

# VMware AirWatch Mobile Content Management Guide

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

Workspace ONE UEM v9.4

**Have documentation feedback?** Submit a Documentation Feedback support ticket using the Support Wizard on [support.air-watch.com](https://support.air-watch.com).

Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

# Table of Contents

---

<b>Chapter 1: Content Management Overview</b>	<b>4</b>
Introduction to Mobile Content Management	5
Requirements for Mobile Content Management	5
<b>Chapter 2: File Storage</b>	<b>9</b>
Overview of Storage Options by Content Type	10
Overview for Content Management Enterprise Integration Solution	10
Set Content Storage Capacity	11
Restrict File Extensions	12
<b>Chapter 3: Corporate File Servers</b>	<b>13</b>
Overview of Corporate File Servers	14
Enable End-User Access to Corporate File Server Content	14
Support for Corporate File Servers	15
Configure an Admin Repository	17
Enable Users to Sync Corporate File Servers	18
Configure Repository Details	19
<b>Chapter 4: AirWatch Managed Content</b>	<b>22</b>
Overview of Workspace ONE UEM Managed Content Repository	23
Configure the Workspace ONE UEM Managed Content Category Structure	23
Upload Content to the Workspace ONE UEM Managed Repository	24
Upload Workspace ONE UEM Managed Content in Batches	25
Local File Storage for Workspace ONE UEM Managed Content	25
<b>Chapter 5: Personal Content Repository</b>	<b>29</b>
Overview of Personal Content Repository	30
Enable Personal Content	31
Roles for Folder Sharing	32
Configure Personal Content Quota Exceptions	33
File Encryption Migration	33

<b>Chapter 6: VMware Content Locker</b>	<b>34</b>
Overview of VMware Content Locker	35
Configure VMware Content Locker	35
Configure Document Extensions	37
VMware Content Locker Capabilities by Platform	38
Matrix of Supported File Type by Platform	44
<b>Chapter 7: App Suite SDK Configurations</b>	<b>47</b>
Default vs Custom SDK Profiles	48
Custom SDK Profile Settings	48
Configure Default SDK Security Settings	49
Expected Behavior for SDK Authentication	53
<b>Chapter 8: VMware Content Locker Collaborate</b>	<b>54</b>
VMware AirWatch Content Apps for Desktop	55
Enable VMware Content Locker Sync	55
Configure Outlook Add-In	56
Enable Digital Signatures in the Self-Service Portal	57
Enable Personal Content Uploads in Socialcast	57
<b>Chapter 9: Application Deployment</b>	<b>59</b>
Overview of Workspace ONE UEM Application Deployment	60
Deploy Workspace ONE UEM Applications	60
Overview for Onboarding VMware Content Locker	60
Enable Onboarding for VMware Content Locker	61
<b>Chapter 10: Overview of Content Management</b>	<b>63</b>
Features	63
Menu Options for Content Management	63
Mobile Content Management Dashboard	64
Content Management List View	64
Options for Content Management	65
Settings for Content Management	66

