Configure the content.

Upload Workspace ONE UEM Managed Content in Batches

Use batch imports to bypass external file share integration in a dedicated SaaS or on-premises deployment with a hardened network.

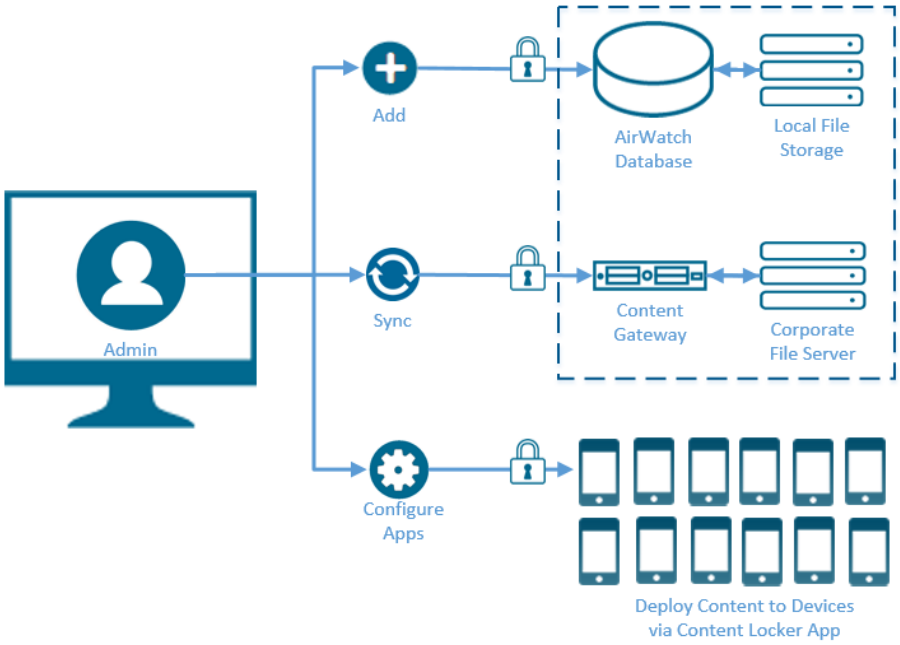
To upload a batch import:

1. Navigate to **Content** > **Batch Status**.
2. Select **Batch Import**.
3. Provide a **Batch Name** and a **Batch Description**.
4. To download a .csv template file, select the information icon ( ).
5. Fill out the CSV file with the file path and other information for content you want to upload.
6. Select **Choose File** and choose the .csv that you created.
7. Select **Open** to select the .csv.
8. Select **Save** to upload your populated Batch File.

Local File Storage for Workspace ONE UEM Managed Content

Local File Storage separates the managed content from the Workspace ONE UEM database, storing it in a dedicated, on-premises location with a connection to the Workspace ONE UEM instance.

Managed content is stored in the Workspace ONE UEM database by default. However, uploading a large volume of managed content can cause issues with the database performance. In this case, on-premises customers can free up space in the database by moving the managed content to an integrated Local File Storage solution.



File Storage

Certain Workspace ONE UEM functionality uses a dedicated file storage service to handle processing and downloads, which reduces the overall burden on your Workspace ONE UEM database and increases its performance. It also includes certain Workspace ONE UEM reports, internal application deployment, and Workspace ONE UEM-managed content. When you enable file storage for any of these functionalities, it is applied to the others automatically. Setting up file storage causes all reports, all internal applications, and all managed content to be stored there.

Configuring file storage manually is only applicable to on-premises customers. It is automatically configured for SaaS customers.

Workspace ONE UEM Reports

As of console version 9.0.2, three new reports were added that appear the same as existing reports but use a revamped back-end framework. This new framework generates reports with greater reliability and faster download times. To take advantage of these benefits, you must set up file storage.

For more information about these reporting updates, see the following Knowledge Base article: https://support.air-watch.com/articles/115002346928.

Internal Applications

When file storage is enabled, all internal application packages that you upload through the UEM console are stored in a file storage location.

File storage is required to deploy Win32 applications (IPA, PAK, APPX, MSI, EXE, and so on) and macOS applications (.dmg, .pkg, .mpkg, and so on) from the Apps & Books area of the UEM console. This feature is called software distribution.

Workspace ONE UEM Managed Content

You can separate the managed content from the Workspace ONE UEM database by storing it in a dedicated file storage location. Uploading large amounts of managed content might cause issues with database performance. In this case, on-premises customers can free up space in the database by moving the managed content to an integrated local file storage solution.

Personal content also moves to the file storage solution is enabled. By default, personal content is stored in the SQL database. If you have a Remote File Storage enabled, personal content is stored in the RFS and not in the file storage or SQL database.

File Storage Requirements

To set up local file storage, you must meet the following requirements.

Important: File Storage is required for Windows 10 Software Distribution.

Create the Shared Folder on a Server in Your Internal Network

- File storage can reside on a separate server or the same server as one of the other AirWatch application servers in your internal network. It is only accessible to components that require access to it, such as the Console and Device Services servers.
- If the Device Services server, Console server, and the server hosting the shared folder are not in the same domain, then establish Domain Trust between the domains to avoid the authentication failure. If the Device Services server or Console server is not joined to any domain, then supplying the domain during service account configuration is sufficient.

Configure the Network Requirements

- **If using Samba/SMB** – TCP: 445, 137, 139. UDP: 137, 138
- **If using NFS** – TCP and UDP: 111 and 2049

Allocate Sufficient Hard Disk Capacity

Your specific storage requirements may vary depending on how you plan to use file storage. The file storage location should have enough space to accommodate the internal apps, managed content, or reports you intend to use. Take into the account the following considerations.

- If you enable caching for internal apps or content, then a best practice is to size the Device Services server for 120 percent of the cumulative size of all the apps/content you need to publish.

- For storing reports, your storage requirements depend on the number of devices, the daily amount of reports, and the frequency with which you purge them. As a starting point, you should plan to allocate at least 50 GB for deployment sizes up to 250,000 devices running about 200 daily reports. Adjust these numbers based on the actual amount you observe in your deployment. Apply this sizing to your Console server as well if you enable caching.

Create a Service Account with Correct Permissions

- Create an account with read and write permissions to the shared storage directory.
- Create the same local user and password on the Console, Device Services, and the server that is being used for File Storage.
- Give the local user read/write/modify permissions to the file share that is being used for the File Storage Path.
- Configure the File Storage Impersonation User in AirWatch with the local user.

You can also use a domain service account instead of a local user account.

Configure File Storage at the Global Organization Group

Configure file storage settings at the Global organization group level in the UEM Console.

For information about configuring Local File Storage, see Configure Local File Storage.

Enable File Storage for Content

Configure file storage for content by using the following procedure.

1. At the Global organization group level, navigate to **Groups & Settings > All Settings > Installation > File Path** and scroll to the bottom of the page.
2. Select the **File Storage Enabled** slider and configure the settings. When file storage is enabled, you can configure an external repository in which files are stored. A disabled setting means that files are stored as binary large objects in the database.

Setting	Description
File Storage Path	Enter the path files are to be stored in the following format: \\{Server Name}\{Folder Name}, where Folder Name is the name of the shared folder you create on the server.
File Storage Caching Enabled	When enabled, a local copy of files requested for download is stored on the Device Services server as a cache copy. Subsequent downloads of the same file retrieve it from the Device Services server as opposed to file storage. If you enable caching, consider accommodating for the amount of space needed on the server. For more information, see File Storage Requirements on page 26. If you integrate with a CDN, then apps and files are distributed through the CDN provider, and a local copy is not stored on the Device Services server. For more information, refer to the **VMware Workspace ONE UEM CDN Integration Guide** (https://resources.air-watch.com/view/8cr52j4hm6xfvt4v2wgg/en).
File Storage Impersonation Enabled	Select to add a service account with the correct permissions.

Setting	Description
File Storage Impersonation Username	Provide a valid service account user name to obtain both read and write permissions to the shared storage directory.
Password	Provide a valid service account password to obtain both read and write permissions to the shared storage directory.