# Chapter 1:

## Content Management Overview

Introduction to Mobile Content Management ..... 5

Requirements for Mobile Content Management ..... 5

## Introduction to Mobile Content Management

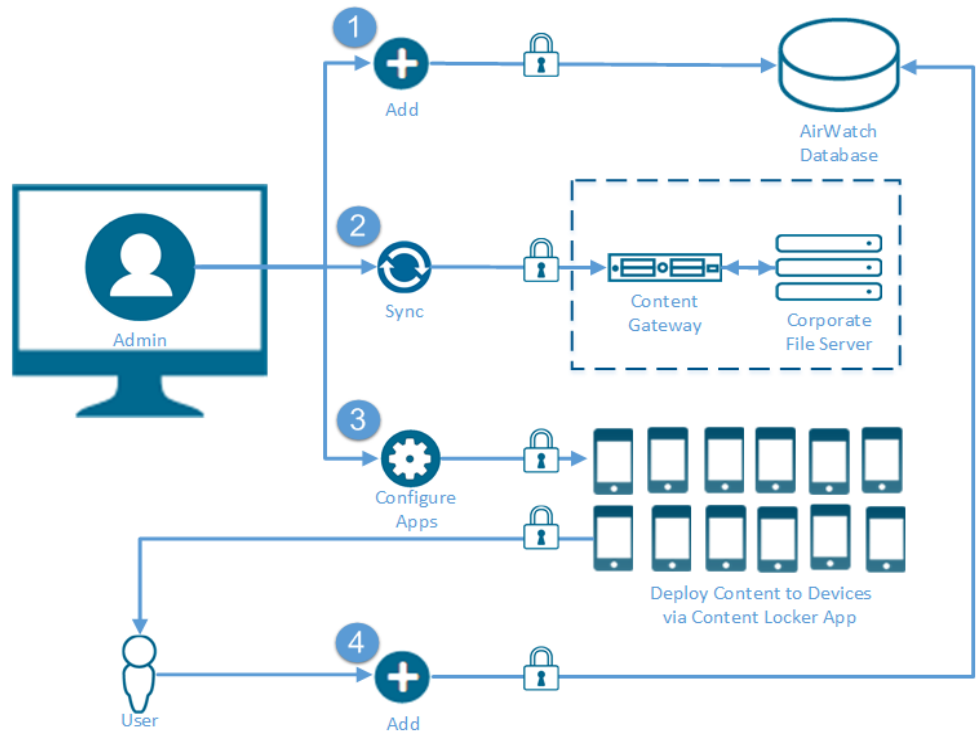
The Mobile Content Management™ (MCM) solution helps your organization address the challenge of securely deploying content to a wide variety of devices using a few key actions. Use the Workspace ONE UEM console to create, sync, or enable a file store known as a repository. Once configured this content 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	<p>The Workspace ONE Unified Endpoint Management (UEM) console supports the latest stable builds of the following web browsers.</p> <ul style="list-style-type: none"><li>• Chrome</li><li>• Firefox</li><li>• Safari</li><li>• Internet Explorer 11</li><li>• Microsoft Edge</li></ul> <div><p><b>Note:</b> If using IE to access the UEM console, navigate to <b>Control Panel &gt; Settings &gt; Internet Options &gt; Security</b> and ensure you have a security level or custom security level that includes the <b>Font Download</b> option being set to <b>Enabled</b>.</p></div> <p>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.</p>																																																	
App Requirements																																																		
	<table><tr><th></th><th>Content Locker</th><th>Content Locker Sync</th><th>Outlook Add-In</th></tr><tr><td rowspan="6">Platform Requirements</td><td>iOS 7.2+</td><td>√</td><td></td></tr><tr><td>Android 3.2+</td><td>√</td><td></td></tr><tr><td>Windows 7</td><td>√*</td><td>√</td><td>√</td></tr><tr><td>Windows 8</td><td>√</td><td>√</td><td>√</td></tr><tr><td>Windows 10</td><td>√</td><td>√</td><td>√</td></tr><tr><td>10.9 Mavericks+</td><td></td><td>√</td><td></td></tr><tr><td rowspan="3">Framework Requirements</td><td>.NET 4.0.3+</td><td>√*</td><td></td><td>√</td></tr><tr><td>.NET 4.5+</td><td></td><td>√</td><td></td></tr><tr><td>Mono</td><td></td><td>√</td><td></td></tr><tr><td rowspan="2">Visual Studio Requirements</td><td>Visual Studio 2010 v10.0.50903</td><td>√*</td><td></td><td>√</td></tr><tr><td>Visual C++ 2008</td><td></td><td>√</td><td></td></tr></table>		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		√	
	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	<b>Select a role that has <i>Content</i>, <i>Content Device Install</i>, and <i>Content Device Remove</i> enabled by default.</b>  Grants access the content management page and control of content distribution.  For more information on creating roles, read the <b>Roles and Added Resources Guide</b> , available on <a href="#">Accessing Other Documents</a> .			
End-User Roles	<b>Enable <i>Manage Content</i> and grant <i>Full Access</i></b>  For more information on creating roles, read the <b>Roles and Added Resources Guide</b> , available on <a href="#">Accessing Other Documents</a> .			
Repository Requirements				
AirWatch Managed Content	<b>Configure the category structure before uploading content</b>  You cannot add subcategories to categories that have content in them.			
Corporate File Server Content	<b>Install Content Gateway</b>  Install Content Gateway to establish a connection in instances where the Workspace ONE UEM server domain cannot access a Corporate File Server. See <a href="#">Support for Corporate File Servers on page 15</a> to review which Workspace ONE UEM supported repositories require, support, or do not support Content Gateway.  For comprehensive installation instructions, read the <b>Content Gateway Installation Guide</b> , available on <a href="#">Accessing Other Documents</a> .			
Personal Content	<b>Purchase Appropriate Bundle or Service</b>  Not all content management packages include personal content management.			
Alternative File Storage Requirements				
Local File Storage	<b>Determine Appropriate Solution for Organization</b>  For more information on available options, see <a href="#">Local File Storage for Workspace ONE UEM Managed Content on page 25</a> .			

Component	Requirement & Description
Remote File Storage	<b>Determine Appropriate Solution for Organization</b> For more information on available options, see <a href="#">Overview of Storage Options by Content Type on page 10</a> .
	<b>Personal Content</b> Current availability limited to content stored in the Personal Content repository. Not all content management packages include personal content management.
	<b>Install Remote File Storage Server</b> If using Remote File Storage as an alternative storage option for Personal Content, follow the installation instructions outlined in the <b>Remote File Storage Installation Guide</b> , available on <a href="#">Accessing Other Documents</a> .
<b>Optional Security Component Requirements</b>	
Content Rendering Engine	<b>Determine Appropriate Solution for Organization</b> Leverage this product to address security concerns for content shared from the Self-Service Portal.
	<b>Install Remote File Storage Server</b> The Content Rendering Engine requires a working instance of the Remote File Server. Installation instructions are outlined in the <b>Remote File Storage Installation Guide</b> , available on <a href="#">Accessing Other Documents</a> .
	<b>Install Content Rendering Engine</b> Follow the installation instructions outlined in the <b>Content Rendering Engine Installation Guide</b> , available on <a href="#">Accessing Other Documents</a> to configure and install this product.
Onboarding	<b>Meet minimum app and OS requirements</b> <ul style="list-style-type: none"> <li>• iOS VMware Content Locker v2.4+</li> <li>• iOS 7+ device</li> </ul>



# Chapter 2:

## File Storage

- Overview of Storage Options by Content Type .....10
- Overview for Content Management Enterprise Integration  
Solution .....10
- Set Content Storage Capacity ..... 11
- Restrict File Extensions ..... 12

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

## Overview for Content Management Enterprise Integration Solution

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 file types listed below:

- Word (doc, docx)
- Excel (xls, xlsx)
- BMP
- PDF
- Power Point (ppt, pptx)
- JPEG, JPG
- PNG
- 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
<b>Organization Group Name</b>	Specify the group to which you want to apply content storage restrictions.
<b>Capacity</b>	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.
<b>Overage Allowed</b>	Enter the amount of overage you want to allow, if any. For SaaS customers, this value is not configurable.
<b>Max File Size</b>	Use the default value of 200 MB as the maximum size for uploads. If operating against this recommendation, 2 GB is the upper limit.
<b>Encryption</b>	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
<b>Whitelist</b>	Enter the file extensions you want to include. Separate extensions using a new line, a comma, or a space.
<b>Blacklist</b>	Enter the file extensions you want to exclude. Separate extensions with a line break, a comma, or a space.
<b>All</b>	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 of Corporate File Servers ..... 14
- Enable End-User Access to Corporate File Server Content ... 14
- Support for Corporate File Servers ..... 15
- Configure an Admin Repository ..... 17
- Enable Users to Sync Corporate File Servers .....18
- Configure Repository Details .....19