3. Select the **Test Connection** button to test the configuration.

Chapter 5:
Personal Content Repository

Overview

The Content Management solution provides the end users with options to manage their personal content on enrolled devices. The Personal Content repository is a location where end users have complete control over the files that are stored within it. Only the deployments that purchased the appropriate licenses can configure the security permissions that enable this repository for end users.

Features

When the Personal Content repository is enabled, the end users are provided with the following capabilities:

- Upload and download the personal content to the repository.
- Access repository content from multiple mediums.
- Manage the personal content stored in the repository.

Accessibility

The end users can access and upload the content to the repository using:

- VMware Content Locker application
- Supported web browser with the Self-Service Portal
- Personal computer with VMware Content Locker Sync

Security

To protect the personal content of end users, Content Management solution provides the following security features:

- The data in transit is secured using SSL encryption.
- The content that is stored and deployed in the Personal Content repository is protected with AES 256-bit encryption.
- VMware Content Locker v2.2 and later for iOS uses the NSFileProtectionComplete class to store the content.

Deployment

Depending on the deployment model, you can store Personal Content repository files in the Workspace ONE UEM database that is hosted on-premises or in the cloud. Alternatively, you can use the Remote File Storage to store the personal content on-premises, regardless of the deployment model.

Storage

The Content Management solution provides you the options to allocate and manage the storage quota for the Personal Content repository. You can also configure individual user storage quotas in the UEM Console at**Groups & Settings > All Settings > Content > Personal Content**.

Enable Personal Content

Enable the Personal Content repository to serve as a dedicated storage location for the content uploaded by the end user.

1. At a Customer level Organization Group, navigate to **Groups & Settings > All Settings > Content > Personal Content**.
2. Set Personal Content to **Enabled** to create a personal content repository, and configure the available fields.
3. Configure **Storage Allocations**.

Setting	Description
Storage Quota	Divide the allocated storage between the Workspace ONE UEM Managed and Personal Content repositories, dedicating an amount of the available storage to Personal Content. By default, all available storage gets dedicated to Personal Content, indicated by the far-right position of the slider.
User Quota	Set the maximum amount of storage any one user can consume, in MB. This quota applies to users in the same Organizational Group hierarchy as Storage Quota.
User Group Quota(s)	Select **Add New** and configure storage exceptions on a user group basis.

4. Configure Shared Links by setting Link Sharing to **Enabled** and enabling the options that appear. Once enabled, end users can share files as links from the VMware Content Locker and the Self-Service Portal.

Setting	Description
Link Sharing	Enable link sharing of documents.
Auto Expire Days	Enable and fill in a numerical value to specify the number of **Days** links remain available for sharing. Disable to leave the option open for end users to configure when they share their links.

Setting	Description
Auto Expire Downloads	Enable and input a numerical value to set the maximum number of **Downloads** before the link expires. Disable to leave the option open for end users to configure when they share their links.
Require Password Protection	Enable and set the **Minimum Length** in characters and the **Complexity** of the password. Disable to leave the option open for end users to configure when they share their links.

5. Configure Shared Folders by setting Folder Sharing to **Enabled** and enabling the options that appear. Once enabled, end users can share folders from the VMware Content Locker and the Self-Service Portal.

Setting	Description
Share with User Groups	Enable to share folders with entire user groups instead of manually listing each user.
Available Sharing Roles	Set the roles available to end users sharing their folders.
Share with External Users	Enable end users to share folders with users external to their Organization Group.
Available Sharing Roles	Set the access privilege role for those users that end users share a folder with. See the Folder Sharing Roles matrix, for an overview of sharing roles and their permissions.
User Quota	Leave the quota at 0 to have all external user uploads count against the folder sharer's quota. Set a quota to give external users dedicated space for uploads.

6. Configure **Email Notifications**.

Setting	Description
Email Notifications	Enable to alert users through email when a folder is shared with them.

7. Set the Data Loss Prevention settings to **Disabled** for maximum security, or set it to **Enabled** for collaboration.

Setting	Description
Allow Open in Email	Enable to allow content to open in emails. Disable for maximum security.
Allow Open in Third Party Apps	Enable to open personal content in other applications. You can set a list of approved apps in the SDK Profile. Disable for maximum security.
Allow Printing	Enable iOS devices to print personal content PDFs using AirPrint. Disable for maximum security.
Watermark	Enable to apply a dynamic watermark to the files rendered in the HTML5 Viewer. By default, the user's email is applied as the file's watermark. You can reconfigure the watermark text in the SDK.

8. Select **Save** to complete your configuration.

Roles for Folder Sharing

Folder sharing roles refer to the permissions that end users can assign when sharing a folder. These permissions apply to the user group or external user with whom an end user shares a folder.

	Owner	Co-Owner	Editor	Reader	Viewer
View File and Folders	✓	✓	✓	✓	✓
Download Files to Computer	✓	✓	✓	✓	
Add Comments to Files	✓	✓	✓	✓	✓
Upload Files to Folder	✓	✓	✓		
Delete Files or Subfolders	✓	✓	✓		
Edit Files	✓	✓	✓		
View Other Folder Collaborators	✓	✓	✓		
View Other Collaborators Activity in Feed	✓	✓	✓	✓	
Modify Sharing of Folder	✓	✓			
Generate Shared Links to Files	✓				
Transfer Folder Ownership	✓				

Configure Personal Content Quota Exceptions

Use the User Storage screen to edit storage quotas for end users on an individual basis, and perform additional management actions. These edited settings provide a final layer of granularity, and override any limits set when configuring Personal Content.

1. Navigate to **Groups & Settings > All Settings > Content > User Storage**.
2. To override user storage on an individual level, select **Edit**. It takes precedence over Organization group or user group storage quota configurations.
3. Select **Delete** to enter a PIN and delete a user's content. A PIN configuration is in place to protect the user content from administrators who might unintentionally delete it.

File Encryption Migration

Collect the unencrypted content and migrate it to an encrypted state on a scheduled basis using the File Encryption Migration scheduler. Use the default schedule values that are populated.

However, administrators with the correct roles, can access and change these settings. To set a custom migration schedule:

1. Navigate to **Groups & Settings > All Settings > Admin > Scheduler** in a *Tenant* Organization Group.
2. Review the default schedule. If necessary, you can also configure a custom schedule.

Chapter 6:
VMware Content Locker

Overview

The Content Management solution provides you the VMware Content Locker app to enable the end users to access the managed content. The VMware Content Locker app is deployed to end-user devices and the managed content is accessed in the app within the configured parameters.

Features

- Content settings to set unique app behaviors.
- Use default SDK settings when configured as part of the AirWatch app suite.
- Content Management Dashboard and list views to manage the content deployment from the UEM console.

Security

- SSL encryption for secure data transit.
- AES 256-bit encryption to protect the deployed content.
- VMware Content Locker v2.2 and later for iOS uses the NSFileProtectionComplete class to store the content.

Configure VMware Content Locker

Provide end users with device side access to the corporate content using the VMware Content Locker app. The configurations set in the UEM console determine the level of freedom provided to end users accessing corporate content from their devices.

1. Navigate to **Groups & Settings > All Settings > Content > Applications > Content Locker**.

2. Configure the **Settings and Policies** settings.

Setting	Description
Application Profile	Set to define the security policies and settings used by this application. Leave as **Default** and configure the Recommended Default SDK settings to define app behavior using Workspace ONE UEM recommendations. Alternatively, select **Custom** application settings to override the default SDK settings and configure a unique set off behaviors for the app.
iOS Profile	Select a custom-created SDK profile from the drop-down list.
Android Profile	Select a custom-created SDK profile from the drop-down list.
Use Legacy Settings and Policies	Only enable legacy settings if directed to do so by a Workspace ONE UEM representative. Legacy settings do not leverage Shared SDK profile settings and should only be implemented in certain edge cases.
Default Authentication Method	Select the authentication method for the applications.
Enable "Keep me signed in"	Enable to allow end users to remain signed in between uses.
Maximum Number of Failed Attempt	Set the number of passcode entry attempts allowed before all data in the VMware Content Locker will be wiped from a device.
Authentication Grace Period (min)	Enter the time (in minutes) after closing the VMware Content Locker before reopening the VMware Content Locker will require users to enter credentials again.
Prevent Compromised Devices	Enable to prevent compromised devices from accessing VMware Content Locker.
Enable Offline Login Compliance	Enable to allow offline login compliance.
Maximum Number of Offline Logins	Enter the number of offline logins allowed before you have to go online.