## Overview of Corporate File Servers

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	✓	✓	✓
CMIS	✓	✓	✓
Google Drive	✓	–	–
Network Share <sup>¥</sup>	✓	✓	✓
OneDrive	✓	–	–
OneDrive for Business	✓	–	–
OneDrive for Business ADFS	✓	–	–
OneDrive for Business OAuth	✓	–	–
SharePoint	✓	✓	✓
SharePoint ADFS	✓	✓	✓
SharePoint O365	✓	✓	✓
SharePoint O365 ADFS	✓	✓	✓
SharePoint O365 OAuth	✓	✓	✓

	Admin	Automatic	Manual
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	✓	✓	✓
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	✓ **	✓ **	✓ **



	Admin	Automatic	Manual
SharePoint O365 ADFS	✓ **	✓ **	✓ **
SharePoint O365 OAuth	✓	✓	✓
SharePoint - Personal (My Sites)	✓ **	—	—
SharePoint WebDAV	✓ **	—	—
SharePoint Windows Auth	✓ **	✓ **	✓ **
WebDAV	✓ *	✓ *	✓ *
<b>Legend:</b>			
¥ =The VMware Content Gateway on Linux servers supports only SMB v2.0 and SMB v3.0. The default supported version is SMB v2.0. ✓ + = Required ✓ = Supported — = Not Supported ✓ * = 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
<b>Name</b>	Label the content directory.
<b>Type</b>	Select a Corporate File Server from the drop-down menu.
<b>Link</b>	Provide the full path to the directory location rather than the root domain. <b>Example:</b> http://SharePoint/Corporate/Documents A URL copied directly from a web browser might not have permission to access a server for certain repository types.
<b>Organization Group</b>	Assign Corporate File Server access to a selected group of users.

Setting	Description
<b>Authentication Type</b>	Select the access level admins have to Corporate File Servers from the UEM console. <ul style="list-style-type: none"> <li>• <b>None</b> – Prevent administrators from viewing and downloading Corporate File Server content from the UEM console.</li> <li>• <b>User</b> – Permit browsing of the repository file structure within the UEM console. Enter credentials into the <b>Username</b> and <b>Password</b> text boxes that appear.</li> </ul>
<b>Access via Content Gateway</b>	Use the Content Gateway if the Workspace ONE UEM server's domain cannot access the Corporate File Server.
<b>Content Gateway</b>	Identify the unique name of the appropriate Content Gateway node from the drop-down menu.
<b>Allow Inheritance</b>	Permit child organization groups to inherit the same access permissions as their parent organization group.
<b>Allow Write</b>	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.
<b>Allow Delete</b>	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
<b>Name</b>	Label the content directory.
<b>User Repository Name</b> <i>(auto template only)</i>	Use look-up values to name the repository after the end user within the VMware Content Locker.
<b>Type</b>	Select a Corporate File Server from the drop-down menu.
<b>Link</b>	A URL copied directly from a web browser might not have permission to access a server for certain repository types.
<b>Link</b> <i>(auto template only)</i>	Use look-up values to create a repository when an end user accesses the VMware Content Locker. <b>Example:</b> https://sharepoint.acme.com/share/{EnrollmentUser}
<b>Link</b> <i>(manual template only)</i>	Provide the path to the directory location using * as a wildcard for a domain link. <b>Example:</b> http://*.sharepoint.com
<b>Organization Group</b>	Assign Corporate File Server access to a specified group of users.
<b>Access via Content Gateway</b>	Use the Content Gateway if the Workspace ONE UEM server's domain cannot access the Corporate File Server.
<b>Allow Inheritance</b>	Allow child organization groups to inherit the same access permissions as their parent organization group.
<b>Allow Write</b>	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 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.

Setting	Description
<b>Document Sharing</b>	It is recommended that you disable the sharing settings for maximum security. You can enable them for configuring end user collaboration.
<b>Access Control</b>	Set to <b>Allow Offline Viewing</b> to give end users the most viewing freedom for their document. Configure <b>Allow Online Viewing Only</b> to ensure that all devices accessing content are compliant, as Workspace ONE UEM cannot scan offline devices for compliance.
<b>Force Encryption</b>	Select to force documents to open in the VMware Content Locker.
<b>Open in Email</b>	Allow content to open in emails.
<b>Allow Open in Third Party Apps</b>	Give permission to open this content in other applications. You can set a list of approved apps in the SDK Profile.
<b>Allow Saving to Other Repositories</b>	Select to allow your end users to save this file to their Personal Content.
<b>Enable Watermark</b>	Select to add a watermark overlay to the file. Configure the Overlay Text for the watermark as part of an SDK profile.
<b>Allow Printing</b>	Give end users 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.
<b>Allow Edit</b>	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
<b>Device Ownership</b>	Define as <b>Any</b> , <b>Corporate-Dedicated</b> , <b>Corporate-Shared</b> , <b>Employee Owned</b> or <b>Undefined</b> .
<b>Organization Groups</b>	Start typing in the field to assign the content to a new group.
<b>User Groups</b>	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
<b>Transfer Method</b>	Specify <b>Any</b> method or <b>Wi-Fi Only</b> from the drop-down menu. Restricting transfers to Wi-Fi forces devices to check in with Workspace ONE UEM to ensure compliance.
<b>Download While Roaming</b>	Enable to allow your end users to download content while roaming.
<b>Download Type</b>	Set to deploy content one of two ways: <ul style="list-style-type: none"> <li>• <b>Automatically</b> – Installs on devices as soon as content becomes available.</li> <li>• <b>On Demand</b> – Installs on devices only at the end user's request.</li> </ul>
<b>Download Priority</b>	Define to let your end users know if the content download is <b>Normal</b> , <b>High</b> or <b>Low</b> priority.
<b>Required</b>	Select to flag content as required in the VMware Content Locker. End users must download and review required content in order for their devices to maintain compliance with Workspace ONE UEM.
<b>Effective Date</b>	Specify to configure a limited range of content availability.
<b>Expiration Date</b>	Specify to configure a limited range of content availability.

4. Select **Save**.

# Chapter 4:

## AirWatch Managed Content

Overview of Workspace ONE UEM Managed Content Repository .....	23
Configure the Workspace ONE UEM Managed Content Category Structure .....	23
Upload Content to the Workspace ONE UEM Managed Repository .....	24
Upload Workspace ONE UEM Managed Content in Batches ..	25
Local File Storage for Workspace ONE UEM Managed Content .....	25

## Overview of Workspace ONE UEM Managed Content Repository

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, see [Configure the Workspace ONE UEM Managed Content Category Structure on page 23](#).

## Configure the Workspace ONE UEM 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
<b>Managed By</b>	Select the organization group or groups you want to apply the category.
<b>Name</b>	Enter a name that is easily recognizable and applies to a clear set of content.
<b>Description</b>	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
<b>Managed By</b>	Review the organization group of the parent category that populates by default.
<b>Name</b>	Enter a name that is easily recognizable and applies to a clear set of content.
<b>Description</b>	Provide a brief description of the subcategory.

## Upload Content to the Workspace ONE UEM 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
<b>Name</b>	Review the filename that automatically populates in this text box.
<b>Organization Group</b>	Review the organization group to which this content deploys.
<b>File</b>	Review the file that populates in this text box.
<b>Storage Type</b>	Ensure that the text box displays AirWatch Managed.
<b>Version</b>	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.
<b>Description</b>	Provide a description of the files you upload.
<b>Importance</b>	Set the content importance as <b>High</b> , <b>Normal</b> , or <b>Low</b> .
<b>Category</b>	Map the uploaded content to a configured Category.



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


Setting	Description
<b>Author</b>	Name the author of the file.
<b>Notes</b>	Provide notes on the file.
<b>Subject</b>	Provide a subject.
<b>Keywords</b>	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.

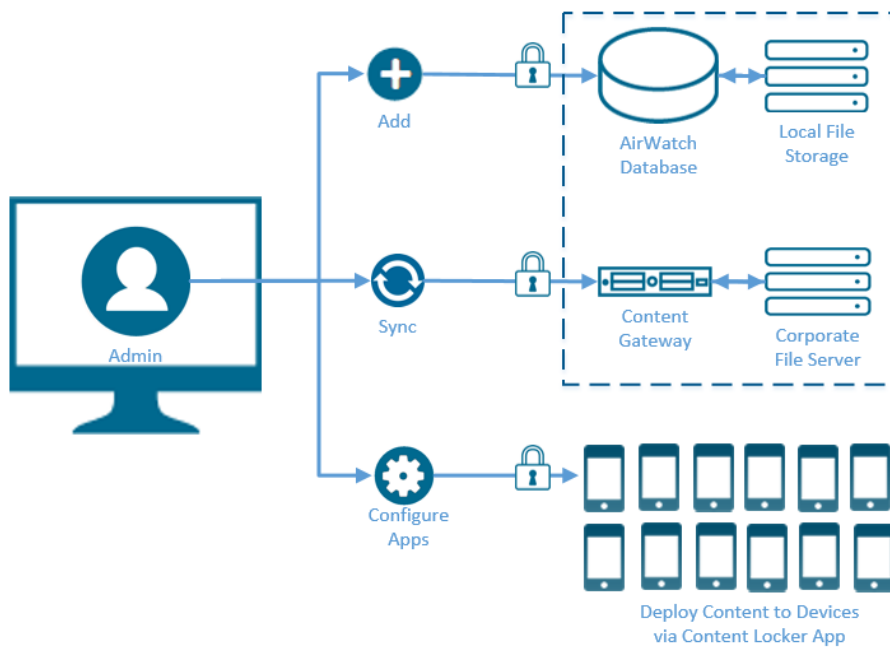
To upload a batch import:

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.



## Introduction to 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

In v9.0.2 console version 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 (.ipa, .pak, .appx, .msi, .exe, and so on) that you upload through the UEM console are stored in a file storage location. File storage is required to deploy Win32 applications 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.

### 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 **File Storage Enabled** and configure the settings.

Setting	Description
<b>File Storage Path</b>	Enter your path in the following format: \\{Server Name}\{Folder Name}, where Folder Name is the name of the shared folder you created on the server.
<b>File Storage Caching Enabled</b>	<p>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.</p> <p>If you enable caching, accommodate for the amount of space needed on the server where these files cache. For more information, see <a href="#">File Storage Requirements on page 27</a>.</p> <p>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 <b>VMware Workspace ONE UEM CDN Integration Guide</b> (<a href="https://resources.air-watch.com/view/8cr52j4hm6xfvt4v2wgg/en">https://resources.air-watch.com/view/8cr52j4hm6xfvt4v2wgg/en</a>).</p>
<b>File Storage Impersonation Enabled</b>	Select to add a service account with the correct permissions.
<b>File Storage Impersonation Username</b>	Provide a valid service account username to obtain both read and write permissions to the shared storage directory.
<b>Password</b>	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 of Personal Content Repository .....30
- Enable Personal Content ..... 31
- Roles for Folder Sharing ..... 32
- Configure Personal Content Quota Exceptions ..... 33
- File Encryption Migration .....33

## Overview of Personal Content Repository

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
<b>Storage Quota</b>	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.
<b>User Quota</b>	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.
<b>User Group Quota(s)</b>	Select <b>Add New</b> 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
<b>Link Sharing</b>	Enable link sharing of documents.
<b>Auto Expire Days</b>	Enable and fill in a numerical value to specify the number of <b>Days</b> links remain available for sharing.  Disable to leave the option open for end users to configure when they share their links.
<b>Auto Expire Downloads</b>	Enable and input a numerical value to set the maximum number of <b>Downloads</b> before the link expires.  Disable to leave the option open for end users to configure when they share their links.
<b>Require Password Protection</b>	Enable and set the <b>Minimum Length</b> in characters and the <b>Complexity</b> 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
<b>Share with User Groups</b>	Enable to share folders with entire user groups instead of manually listing each user.