3. Configure the **General** settings.

Setting	Description
Numbers of Days to Keep Content New	Select the number of days recently added documents will be labeled as new in the VMware Content Locker.

Setting	Description
Block Enrollment via Content Locker, Boxer, and Browser	Enable to prevent enrollment through VMware Content Locker, VMware Boxer, and VMware Browser. If Content Locker uses the VMware AirWatch SDK for iOS in Objective-C, then MDM enrollment is required for the single-sign on SDK setting to function correctly.
Change Repository Name	Enable to change the repository name in the **Root Repository Name** field that appears.
Root Repository Name	Enter the new repository name you want to use.
Allow Hyperlinks	Enable to allow end users to open hyperlinks located in documents in the **Open Internet Links with** field that appears.
Open Internet Links with	Select the application in which to open hyperlinks.
Local Storage	Enable to provide a storage alternative for user content. Local storage saves on the device and doesn't sync with other Personal Content in the cloud. Disable local storage to force all user content to save in a location that syncs with other Personal Content in the cloud.
Upload on Wi-Fi Only	Enable to restrict uploads from VMware Content Locker to Wi-Fi connections only.

4. Implement the **Terms of Use** agreement for your app.

5. Assign **Notifications** to Content Locker applications for the specified platform:

Setting	Description
Application Type	Indicate as **System** or **Internal**.
Application Name	Assign to the application.
Bundle ID	Assign to the application.
Badge Count	Set to **Required**, **Updates Only** or **None**. **Required**: Badge Count represents the number of required documents that the User has not opened through the Content Locker. (Windows Only) The Badge Count tracks the 'read' status for required documents per user across multiple devices. When a user with multiple devices reads a required document, then all other devices reflect the document as read. **Updates Only** (For Downloaded Content): Badge Count represents the number of downloaded documents that have updates or new versions available. **None**: Badge Counts are disabled for Content Locker.

6. Set the **Client Download** for **VMware Content Locker for Windows PC** to **Enabled** to allow your end users to download the Content Locker for their desktop from the **Self-Service Portal**.

   Leave **Disabled** if your organization uses an enterprise deployment of VMware Content Locker for Windows PC.

7. Select **Save**.

Configure Document Extensions

Document extensions enable end users to interact with the Content Locker files from within third-party applications. This functionality requires specific configurations within the UEM console and special consideration for certain types of corporate file servers.

Ensure that document extension functionality appears on devices with VMware Content Locker v3.1 and later by completing the required configurations in the UEM console.

Disable Application Whitelisting

1. Navigate to **Apps > Settings and Policies > Security Policies**.
2. Set **Limit Documents to Open Only in Approved Apps** to **No**.
3. Select **Save**.

Enable Open Into

Open Into option must be enabled for the end users to use the export functionality within Microsoft Office 365 apps.

1. Navigate to **Content > Repositories > Admin Repositories**.
2. Select the **Edit** icon next to the Corporate File Server that syncs to end-user devices.
3. On the **Security** tab, select **Allow Open In Third Party Apps** and then **Save**.

(Android Only) Enable Storage Access from Third-Party Apps

If you are using Android SDK Default settings:

1. Navigate to **Apps > Settings and Policies > Settings > Custom Settings**.
2. Select **Enable Custom Settings** and paste {"PolicyEnableFileProvider": "true"}.
3. Select **Save**.

If you are using a custom SDK profile for Content Locker:

1. If you have an existing custom profile, navigate to **Apps > Settings > Profiles > Custom Profile > Custom Settings Payload**.
2. If you want to add a custom profile, navigate to **Apps > Settings > Profiles > Add Profile > SDK Profile > Android > Custom Settings > Custom Settings Payload**.
3. Paste {"PolicyEnableFileProvider": "true"} and select **Save**. If you have multiple custom settings, append the PolicyEnableFileProvider key after your existing custom key within { }. For example, { "CustomSetting Default": "true”, "PolicyEnableFileProvider": "true" }

(Android Only) Limitation of Storage Access from Third-Party Apps

- Allow Open in third-party apps flag is considered to allow or deny access to third-party apps. 'Allow Email' permission flag is not considered for a file since it cannot be determined (based on application ID) whether the third-party app is an email app or not.

- Support for Android framework to provide the Content file and storage access from third-party apps is disabled by default to manage app containers and the data shared between them.
- Local Storage files are not accessible since Open In functionality for third-party apps is disabled by default.
- When Content Locker authentication is enabled, you must have Content Locker unlocked to access it through a third-party app (displays message).
- If your admin has configured an app whitelist and the third-party app is not whitelisted, then you cannot open or create files through Content Locker.
- For the Managed content, all the content is available while browsing through a third-party app. For other repositories, content is available (for one level) only for those folders that are synced in Content Locker.

VMware Content Locker Capabilities by Platform

The following matrix applies to the platform version of VMware Content Locker available in the app store as of August 2018.

Features	iOS	Android	Win 10	Win 8	Win PC
Security					
Authentication					
Basic	✓	✓	✓	✓	✓
AD/LDAP	✓	✓	✓	✓	✓
Token	✓	✓	✓	✓	✓
Second Factor Passcode	✓	✓	✓	✓	
Encryption					
SSL Encryption in Transit	✓	✓	✓	✓	✓
AES 256-Bit Encryption at Rest	✓	✓	✓	✓	✓
In Memory Encryption	✓	✓			
FIPS 140-2	✓	✓	✓	✓	
Certificate Pinning	✓				
IT Policies					
Compromised Detection	✓	✓	✓	✓	
Automatic offline revocation when device is compromised	✓	✓			
Require Enrollment	✓	✓	✓	✓	✓
Automatic offline revocation when document expires	✓	✓	✓	✓	✓
Maximum number of offline logins	✓	✓	✓	✓	✓
Wipe content at Maximum number of failed login attempts	✓	✓	✓	✓	✓

Features	iOS	Android	Win 10	Win 8	Win PC
Prevent deleting mandatory content	✓	✓	✓	✓	
DLP					
Prevent Copy/Paste	✓	✓	✓	✓	
Enable/Disable Print	✓				
Enable/Disable Open in Third Party Application(s)	✓	✓	✓	✓	✓
Enable/Disable Sharing via Email	✓	✓			
Enable/Disable Document Level Encryption	✓	✓	✓	✓	✓
Enable/Disable Document Watermarking	✓ *	✓ *			
*The watermark feature is available for only admin repositories, user repositories, and Workspace ONE UEM managed content. It is not available for Personal Content and email attachments opened in Content Locker					
Enable/Disable Screen Capture		✓ **			
** For Content Locker, Enable Screen Capture must be set to *Yes* to allow users to take screenshot of the documents and media content. It also enables the Screen Mirroring feature using third party apps like Vysor. If Enable Screen Capture is set to *No*, users can only take screenshot of the Content Locker home screen and folders. Screen Mirroring is also disabled.					
Data Collection					
Install Content	✓	✓	✓	✓	✓
Open/Close Content	✓	✓	✓	✓	✓
Uninstall/Delete Content	✓	✓	✓	✓	✓
Session Status	✓	✓	✓	✓	✓
Mobile Experience					
Access					
Keep Me Signed In	✓	✓	✓	✓	
Authenticate with back-end credentials (Active Directory)	✓	✓	✓	✓	✓
Integrate with Workspace ONE UEM Single-Sign-On	✓	✓		✓	✓
Workspace ONE UEM Single-Sign-On with Agent as Broker App	✓	✓		✓	
Allow Offline Access	✓	✓	✓	✓	✓
Standalone MCM	✓	✓	✓	✓	✓
Customize Terms of Use	✓	✓	✓	✓	✓
Content Views					
Featured Content (Folder, File, Category)	✓	✓	✓	✓	✓
All Content (All/Installed/Uninstalled)	✓	✓	✓	✓	✓
Recent Activity (Recently Updated and Viewed)	✓	✓	✓	✓	✓