Setting	Description
<b>Available Sharing Roles</b>	Set the roles available to end users sharing their folders.
<b>Share with External Users</b>	Enable end users to share folders with users external to their Organization Group.
<b>Available Sharing Roles</b>	Set the access privilege role for those users that end users share a folder with. See the <a href="#">Folder Sharing Roles</a> matrix, for an overview of sharing roles and their permissions.
<b>User Quota</b>	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
<b>Email Notifications</b>	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
<b>Allow Open in Email</b>	Enable to allow content to open in emails. Disable for maximum security.
<b>Allow Open in Third Party Apps</b>	Enable to open personal content in other applications. You can set a list of approved apps in the SDK Profile. Disable for maximum security.
<b>Allow Printing</b>	Enable iOS devices to print personal content PDFs using AirPrint. Disable for maximum security.
<b>Watermark</b>	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	✓	✓	✓		



	Owner	Co-Owner	Editor	Reader	Viewer
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 of VMware Content Locker .....	35
Configure VMware Content Locker .....	35
Configure Document Extensions .....	37
VMware Content Locker Capabilities by Platform .....	38
Matrix of Supported File Type by Platform .....	44

## Overview of VMware Content Locker

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
<b>Application Profile</b>	Set to define the security policies and settings used by this application.  Leave as <b>Default</b> and configure the Recommended Default SDK settings to define app behavior using Workspace ONE UEM recommendations.  Alternatively, select <b>Custom</b> application settings to override the default SDK settings and configure a unique set off behaviors for the app.
<b>iOS Profile</b>	Select a custom-created SDK profile from the drop-down list.
<b>Android Profile</b>	Select a custom-created SDK profile from the drop-down list.
<b>Use Legacy Settings and Policies</b>	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.
<b>Default Authentication Method</b>	Select the authentication method for the applications.

Setting	Description
<b>Enable "Keep me signed in"</b>	Enable to allow end users to remain signed in between uses.
<b>Maximum Number of Failed Attempt</b>	Set the number of passcode entry attempts allowed before all data in the VMware Content Locker will be wiped from a device.
<b>Authentication Grace Period (min)</b>	Enter the time (in minutes) after closing the VMware Content Locker before reopening the VMware Content Locker will require users to enter credentials again.
<b>Prevent Compromised Devices</b>	Enable to prevent compromised devices from accessing VMware Content Locker.
<b>Enable Offline Login Compliance</b>	Enable to allow offline login compliance.
<b>Maximum Number of Offline Logins</b>	Enter the number of offline logins allowed before you have to go online.

3. Configure the **General** settings.

Setting	Description
<b>Numbers of Days to Keep Content New</b>	Select the number of days recently added documents will be labeled as new in the VMware Content Locker.
<b>Block Enrollment via Content Locker, Boxer, and Browser</b>	<p>Enable to prevent enrollment through VMware Content Locker, VMware Boxer, and VMware Browser.</p> <p>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.</p>
<b>Change Repository Name</b>	Enable to change the repository name in the <b>Root Repository Name</b> field that appears.
<b>Root Repository Name</b>	Enter the new repository name you want to use.
<b>Allow Hyperlinks</b>	Enable to allow end users to open hyperlinks located in documents in the <b>Open Internet Links with</b> field that appears.
<b>Open Internet Links with</b>	Select the application in which to open hyperlinks.
<b>Local Storage</b>	<p>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.</p> <p>Disable local storage to force all user content to save in a location that syncs with other Personal Content in the cloud.</p>
<b>Upload on Wi-Fi Only</b>	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
<b>Application Type</b>	Indicate as <b>System</b> or <b>Internal</b> .
<b>Application Name</b>	Assign to the application.
<b>Bundle ID</b>	Assign to the application.
<b>Badge Count</b>	<p>Set to <b>Required</b>, <b>Updates Only</b> or <b>None</b>.</p> <p><b>Required:</b> 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.</p> <p><b>Updates Only</b> (For Downloaded Content): Badge Count represents the number of downloaded documents that have updates or new versions available.</p> <p><b>None:</b> Badge Counts are disabled for Content Locker.</p>

- 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.

- 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

- Navigate to **Apps > Settings and Policies > Security Policies**.
- Set **Limit Documents to Open Only in Approved Apps** to **No**.
- 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.

- Navigate to **Content > Repositories > Admin Repositories**.
- Select the **Edit** icon next to the Corporate File Server that syncs to end-user devices.
- 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 April 2018.

Features	iOS	Android	Win 10	Win 8	Win PC
Security					
Authentication					
Basic	✓	✓	✓	✓	✓
AD/LDAP	✓	✓	✓	✓	✓

Features	iOS	Android	Win 10	Win 8	Win PC
Token	✓	✓	✓	✓	✓
Second Factor Passcode	✓	✓	✓	✓	
<b>Encryption</b>					
SSL Encryption in Transit	✓	✓	✓	✓	✓
AES 256-Bit Encryption at Rest	✓	✓	✓	✓	✓
In Memory Encryption	✓	✓			
FIPS 140-2	✓	✓	✓	✓	
Certificate Pinning	✓				
<b>IT Policies</b>					
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	✓	✓	✓	✓	✓
Prevent deleting mandatory content	✓	✓	✓	✓	
<b>DLP</b>					
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.				