Features	iOS	Android	Win 10	Win 8	Win PC
New Content	✓	✓	✓	✓	✓
Favorite Content	✓	✓	✓	✓	✓
Tile and List Views of content	✓		✓	✓	
Full-screen mode for images/PDFs	✓	✓	✓	✓	
View Required Content	✓		✓	✓	
Swipe through all images in a folder/view	✓				
Grid view of all images	✓				
File Management					
Sort Content (alphabetically, chronologically, importance)	✓	✓	✓	✓	✓
Filter Content (File Type, download status)	✓	✓	✓	✓	✓
Delete On-Demand documents	✓	✓	✓	✓	✓
Import and Upload new documents/new versions	✓	✓	✓	✓	
2-way sync for WebDav, network shares	✓	✓			
2- way sync for Google Drive, One Drive	✓	✓			
Check-In/Check-Out to SharePoint	✓	✓			
Add comments to files at SharePoint Check-in		✓			
User Generated Content- Capture Pictures or Video in VMware Content Locker	✓	✓			
Add, Copy, Multi-Select files or folders	✓	✓	✓		✓
User Generated Content – Add Audio Files	✓				
User Generated Content – Add Office Files	✓	✓			
User Generated Content – Add Text Files	✓	✓			
Queue Multiple Document Downloads Simultaneously	✓	✓	✓		✓
Manage Downloads (Pause/Resume/Cancel/Re-order)	✓		✓		✓
Manage Uploads (Pause/Resume/Cancel/Re-order)	✓				
Usability					
Search Strings within Documents (PDF Only)	✓	✓	✓	✓	
Thumbnail navigation/scrub bar	✓		✓	✓	
View Table of Contents	✓	✓	✓	✓	
Multi-Tab Document Viewing(File type restrictions apply)	✓		✓		
Bookmarking (PDF Only)	✓	✓	✓	✓	
Edit Bookmarks	✓		✓	✓	

Features	iOS	Android	Win 10	Win 8	Win PC
Night-Mode (PDF)	✓		✓	✓	
Presentation Mode (native pointer for presenting content)	✓				
Support for Links in PDFs	✓	✓	✓	✓	✓
View Updates	✓	✓	✓	✓	✓
Search Documents Based on Keywords	✓	✓	✓	✓	
Highlight search results	✓	✓	✓	✓	
View Last Successful Sync (Sync Status)	✓	✓	✓	✓	✓
User Managed Content (Personal/Local Storage)					
Personal Content Policies					
Enable/Disable access to Personal Content	✓	✓	✓	✓	✓
Storage quota control by user and group	✓	✓	✓	✓	✓
Store Personal Content in Remote File Storage (RFS)	✓	✓	✓	✓	✓
Enable/Disable Link Sharing	✓	✓	✓	✓	
Enforce link sharing polices for max days, max downloads, password	✓	✓	✓	✓	
Enable/Disable Folder Sharing	✓	✓	✓	✓	
File Management					
Add/Remove Files(s)	✓	✓	✓	✓	
Add new version	✓	✓	✓	✓	
Move File(s)/Folder(s)	✓	✓	✓	✓	
Add/Remove Folder(s)	✓	✓	✓	✓	
Removed files goes to Trash	✓	✓	✓	✓	
Open external files into Personal Content	✓	✓	✓	✓	
Automatically Upload document upon opening in VMware Content Locker	✓	✓			
Collaboration					
Add and Save PDF Annotations	✓	✓	✓	✓	
Edit and Save Office Documents (Word, Excel, PPT)	✓	✓			
Generate and share links to Personal Content from the device	✓	✓	✓	✓	
Share Personal Content Folders and Add Collaborators from device	✓	✓	✓	✓	

Features	iOS	Android	Win 10	Win 8	Win PC
View shared folders with Files (Co-Owner, Editor, Reader)	✓	✓	✓	✓	✓
Display Collaborators & Roles by each Shared Folder	✓	✓	✓	✓	
Add Comments to File Versions	✓				
View Activity Feed of Comments & Revision History per Document	✓				
Save Drafts locally	✓				
Notify User when update is available for document	✓	✓	✓	✓	
Customization and Integration					
External File Repository Integration					
Share Point 2007	✓	✓	✓	✓	✓
Share Point 2010	✓	✓	✓	✓	✓
Share Point 2013	✓	✓	✓	✓	✓
Share Point Online (Office 365)	✓	✓	✓	✓	✓
Network File Share	✓	✓	✓	✓	✓
WebDAV	✓	✓		✓	✓
FileServer (HTTP)	✓	✓		✓	
Google Drive	✓	✓	✓	✓	✓
OneDrive	✓	✓	✓	✓	✓
CMIS	✓	✓		✓	✓
User Added Repository Support	✓	✓	✓	✓	✓
One Drive for Business	✓	✓			
Box	✓	✓	✓		
Localization					
Arabic	✓	✓	✓	✓	✓
Chinese - Simplified	✓	✓	✓	✓	✓
Chinese - Traditional	✓	✓	✓	✓	✓
Czech	✓	✓	✓	✓	✓
Danish	✓	✓	✓	✓	✓
Dutch	✓	✓	✓	✓	✓
English	✓	✓	✓	✓	✓
French	✓	✓	✓	✓	✓
Hebrew	✓	✓	✓		✓

Features	iOS	Android	Win 10	Win 8	Win PC
German	✓	✓	✓	✓	✓
Italian	✓	✓	✓	✓	✓
Japanese	✓	✓	✓	✓	✓
Korean	✓	✓	✓	✓	✓
Polish	✓	✓	✓	✓	✓
Portugese - Brazil	✓	✓	✓	✓	✓
Russian	✓	✓	✓	✓	✓
Spanish	✓	✓	✓	✓	✓
Swedish	✓	✓	✓	✓	✓
Turkish	✓	✓	✓	✓	✓
Email Attachment and Integration					
Allow Viewing of Attachments and saving to VMware Content Locker	✓	✓	✓	✓	
Allow Viewing, Extracting and Saving of zipped attachments to VMware Content Locker	✓	✓	✓		
Allow Editing of Email Attachments	✓	✓			
Allow Reshare of Email Attachments	✓	✓			
Multi-Select Content and Send as Email Attachments (Individual Attachments)	✓				
Select Folders and Send as Email Attachments (Zipped Folder)	✓				
VMware Browser Integration					
Allow Viewing and Saving of VMware Browser Downloads	✓	✓			
*File type supported for editing.					

Matrix of Supported File Type by Platform

The following matrix applies to the version of VMware Content Locker available in the app store as of August 2018.

Supported File Types	iOS	Android	Windows 10
AD/Azure RMS	✓	✓ Content Locker v3.5+	
AAC (audio/aac)	✓	✓	

Supported File Types	iOS	Android	Windows 10
ALAC (audio/m4a)	✓	✓	
WAV (audio/wav)	✓	✓	
MP3 (audio/mpeg)	✓	✓	
MOV (video/quicktime)	✓	✓	
MP4 (video/mp4)	✓	✓	
M4B, M4R,	✓		
M4V	✓	✓	
CSV (.csv)	✓ View only	✓ View only	✓ View only
ePub (.epub)	✓		
iBooks			
iWorks - Keynote (.key) application/vnd.apple.keynote	✓ View Only		
iWorks - Numbers (.numbers) application/vnd.apple.numbers	✓ View Only		
iWorks - Pages (.pages) application/vnd.apple.pages	✓ View Only		
MS Office - Excel (.xls/.xlsx) application/vnd.ms-excel	✓ Edit Only	✓ Edit Only	✓
XLSM	✓	✓	
MS Office - PowerPoint (.ppt/.pptx) application/vnd.ms-powerpoint	✓ Edit Only	✓ Edit Only	✓
PPTM	✓		
MS Office - Word (.doc/.docx) application/msword	✓ Edit Only	✓ Edit Only	✓
DOCM	✓		
MS Office - Password Protected (.docx, .pptx, .xlsx MS Office 2007 or later)	✓ Edit Only	✓	
Editing is not supported for .doc files			
HTML (.html) text/html	✓	✓	✓
PDF (.pdf) application/pdf	✓ Edit Only	✓ Edit Only	✓
Rich Text Format (.rtf) application/rtf	✓	✓	

Supported File Types	iOS	Android	Windows 10
Rich Text Format Directory (.rtfd) application/octet-stream	✓		
XML (.xml) application/xml	✓	✓	✓
PNG (.png) image/png	✓	✓	✓
JPG (.jpg) image/jpeg	✓	✓	✓
TIF (.tif, .tiff) image/tif	✓	✓	✓
Bitmap (.bmp) image/bmp	✓	✓	✓
GIF (.gif) image/gif	✓	✓	✓
Zip (.zip) application/zip	✓	✓	✓
Password Protected Zip	✓	✓	✓
RAR (.rar) application/rar	✓		
Password Protected RAR			
GZIP (.gzip) application/zip		✓	
BZIP (.bzip) application/zip			
BZIP2 (.bzip2) application/zip		✓	
TAR (.tar) application/zip		✓	
TXT	✓	✓	✓
MSG	✓		

*File type supported for editing

**View only, presentation mode not available

Chapter 7:
App Suite SDK Configurations

Default vs Custom SDK Profiles

When you configure your application, you select a custom or a default application profile. This action applies an SDK profile to the application, giving deployed Workspace ONE UEM applications additional features.

To ensure your application configuration runs smoothly , it is helpful to:

- Know the difference between a Custom and Default SDK profile.
- Determine if a Custom or a Default SDK profile is more appropriate for your application.
- Ensure you have configured the SDK profile type that you want to apply.

Use the following chart to determine if you want to apply a **Default** or **Custom** SDK profile to your application, and to direct you to the configuration instructions for the profile you use.

You can define SDK profiles using two different profile types: **Default** or a **Custom** SDK application profile.

	Default	Custom
Implementation	Share SDK profile settings across *all* applications set up at a particular organization group (OG) or below.	Apply SDK profile settings to a *specific* application, and override the Default Settings SDK profiles.
Advantage	Provides a single point of configuration for all of your apps in a particular OG and its child groups.	Offers granular control for specific applications and overrides the Default Settings SDK profiles.
Configure	**Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies**	**Groups & Settings > All Settings > Apps > Settings and Policies > Profiles**
Read More	Continue reading this section to learn which default SDK profiles apply to deployed apps.	Learn more about custom SDK profile settings in the **VMware Workspace ONE UEM Mobile Application Management Guide**.

Custom SDK Profile Settings

Workspace ONE UEM recommends using default settings for ease of maintenance and a consistent end user experience between Workspace ONE UEM and wrapped apps. However, Custom SDK setting are available to address cases where a single app needs to exhibit unique behaviors that differ from the rest of the app suite.

Enable **Custom Applications Settings** to override default SDK settings, and configure unique behaviors that only apply to a single app.

Setting	Description
Authentication Method	Defaults to Single Sign-On. Ensure you require MDM enrollment so that Single Sign-On can function properly.
iOS Profile	Select a custom-created SDK profile from the drop-down list the settings profile for iOS devices.
Android Profile	Select a custom-created SDK profile from the drop-down list the settings profile for Android devices.
Use Legacy Settings and Policies	Only enable legacy settings if directed to do so by a Workspace ONE UEM representative. Legacy settings do not leverage Shared SDK profile settings and should only be implemented in certain edge cases.
Default Authentication Method	Select the authentication method for the applications.
Enable "Keep me signed in"	Enable to allow end users to remain signed in between uses.
Maximum Number of Failed Attempt	Set the number of passcode entry attempts allowed before all data in the VMware Content Locker is wiped from a device and the device is enterprise wiped.
Authentication Grace Period (min)	Enter the time (in minutes) after closing the VMware Content Locker before reopening the VMware Content Locker will require users to enter credentials again.
Prevent Compromised Devices	Enable to prevent compromised devices from accessing VMware Content Locker.
Enable Offline Login Compliance	Enable to allow offline login compliance.
Maximum Number of Offline Logins	Enter the number of offline logins allowed before you have to go online.

Configure Default SDK Security Settings

Default SDK settings apply across AirWatch and wrapped applications, providing a unified user experience on devices. Because the configured SDK settings apply to all AirWatch and wrapped applications by default, you can configure the default SDK profile with the entire AirWatch and wrapped application suite in mind.

Before You Begin

Not all platforms or AirWatch applications support all available default SDK profile settings. A configured setting only works on the device when it is supported by the platform and app. This also means that an enabled setting might not work uniformly across a multi-platform deployment, or between applications. The SDK Settings matrix covers the available SDK profile settings and the apps and platforms they apply to.

Key Assumptions

The recommendations provided apply to an app suite that includes:

- VMware Browser
- AirWatch Inbox
- VMware Content Locker
- Enrolled devices
- AirWatch or wrapped apps
- SDK settings available as of August 2018.

1. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies**.
2. Configure **Security Policies**.

Action	Description	Rec
Authentication Type		
Passcode	Prompt end users to authenticate with a user-generate passcode when the app first launches, and after an app session timeout. Enabling or disabling SSO determines the number of app sessions that get established.	–
Username and Password	Prompt end user to authenticate by re-entering their enrollment credentials when the app first launches, and after an app session timeout. Enabling or disabling SSO determines the number of app sessions that get established.	–
Disabled	Allow end user to open apps without entering credentials.	√
SSO		
Enabled	Establish a single app session across all AirWatch and AirWatch wrapped apps.	√
Disabled	Establish app sessions on a per app basis.	–
Offline Access		
Enabled	Allow end users to open and use AirWatch and wrapped apps when disconnected from Wi-Fi. Offline AirWatch apps cannot perform downloads, and end users must return online for a successful download. Configure the Maximum Period Allowed Offline to set limits on offline access.	√
Disabled	Remove access to AirWatch and wrapped apps on offline devices.	–
Compromised Protection		
Enabled	Override MDM protection. App level Compromised Protection blocks compromised devices from enrolling, and enterprise wipes enrolled devices that report a compromised status.	√

Disabled	Rely solely on the MDM compliance engine for compromised device protection.	–
Data Loss Prevention		
Enabled	Access and configure settings intended to reduce data leaks.	√
Enable Copy And Paste		
Allows an application to copy and paste on devices when set to **Yes**.		
Enable Printing		
Allows an application to print from devices when set to **Yes**.		
Enable Camera		
Allows applications to access the device camera when set to **Yes**.		
Enable Composing Email		
Allows an application to use the native email client to send emails when set to **Yes**.		

Enable Data Backup	
Allows wrapped applications to sync data with a storage service like iCloud when set to **Yes**.	
Enable Location Services	
Allows wrapped applications to receive the latitude and longitude of the device when set to **Yes**.	
Enable Bluetooth	
Allows applications to access Bluetooth functionality on devices when set to **Yes**.	
Enable Screenshot	
Allows applications to access screenshot functionality on devices when set to **Yes**.	

Enable Watermark	
Displays text in a watermark in documents in the VMware Content Locker when set to Yes. Enter the text to display in the Overlay Text field or use lookup values. You cannot change the design of a watermark from the AirWatch Console	

Limit Documents to Open Only in Approved Apps		
Enter options to control the applications used to open resources on devices. (iOS only) You can use VMware AirWatch Configuration values to restrict users from importing files from third-party applications into Content Locker. For more information, see **Configure Import Restriction in Content Locker** section.		
Allowed Applications List		
Enter the applications that you allow to open documents.		
Disabled	Allow end user access to all device functions.	–

3. **Save**.

4. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Settings**.

5. Configure **Settings**.

Branding		
Enabled	Apply specific organizational logo and colors, where applicable settings apply, to the app suite.	–
Disabled	Maintain the AirWatch brand throughout the app suite.	√
Logging		
Enabled	Access and configure settings related to collecting logs.	√
Logging Level Choose from a spectrum of recording frequency options: • **Error** – Records only errors. An error displays failures in processes such as a failure to look up UIDs or an unsupported URL. • **Warning** – Records errors and warnings. A warning displays a possible issue with processes such as bad response codes and invalid token authentications. • **Information** – Records a significant amount of data for informational purposes. An information logging level displays general processes as well as warning and error messages. • **Debug** – Records all data to help with troubleshooting. This option is not available for all functions.		
Send logs over Wi-Fi only Select to prevent the transfer of data while roaming and to limit data charges.		
Disabled	Do not collect any logs.	–
Analytics		
Enabled	Collect and view useful statistics about apps in the SDK suite.	√
Disabled	Do not collect useful statistics.	–
Custom Settings		
Enabled	Apply custom XML code to the app suite.	–
Disabled	Do not apply custom XML code to the app suite.	√

6. **Save**.