Features	iOS	Android	Win 10	Win 8	Win PC
<b>Data Collection</b>					
Install Content	✓	✓	✓	✓	✓
Open/Close Content	✓	✓	✓	✓	✓
Uninstall/Delete Content	✓	✓	✓	✓	✓
Session Status	✓	✓	✓	✓	✓
<b>Mobile Experience</b>					
<b>Access</b>					
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	✓	✓	✓	✓	✓
<b>Content Views</b>					
Featured Content (Folder, File, Category)	✓	✓	✓	✓	✓
All Content (All/Installed/Uninstalled)	✓	✓	✓	✓	✓
Recent Activity (Recently Updated and Viewed)	✓	✓	✓	✓	✓
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	✓				
<b>File Management</b>					
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	✓	✓			



Features	iOS	Android	Win 10	Win 8	Win PC
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)	✓				
<b>Usability</b>					
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	✓		✓	✓	
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)	✓	✓	✓	✓	✓
<b>User Managed Content (Personal/Local Storage)</b>					
<b>Personal Content Policies</b>					
Enable/Disable access to Personal Content	✓	✓	✓	✓	✓
Storage quota control by user and group	✓	✓	✓	✓	✓
Store Personal Content in Remote File Storage (RFS)	✓	✓	✓	✓	✓

Features	iOS	Android	Win 10	Win 8	Win PC
Enable/Disable Link Sharing	✓	✓	✓	✓	
Enforce link sharing policies for max days, max downloads, password	✓	✓	✓	✓	
Enable/Disable Folder Sharing	✓	✓	✓	✓	
<b>File Management</b>					
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	✓	✓			
<b>Collaboration</b>					
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	✓	✓	✓	✓	
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	✓	✓	✓	✓	
<b>Customization and Integration</b>					
<b>External File Repository Integration</b>					
Share Point 2007	✓	✓	✓	✓	✓
Share Point 2010	✓	✓	✓	✓	✓
Share Point 2013	✓	✓	✓	✓	✓
Share Point Online (Office 365)	✓	✓	✓	✓	✓

Features	iOS	Android	Win 10	Win 8	Win PC
Network File Share	✓	✓	✓	✓	✓
WebDAV	✓	✓		✓	✓
FileServer (HTTP)	✓	✓		✓	
Google Drive	✓	✓	✓	✓	✓
OneDrive	✓	✓	✓	✓	✓
CMIS	✓	✓		✓	✓
User Added Repository Support	✓	✓	✓	✓	✓
One Drive for Business	✓	✓			
Box	✓	✓	✓		
<b>Localization</b>					
Arabic	✓	✓	✓	✓	✓
Chinese - Simplified	✓	✓	✓	✓	✓
Chinese - Traditional	✓	✓	✓	✓	✓
Czech	✓	✓	✓	✓	✓
Danish	✓	✓	✓	✓	✓
Dutch	✓	✓	✓	✓	✓
English	✓	✓	✓	✓	✓
French	✓	✓	✓	✓	✓
Hebrew	✓	✓	✓		✓
German	✓	✓	✓	✓	✓
Italian	✓	✓	✓	✓	✓
Japanese	✓	✓	✓	✓	✓
Korean	✓	✓	✓	✓	✓
Polish	✓	✓	✓	✓	✓
Portugese - Brazil	✓	✓	✓	✓	✓
Russian	✓	✓	✓	✓	✓
Spanish	✓	✓	✓	✓	✓
Swedish	✓	✓	✓	✓	✓
Turkish	✓	✓	✓	✓	✓
<b>Email Attachment and Integration</b>					
Allow Viewing of Attachments and saving to VMware Content Locker	✓	✓	✓	✓	

Features	iOS	Android	Win 10	Win 8	Win PC
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)	✓				
<b>VMware Browser Integration</b>					
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 April 2018.

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

Supported File Types	iOS	Android	Windows 10
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	✓	✓	
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		✓	

Supported File Types	iOS	Android	Windows 10
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 .....	48
Custom SDK Profile Settings .....	48
Configure Default SDK Security Settings .....	49
Expected Behavior for SDK Authentication .....	53

## 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
<b>Implementation</b>	Share SDK profile settings across <i>all</i> applications set up at a particular organization group (OG) or below.	Apply SDK profile settings to a <i>specific</i> application, and override the Default Settings SDK profiles.
<b>Advantage</b>	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.
<b>Configure</b>	<b>Groups &amp; Settings &gt; All Settings &gt; Apps &gt; Settings and Policies &gt; Security Policies</b>	<b>Groups &amp; Settings &gt; All Settings &gt; Apps &gt; Settings and Policies &gt; Profiles</b>
<b>Read More</b>	Continue reading this section to learn which default SDK profiles apply to deployed apps.	Learn more about custom SDK profile settings in the <b>VMware Workspace ONE UEM Mobile Application Management Guide</b> .

## 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 settings 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
<b>Authentication Method</b>	Defaults to Single Sign-On. Ensure you require MDM enrollment so that Single Sign-On can function properly.
<b>iOS Profile</b>	Select a custom-created SDK profile from the drop-down list the settings profile for iOS devices.
<b>Android Profile</b>	Select a custom-created SDK profile from the drop-down list the settings profile for Android devices.



Setting	Description
<b>Use Legacy Settings and Policies</b>	Only enable legacy settings if directed to do so by an Workspace ONE UEM representative. Legacy settings do not leverage Shared SDK profile settings and should only be implemented in certain edge cases.
<b>Default Authentication Method</b>	Select the authentication method for the applications.
<b>Enable "Keep me signed in"</b>	Enable to allow end users to remain signed in between uses.
<b>Maximum Number of Failed Attempt</b>	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.
<b>Authentication Grace Period (min)</b>	Enter the time (in minutes) after closing the VMware Content Locker before reopening the VMware Content Locker will require users to enter credentials again.
<b>Prevent Compromised Devices</b>	Enable to prevent compromised devices from accessing VMware Content Locker.
<b>Enable Offline Login Compliance</b>	Enable to allow offline login compliance.
<b>Maximum Number of Offline Logins</b>	Enter the number of offline logins allowed before you have to go online.

## Configure Default SDK Security Settings

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

### Before You Begin

Not all platforms or Workspace ONE UEM applications support all available default SDK profile settings. A configured setting only expresses as a device side behavior when it has a full platform and app-side support. This also means that an enabled setting might not express 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
- Enrolled devices
- Workspace ONE UEM Inbox
- Workspace ONE UEM or wrapped apps
- VMware Content Locker
- SDK settings available as of April 2018.

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

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

Action	Description	Rec
<b>Data Loss Prevention</b>		
<b>Enabled</b>	Access and configure settings intended to reduce data leaks.	√
	<b>Enable Printing</b>	
	Allows an application to print from devices when set to <b>Yes</b> .	
	<b>Enable Camera</b>	
	Allows applications to access the device camera when set to <b>Yes</b> .	
	<b>Enable Composing Email</b>	
	Allows an application to use the native email client to send emails when set to <b>Yes</b> .	
	<b>Enable Copy And Paste Out</b>	
	Allows users to copy and paste data from Workspace ONE UEM applications (containerized applications such as Boxer, Browser, Content Locker) to external applications (non-containerized applications). Select <b>No</b> to allow copy and paste actions only between Workspace ONE UEM apps.	
	<b>Enable Copy And Paste Into</b>	
	Allow users to cut, copy, and paste data from external applications (non-containerized applications) into Workspace ONE UEM applications (containerized applications such as Boxer, Browser, Content Locker).	
	<b>Enable Data Backup</b>	
	Allows wrapped applications to sync data with a storage service like iCloud when set to <b>Yes</b> .	
	<b>Enable Location Services</b>	
	Allows wrapped applications to receive the latitude and longitude of the device when set to <b>Yes</b> .	
	<b>Enable Bluetooth</b>	
	Allows applications to access Bluetooth functionality on devices when set to <b>Yes</b> .	
	<b>Enable Screenshot</b>	
	Allows applications to access screenshot functionality on devices when set to <b>Yes</b> .	
	<b>Enable Watermark</b>	
	Displays text in a watermark in documents in the VMware Content Locker when set to <b>Yes</b> . Enter the text to display in the <b>Overlay Text</b> field or use lookup values. You cannot change the design of a watermark from the UEM console.	
	<b>Limit Documents to Open Only in Approved Apps</b>	
	Enter options to control the applications used to open resources on devices.	
	<b>Allowed Applications List</b>	
	Enter the applications that you allow to open documents.	

Action	Description	Rec
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 Workspace ONE UEM brand throughout the app suite.	✓
Logging		
Enabled	Access and configure settings related to collecting logs.	✓
	<b>Logging Level</b>	
	Choose from a spectrum of recording frequency options:	
	<ul style="list-style-type: none"> <li>• <b>Error</b> – Records only errors. An error displays failures in processes such as a failure to look up UIDs or an unsupported URL.</li> <li>• <b>Warning</b> – Records errors and warnings. A warning displays a possible issue with processes such as bad response codes and invalid token authentications.</li> <li>• <b>Information</b> – Records a significant amount of data for informational purposes. An information logging level displays general processes as well as warning and error messages.</li> <li>• <b>Debug</b> – Records all data to help with troubleshooting. This option is not available for all functions.</li> </ul>	
	<b>Send logs over Wi-Fi only</b>	
	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.**

## 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
<b>Disabled</b>	Enabled	Single	Enrollment Credentials	Open apps without prompting end users to enter credentials.
<b>Passcode</b>	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.
<b>Username and Password</b>	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.
<b>Passcode</b>	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.
<b>Username and Password</b>	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.

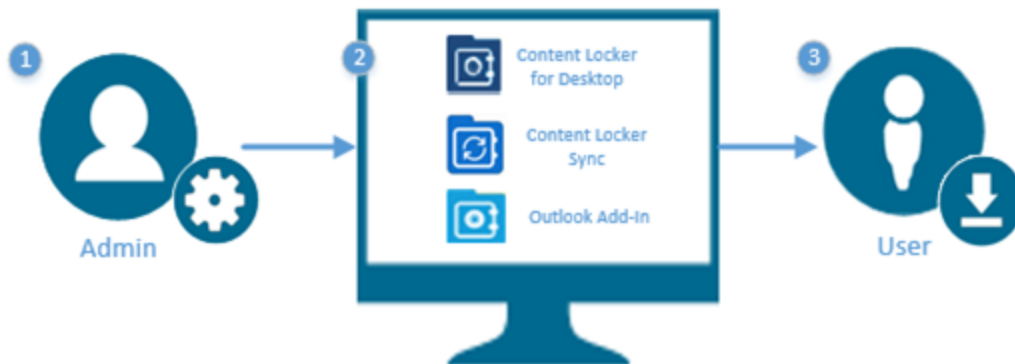
# Chapter 8:

## VMware Content Locker Collaborate

VMware AirWatch Content Apps for Desktop .....	55
Enable VMware Content Locker Sync .....	55
Configure Outlook Add-In .....	56
Enable Digital Signatures in the Self-Service Portal .....	57
Enable Personal Content Uploads in Socialcast .....	57