(iOS Only) Configure Import Restriction in Content Locker

You can use the configuration keys in UEM console to restrict import of content from third-party applications into the Content Locker. The configuration keys can be used to allow content import from only whitelisted set of native applications.

Use the following configuration keys to restrict or allow content import from third-party applications into Content Locker.

Configuration Key	Value Type	Supported Values	Description
{"ContentImportRestriction"}	Boolean	true = restriction enabled false = restirction disabled For example, {"ContentImportRestriction": true}.	When enabled, device users cannot import content from any non-whitelisted third-party applications including the native iOS applications into the Content Locker.
{"ContentImportAllowNativeApps"}	Boolean	true = import from native applications are allowed false = import from native applications are not allowed For example, {"ContentImportAllowNativeApps": true}	When enabled, the device users can import content from native applications when the import restriction is enabled.

The ContentImportRestriction and ContentImportAllowNativeApps configuration values can be used in combination to configure the import restriction as per your requirement. If you want to allow import of content from all native apps, enable the ContentImportAllowNativeApps key. The ContentImportAllowNativeApps key is enabled by default and allows import from all native apps such as iOS native Email, Files, Safari, AirDrop, and such. When enabled, the device users can open and import content from non-whitelisted apps into Content Locker using the web versions of the non-whitelisted applications (using Safari).

If you want to allow only specific applications, disable the ContentImportAllowNativeApps key and add the allowed applications in the whitelist.

If you want to restrict importing of content from specific native apps, disable the ContentImportAllowNativeApps key and add the allowed native applications in the whitelist.

Note: The Limit Documents to Open Only in Approved Apps option must be enabled in the Data Loss Prevention settings before enabling the configuration key values. Safari and AirDrop cannot be whitelisted as there is no associated bundle ID.

If you are using SDK Default settings:

1. Navigate to **Group & Settings** > **All Settings**.
2. From All Settings, navigate to **Apps** > **Settings&Policies** > **Settings**.
3. Select **Enable Custom Settings** and paste the configuration keys as per your requirement. For example, to allow import only from native apps, { "ContentImportRestriction": true, "ContentImportAllowNativeApps": true}.
4. To allow importing from a specific list of apps (whitelist):
   a. Navigate to **Settings and Policies** > **Security Policies**.
   b. Select the **Allowed Applications List** text box and list the applications you want to allow the users to import content into the Content Locker.
5. Select **Save**.

If you are using a custom SDK profile for Content Locker:

1. Navigate to **Group & Settings** > **All Settings**.
2. If you have an existing custom profile, navigate to **Apps** > **Settings & Policies** > **Profiles** > **Custom Profile** > **Custom Settings**.
3. If you want to add a custom profile, navigate to **Apps** > **Settings & Policies**> **Profiles** > **Add Profile** > **SDK Profile** > **iOS**> **Custom Settings**.
4. From Custom Settings, select **Configure** and paste the configuration keys as per your requirement. For example to allow import only from native apps, { "ContentImportRestriction": true, "ContentImportAllowNativeApps": true}.
5. From the Restriction section, select **Restrict documents to be opened in following apps** and add the list of apps that you want to allow as per your requirement (whitelist).
6. Select **Save**.

(iOS Only) Configure PDF Autosave in Content Locker

From Content Locker v4.13.2, the device users can enable or disable the PDF Autosave functionality by using the Enable PDF Autosave setting in the Content Locker app. The PDF Autosave setting is disabled by default. The PDF Autosave function can be set to 30 seconds, 60 seconds, and 120 seconds respectively using the Autosave time in seconds setting in the Content Locker. The administrators can use the configuration key provided by VMware AirWatch in the AirWatch Console to force enable the PDF Autosave functionality in Content Locker. When enabled using the configuration key, the device users cannot disable the PDF Autosave function and the Enable PDF Autosave setting is unavailable in the Content Locker. When the PDF Autosave function is enabled, the changes made to a PDF file when an autosave is in progress are not saved. After every instance of an autosave, the PDF document is reloaded.

Use the following configuration key to enable PDF Autosave function is Content Locker:

Configuration Key	Value Type	Supported Values	Description
{ "ContentPDFAutoSaveEnabled" }	Boolean	true = enabled false = can be enabled or disabled by the device user	When set to True, the PDF Autosave functionality is enabled and the device users cannot disable the setting. The Enable PDF Autosave setting in the Content Locker is unavailable to the device users.

If you are using SDK Default settings:

1. Navigate to **Group & Settings** > **All Settings**.
2. From All Settings, navigate to **Apps** > **Settings & Policies** > **Settings**.
3. Select **Enable Custom Settings** and paste the configuration keys as per your requirement.
   For example, to enable PDF Autosave, { "ContentPDFAutoSaveEnabled": true }.
4. Select **Save**.

If you are using a custom SDK profile for Content Locker:

1. Navigate to **Group & Settings** > **All Settings**.
2. If you have an existing custom profile, navigate to **Apps** > **Settings & Policies** > **Profiles** > **Custom Profile** > **Custom Settings**.
3. If you want to add a custom profile, navigate to **Apps** > **Settings & Policies**> **Profiles** > **Add Profile** > **SDK Profile** > **iOS**> **Custom Settings**.
4. From Custom Settings, select **Configure** and paste the configuration keys as per your requirement.
   For example, to enable PDF Autosave, { "ContentPDFAutoSaveEnabled": true }.
5. Select **Save**.

(iOS and Android Only) Configure Privacy Settings for Content Locker

Use the configuration keys in the UEM console to perform additional privacy disclosure and data collection practices. End users who are upgrading or are starting to use the latest version of Content Locker are presented with new privacy dialog screen upon the application launch. For more information about the privacy notice and data sharing settings, see https://support.workspaceone.com/articles/360005402834.

The privacy dialog screen lets the user know the following information:

- **Data collected by the app** – Provides a summary of data that is collected and processed by the application. Some of this data is visible to administrators of the Workspace ONE UEM administration console.
- **Device Permissions** – Provides a summary of device permissions requested for the app to enable product features and functionality, such as push notifications to the device.
- **Company's privacy policy** – By default, a message is displayed to the user to contact their employer for more information. You can configure the privacy policy URL in the UEM console. Once configured, the user can access the employer's privacy policy from the app.

Use the following configuration keys to enable privacy notice and data sharing settings in Content Locker:

Configuration Key	Value Type	Supported Values	Description
{ "DisplayPrivacyDialog" }	Integer	0 = disabled 1 = enabled (default)	When set to '1' (enabled), Content locker displays a privacy notice to the users about the data that is collected and the permissions that are required on the device for the optimal functioning of the app.
{ "PolicyAllowFeatureAnalytics" }	Integer	0 = disabled 1 = enabled (default)	When set to '1' (enabled), Content locker displays a notice to the users about the option to opt-in to anonymous feature usage analytics that help VMware improve product functionality and invent new product capabilities. When set to '0', the data sharing notice is not displayed and no data is collected from the device to optimize the app experience.
{ "PolicyAllowCrashReporting" }	Boolean	True = enabled False = disabled	When set to True, app crashes are reported back to VMware.
{ "PrivacyPolicyLink" }	String	"https://www.url.com"	Provide the Policy URL that you want your users to visit when Your company's privacy policy is selected from the Privacy notice.

If you are using SDK Default settings:

1. Navigate to **Group & Settings** > **All Settings**.
2. From All Settings, navigate to **Apps** > **Settings & Policies** > **Settings**.
3. Select **Enable Custom Settings** and paste the configuration keys as per your requirement.
   For example, to enable Crash reporting, { "PolicyAllowCrashReporting": true}.
4. Select **Save**.