## 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
<b>VMware Content Locker for Desktop</b>	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.
<b>VMware Content Locker Sync</b>	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.
<b>VMware Content Locker Outlook Add-In</b>	Enables end users to send shared links to 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
<b>VMware Content Locker Sync</b>	<b>Enable</b> sync functionality associated with the product.
<b>Client Download</b>	<b>Enable</b> the end-user sync client downloads from the Self-Service Portal. <b>Disable</b> the end-user sync client downloads if implementing an enterprise deployment of Content Locker Sync using the MSI installer.
<b>Require MDM Enrollment</b>	<b>Enable</b> 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 **sTerms 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
<b>Client Download</b>	<b>Enable</b> to allow end users to download the Outlook Add-In client from the Self-Service Portal. <b>Disable</b> if your organization does an enterprise deployment of Outlook Add-In.
<b>Automatically convert attachments to links</b>	<b>Enable</b> to automatically convert large attachments into a link. Enter the amount that triggers the conversion of attachments to links into the field that appears.
<b>Recommend converting attachments to links</b>	<b>Enable</b> 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
<b>eSignature Provider</b>	Select your organization's eSignature provider from the drop-down menu. Unlisted providers are unavailable for integration.
<b>URL</b>	Provide your account URL in the field.
<b>Integration Key</b>	Provide the account integration key in the field.
<b>Username</b>	Provide your account username in the field.
<b>Password</b>	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
<b>Service</b>	Enter <b>Socialcast</b> as the service name.
<b>Account Type</b>	Select <b>Admin</b> from the drop-down menu.
<b>API Key</b>	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
<b>AirWatch Domain</b>	Provide the URL of your Workspace ONE UEM instance.
<b>API Key</b>	Paste the API key you copied from the UEM console into the text box.

# Chapter 9:

## Application Deployment

Overview of Workspace ONE UEM Application Deployment	60
Deploy Workspace ONE UEM Applications .....	60
Overview for Onboarding VMware Content Locker .....	60
Enable Onboarding for VMware Content Locker .....	61

## Overview of 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 your AirWatch representative 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
<b>Managed By</b>	View the organization group the application uploads in.
<b>Platform</b>	Choose the appropriate platform.
<b>Name</b>	Enter a descriptive name in the field to help search for the application in an app store.
<b>Search App Store</b>	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
<b>VMware Content Locker</b>	Locked in the Required Content View	Locked in the Required Content View
<b>Other Device Apps</b>	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, onboarding, 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**.

- Set **Onboarding** to **Enabled** and configure the settings that appear.

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

- Select **Save**.

# Chapter 10:

## Overview of Content Management

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 64](#) and [Settings for Content Management on page 66](#).

### 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.
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.

Setting	Description
<b>Categories</b>	Add categories and subcategories. Added categories are displayed on the screen in a list view with an action menu.
<b>Featured Content</b>	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.
<b>Batch Status</b>	Perform a Batch Import and review the details of your uploaded batch from this screen.
<b>Settings</b>	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
<b>Storage History</b>	Overview storage quotas using the six-bar graphical summary.
<b>User/Content Status</b>	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.
<b>Content Engagement</b>	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.
<b>User Breakdown</b>	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
<b>AirWatch Managed</b>	View and manage the content you directly added to the UEM console in this default list view.



Setting	Description
<b>AirWatch Managed Menu</b>	Act on AirWatch Managed Content using the available list view options. <ul style="list-style-type: none"> <li>• <b>Add Content</b> – Select to add AirWatch Managed Content to the UEM console.</li> <li>• <b>Storage Used</b> – Review the status bar to see the percentage of allotted storage consumed by end users.</li> </ul>
<b>Corporate File Servers</b>	View and manage synced repositories in this list view, or use the content list views for individual repositories.
<b>Corporate File Servers Menu</b>	To display configured repositories in the list view, select <b>Show Repositories</b>
<b>Filter</b>	Find desired documents using the available filters. <ul style="list-style-type: none"> <li>• <b>Category</b> – Filter content using the categories assigned from the UEM console.</li> <li>• <b>Type</b> – Filter content based on the file type.</li> <li>• <b>Expiration Status</b> – Filter content to display only the content set to expire in 14 days.</li> </ul>
<b>Active/Inactive</b>	Information about the content availability to end users. <ul style="list-style-type: none"> <li>• Green circles display next to active content.</li> <li>• Red circles display next to inactive content. Inactive content is not searchable, viewable, or sent automatically to devices.</li> </ul>
<b>Name</b>	Select to edit the general <b>Info</b> , <b>Details</b> , <b>Previous Version</b> , <b>Security</b> , <b>Assignment</b> , and <b>Deployment</b> information you configured when adding your content. You can also download or delete previous content versions.
<b>Action Menu</b>	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
<b>Edit</b>						
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.	✓					
<b>Delete</b>						
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.						✓
<b>Add</b>						
Update an existing file with a new version, archiving the original file.	✓					
Add a subcategory to a category.						✓
<b>Sync</b>						
Initiate a sync between Workspace ONE UEM and integrated Corporate File Servers.		✓	✓	✓	✓	
<b>View Devices</b>						
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.	✓	✓	✓	✓	✓	
<b>Additional Options</b>						
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
<b>Applications</b>	Access the configuration screens for VMware Content Locker, VMware Content Locker Sync, and the Outlook Add-In.
<b>Content Gateway</b>	Configure Content Gateway and download the installer.
<b>Personal Content</b>	Enable and configure Personal Content settings for end users.
<b>User Storage</b>	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.
<b>Remote Storage</b>	Configure Remote File Storage and download the installer
<b>Content Viewer</b>	Configure Content Rendering Engine and download the installer.
<b>Advanced</b>	Configure file type restrictions, on-boarding and requiring content for on-boarding, and integrating with a third-party e-Signature vendor.