If you are using a custom SDK profile for Content Locker:

1. Navigate to **Group & Settings** > **All Settings**.
2. If you have an existing custom profile, navigate to **Apps** > **Settings & Policies** > **Profiles** > **Custom Profile** > **Custom Settings**.
3. If you want to add a custom profile, navigate to **Apps** > **Settings & Policies**> **Profiles** > **Add Profile** > **SDK Profile** > **iOS**> **Custom Settings**.
4. From Custom Settings, select **Configure** and paste the following configuration keys as per your requirement.
5. Select **Save**.

Expected Behavior for SDK Authentication

Enabling or disabling SSO determines the number of app sessions established, impacting the number of authentication prompts end users receive.

Authentication Type	SSO	Sessions	Credentials	Expected Behavior
Disabled	Enabled	Single	Enrollment Credentials	Open apps without prompting end users to enter credentials.
Passcode	Enabled	Single	Passcode	Prompts at first launch of first app, establishing a single app session. The next authentication prompt occurs after the session times out.
Username and Password	Enabled	Single	Enrollment Credentials	Prompts at first launch of first app, establishing a single app session. The next authentication prompt occurs after the session times out.
Passcode	Disabled	Per App	Passcode	Prompts on a per app basis, establishing individual app sessions. Note that each app may have a unique passcode. The next authentication prompt occurs when launching a new app, or an individual app session times out.
Username and Password	Disabled	Per App	Enrollment Credentials	Prompts on a per app basis, establishing individual app sessions. The next authentication prompt occurs when launching a new app, or an individual app session times out.

Chapter 8:
VMware AirWatch Content Apps for Desktop

Content Apps for Desktop consist of a suite of apps that deploy to end users in the Self-Service Portal. These apps help the end users access the content they stored in the Personal Content Repository, and facilitate secure collaboration.

1. Workspace ONE UEM administrator enables and configures Personal Content in the Workspace ONE UEM console.
2. Workspace ONE UEM administrator sets the end-user availability of content desktop apps, and manages associated security configurations from the UEM console.

App	Description
VMware Content Locker for Desktop	Allows end users to access the important content on their devices while simultaneously safeguarding those files. Any content accessed through the VMware Content Locker opens inside the application, ensuring that it cannot be copied, saved, or shared without approval.
VMware Content Locker Sync	Syncs content added to a designated folder on an end user's PC or Mac computer with the Personal Content repository. In addition to the end user's personal computer, synced content becomes accessible to an end user from any browser through the Self-Service Portal, and on mobile devices using the VMware Content Locker application.

App	Description
VMware Content Locker Outlook Add-In	Enables end users to send shared links of a file in their Personal Content repository, rather than sending the file as an attachment. This option secures files by allowing only those users with access to the link ability to view the file, forcing file sharing to occur within the confines of the VMware Content Locker. The add-in also allows you to update the file while maintaining user access to the shared link. You can also revoke access to the link at any time.

3. End users download and use desktop apps, available in the Self-Service Portal, at their own discretion.

Enterprise Deployments of Desktop Apps

Administrators implementing an enterprise deployment of the content apps for desktop can configure the MSI installer and provide the functionality prepackaged on the desktop.

Enable VMware Content Locker Sync

Syncs content added to a designated folder on an end user's PC or Mac computer with the Personal Content repository. In addition to the end user's personal computer, synced content becomes accessible to an end user from any browser through the Self-Service Portal, and on mobile devices using the VMware Content Locker application.

To enable and configure the Sync Client and its basic features:

1. Navigate to **Groups & Settings > All Settings > Content > Applications > VMware Content Locker Sync**.
2. **Enable** or **Disable** features to set the sync client behavior.

Setting	General
VMware Content Locker Sync	**Enable** sync functionality associated with the product.
Client Download	**Enable** the end-user sync client downloads from the Self-Service Portal. **Disable** the end-user sync client downloads if implementing an enterprise deployment of Content Locker Sync using the MSI installer.
Require MDM Enrollment	**Enable** a requirement for end users to have managed devices to authenticate successfully into Content Locker Sync. This requirement does not apply to end users who authenticated before the configuration of this setting.

3. Select the s**Terms of Use agreement** for Windows.
4. If implementing Client Downloads, verify that the appropriate **Link Sharing** settings are enabled.

Configure Outlook Add-In

Enable and configure the Outlook Add-In in the UEM console so that end users can download it in the Self-Service Portal and use it to secure email attachments.

To configure the Outlook add-in:

1. Navigate to **Groups & Settings > All Settings > Content > Applications > Outlook Add-In**.
2. Configure the settings.

Setting	Description
Client Download	**Enable** to allow end users to download the Outlook Add-In client from the Self-Service Portal. **Disable** if your organization does an enterprise deployment of Outlook Add-In.
Automatically convert attachments to links	**Enable** to automatically convert large attachments into a link. Enter the amount that triggers the conversion of attachments to links into the field that appears.
Recommend converting attachments to links	**Enable** to recommend end users convert attachments into a link. Enter the amount that triggers the conversion of attachments to links into the field that appears.

Enable Digital Signatures in the Self-Service Portal

Integrate with a third-party eSignature Client so that end users can request a digital signature when they share files from the Self Service Portal.

To configure digital signatures:

1. Navigate to **Groups & Settings > All Settings > Content > Advanced > eSignature**.
2. Set **Enable eSignatures** to **Enabled** and configure the settings.

Setting	Description
eSignature Provider	Select your organization's eSignature provider from the drop-down menu. Unlisted providers are unavailable for integration.
URL	Provide your account URL in the field.
Integration Key	Provide the account integration key in the field.
Username	Provide your account username in the field.
Password	Provide your account password in the field.

3. Select **Test Connection**. If the test is successful, select **Save**.

Enable Personal Content Uploads in Socialcast

Integration with Socialcast allows the end user upload their Personal Content to Socialcast. Integration requires configurations in both the UEM console and the Socialcast Admin Console.

Generating an API token in the UEM Console

1. Navigate to **Groups & Settings > All Settings > System > Advanced > API > Rest API > Add**.
2. Complete the text boxes that appear.

Setting	Description
Service	Enter **Socialcast** as the service name.
Account Type	Select **Admin** from the drop-down menu.
API Key	Copy the key that automatically generates. Upload this key into Socialcast.

3. Select **Save** to generate your token.

Uploading the API token in the Socialcast Admin Console

1. Log into the Socialcast Admin Console.

   For more information on setting up a Socialcast Community, see http://developers.socialcast.com/admin/setting-up-a-socialcast-community/.

2. Navigate to the **Security** tab.

   For more information on Security configurations for Socialcast, see http://developers.socialcast.com/admin/customizing-the-community/security/#restrict-attachments.

3. Enable Content Locker attachments and complete the text boxes.

Setting	Description
AirWatch Domain	Provide the URL of your Workspace ONE UEM instance.
API Key	Paste the API key you copied from the UEM console into the text box.

Chapter 9:
Workspace ONE UEM Application Deployment

Control how Workspace ONE UEM applications deploy to your end users and other security configurations from the UEM console. Once deployed, end users can download and use these apps.

The **VMware Workspace ONE UEM Mobile Application Management (MAM) Guide** covers the process for deploying public applications in full detail. While the VMware Content Locker application is available in the public app store, your organization needs to purchase licenses per device to take advantage of the Workspace ONE UEM MCM solution. Please see http://www.air-watch.com/pricing or contact Workspace ONE Support for more information.

Deploy Workspace ONE UEM Applications

Configure Workspace ONE UEM Applications to deploy as public apps.

Utilize this simplified deployment workflow to seamlessly push Workspace ONE UEM applications to end users.

1. Navigate to **Apps & Books > Applications > Native > Public**.
2. Select **Add Application**.
3. Configure the fields on the screen that appears:

Setting	Description
Managed By	View the organization group the application uploads in.
Platform	Choose the appropriate platform.
Name	Enter a descriptive name in the field to help search for the application in an app store.
Search App Store	Select to search for the application in the app store. In order to search the Google Play Store in an on-premises deployment, you must integrate a Google Account with the Workspace ONE UEM MDM environment.

4. Review the information that automatically populates in the **Info** tab.
5. Add smart groups from the **Assignment** tab.
6. Use the **Deployment** tab to determine how your end users receive the app. End users find and download recommended apps in the app store. To make finding and deploying it easier, you can recommend it through Workspace ONE UEM or automatically push it to your devices.
7. Assign **Terms of Use**, if desired.
8. **Save and Publish**.

Overview for Onboarding VMware Content Locker

Onboarding requires end users to review and acknowledge training materials and videos before gaining full access to VMware Content Locker on their devices.

Single App Mode

Maximize Onboarding functionality, by configuring required content and pushing a single app mode profile to end-users devices. Once Onboarding completes, remove the profile to allow end users to access full device functionality.

Alternatively, configure Onboarding without single app mode to provide a more flexible experience for end users. In this set up end users cannot access the Content Locker until they view the required content, but they can still use their device.

	With Single App Mode	Without Single App Mode
VMware Content Locker	Locked in the Required Content View	Locked in the Required Content View
Other Device Apps	Inaccessible. The device remains locked in the Required Content View.	Accessible. End users can still use their devices.

User Experience

Before you enforce content viewing, consider how these choices affect the end-user experience. For example, pushing required content to a device out in the field might confuse end users, resulting in help desk tickets. In general, on-boarding, or in a similar guided scenario, provides an appropriate level of context for the limited device behavior, reducing the likelihood of end-user confusion.

Also, consider the impact of deploying Content Locker in single app mode, as it restricts device functionality to a single app, in this case, Content Locker. If planning to remove the single app mode restriction at a set time, ensure that the end users does not access other apps. Also, ensure that the end users perform work related tasks on their devices while their devices are restricted.

Enable Onboarding for VMware Content Locker

Onboarding provides a deployment option for Content Locker that locks the app into a view that only displays the required content until that content is viewed.

To enable onboarding:

1. Meet minimum OS and app requirements.
2. Determine and configure enrollment flow.
3. Navigate to **Content > Settings > Advanced > Onboarding**.
4. Set **Onboarding** to **Enabled** and configure the settings that appear.

Setting	Description
Administrative Unlock Code	Set this code to override the supervised mode as an admin.
Entrance Message	Provide a message to end users explaining that they must view the required content before they can use their device.
Exit Message	Provide a message to end users explaining they viewed all the require content and are now free to use their device.

5. Select **Save.**

Chapter 10:
Content Management using Workspace ONE Console

Overview

The Content Management solution provides you multiple options to manage the content that is stored, synced, or deployed from the Workspace ONE UEM console.

Features

The Content Management solution provides the following functionalities to manage the content:

- Content Management Dashboard for quick overview of the users and managed content.
- List View for viewing and managing the content.
- Content Settings menu to configure repository, storage, deployment, and management options for different types of content.

For more information about Content Management options and different settings available to manage content deployed from the UEM console, see Mobile Content Management Dashboard on page 66 and Settings for Content Management on page 69.

Menu Options for Content Management

In addition to the default view in the console, there are several other screens that simplify content management. They display in a secondary navigation menu to the left of the Content Dashboard in the UEM console.

Review the available menu options for Content Management.

Setting	Description
List View	Toggle between the AirWatch Managed and Corporate File Server list view.

Setting	Description
Repositories	Select repositories for accessing the repository configuration options. There are two types of repositories, admin added repositories and user added repositories. Users add repositories using the templates you configure in the console.
Categories	Add categories and subcategories. Added categories are displayed on the screen in a list view with an action menu.
Featured Content	Manage the featured content you added from the List View or the Categories List View on this screen. Featured content is displayed prominently within the VMware Content Locker, providing easy access to high volume content. Use this screen to control the order in which featured content is displayed in the VMware Content Locker using drag or deleting irrelevant content.
Batch Status	Perform a Batch Import and review the details of your uploaded batch from this screen.
Settings	Select to access content specific settings.

Mobile Content Management Dashboard

View and manage the general content status of your device fleet from the Content Management Dashboard, the default content view. Use this centralized page in the console to gain immediate insights about users, to analyze the content for making business decisions, and to act on warnings.

Following are the different views and parameters that are displayed on the dashboard.

Setting	Description
Storage History	Overview storage quotas using the six-bar graphical summary.
User/Content Status	Summarize device content compliance at a glance using the status icon graphics. Each graphic fills to represent the percentage of devices or files that are in trouble. Select these icons to view devices that are out of compliance and to take administrative action.
Content Engagement	Learn which documents are the most useful and in-demand for your end users and the documents that you might consider deprecating. Select the displayed information to navigate directly to a page where you can edit your content.
User Breakdown	Information about end-user activity Today, This Week, or This Month. The icons represent your end users and are filled in with the percent of end users who are active.

Content Management List View

Act on the uploaded AirWatch Managed and synced Corporate File Server content from the Workspace ONE UEM console Content List View. The Content List View populates with the information you entered while uploading your content or repositories, providing an overview of all content.

Access this list by navigating to **Content > List View**.

Setting	Description
AirWatch Managed	View and manage the content you directly added to the UEM console in this default list view.

Setting	Description
AirWatch Managed Menu	Act on AirWatch Managed Content using the available list view options. • **Add Content** – Select to add AirWatch Managed Content to the UEM console. • **Storage Used** – Review the status bar to see the percentage of allotted storage consumed by end users.
Corporate File Servers	View and manage synced repositories in this list view, or use the content list views for individual repositories.
Corporate File Servers Menu	To display configured repositories in the list view, select **Show Repositories**
Filter	Find desired documents using the available filters. • **Category** – Filter content using the categories assigned from the UEM console. • **Type** – Filter content based on the file type. • **Expiration Status** – Filter content to display only the content set to expire in 14 days.
Active/Inactive	Information about the content availability to end users. • Green circles display next to active content. • Red circles display next to inactive content. Inactive content is not searchable, viewable, or sent automatically to devices.
Name	Select to edit the general **Info**, **Details**, **Previous Version**, **Security**, **Assignment**, and **Deployment** information you configured when adding your content. You can also download or delete previous content versions.
Action Menu	Manage your content using the available menu options. The two Content List View action menus differ slightly.

Options for Content Management

Use these options to manage uploaded or synced content and metadata in List View and other menus on Workspace ONE UEM console.

Action						
	AirWatch Managed	Corporate File Servers	Automatic Template	Manual Template	User-Added Repository	Category
Edit						
Manage file settings on an individual basis. Edited settings only affect the individual file, not the entire repository's settings.	✓	✓	✓	✓	✓	

Action						
Download a local copy of a previous file version.	✓					
Delete a previous file version from the console.	✓					
Update an existing file with a new version, archiving the original file.	✓					
Delete						
Remove a file from the UEM Console.	✓					
Remove file metadata from the UEM Console.		✓	✓	✓	✓	
Initiate a manual sync between the network content and AirWatch.		✓	✓	✓	✓	
Remove an empty subcategory or empty category from the UEM Console.						✓
Add						
Update an existing file with a new version, archiving the original file.	✓					
Add a subcategory to a category.						✓
Sync						
Initiate a sync between Workspace ONE UEM and integrated Corporate File Servers.		✓	✓	✓	✓	
View Devices						
Open a device list, view the device an individual file is assigned to.	✓	✓	✓	✓	✓	
Push an individual file to a selected device.	✓	✓	✓	✓	✓	
Remove an individual file from a selected device.	✓	✓	✓	✓	✓	
Additional Options						
Add a file to Featured Content so that the file displays prominently within the VMware Content Locker.	✓	✓	✓	✓	✓	✓
Download a local copy of the file.	✓	✓	✓	✓	✓	
Remove a file from the UEM Console.	✓					
Remove file metadata from the UEM Console.		✓	✓	✓	✓	

Settings for Content Management

Content Management settings consist of various configurations related to content management.

To access the menu of available configurations, select **Settings**.

Setting	Description
Applications	Access the configuration screens for VMware Content Locker, VMware Content Locker Sync, and the Outlook Add-In.
Content Gateway	Configure Content Gateway and download the installer.
Personal Content	Enable and configure Personal Content settings for end users.
User Storage	Configure storage quota exceptions for individual users. These exceptions provide the most granular level of storage assignment, and override organization or user group configurations set in Personal Content.
Remote Storage	Configure Remote File Storage and download the installer
Content Viewer	Configure Content Rendering Engine and download the installer.
Advanced	Configure file type restrictions, on-boarding and requiring content for on-boarding, and integrating with a third-party e-Signature vendor.