Mobile Content Management

VMware Workspace ONE UEM 2011

vmware®

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

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

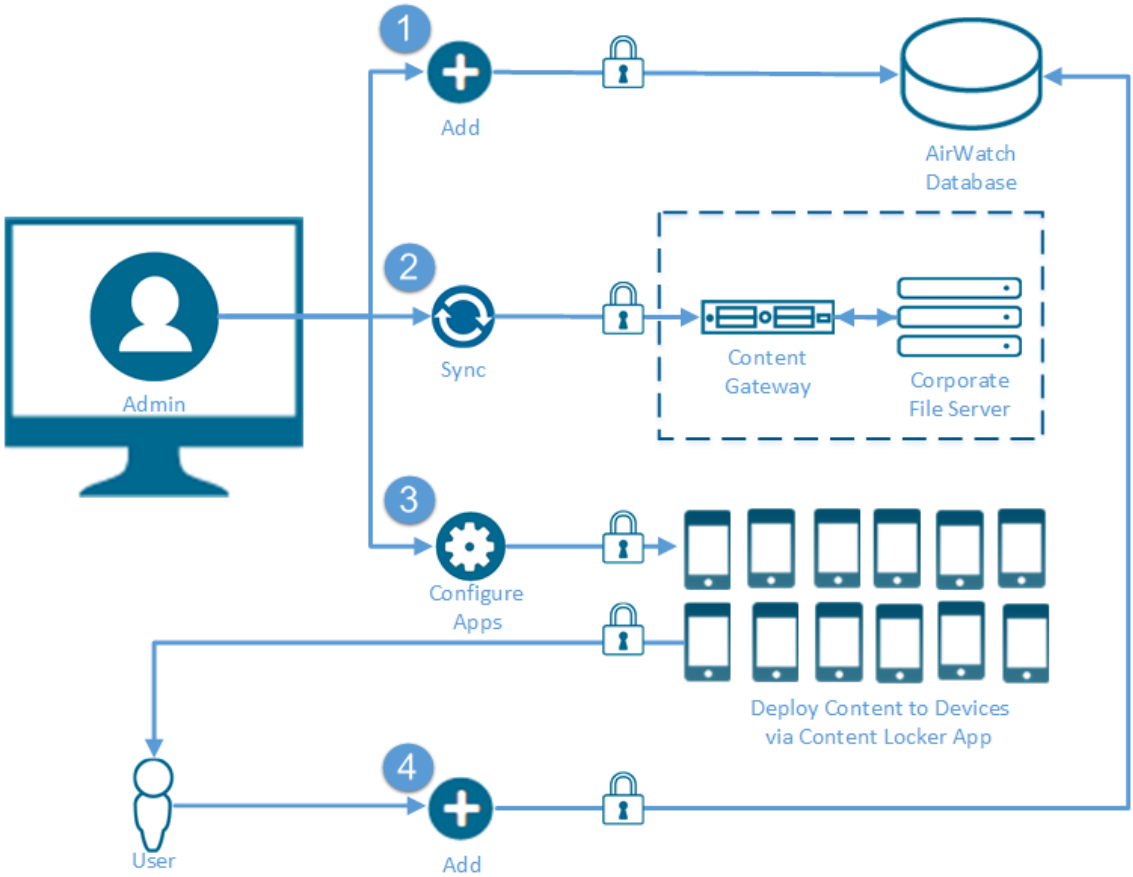
Contents

Introduction to Mobile Content Management

1

Workspace ONE UEM powered by AirWatch provides the Mobile Content Management™ (MCM) solution that 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 Workspace ONE Content app.

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



1 **UEM 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 Workspace ONE Content** – Refers to the app that deploys to end-user devices, enabling access to content within the configured set of parameters.

This chapter includes the following topics:

Requirements for Mobile Content Management

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

Component	Requirement & Description
Software and Hardware Requirements	
Supported Browsers	The Workspace ONE Unified Endpoint Management (UEM) console supports the latest stable builds of the following web browsers. ■ Chrome ■ Firefox ■ Safari ■ Internet Explorer 11 ■ Microsoft Edge **Note** If using IE to access the UEM console, navigate to **Control Panel > Settings > Internet Options > Security** and ensure you have a security level or custom security level that includes the **Font Download** option being set to **Enabled**. If you are using a browser older than those listed above, upgrade your browser to guarantee the performance of the UEM console. Comprehensive platform testing has been performed to ensure functionality using these web browsers. The UEM console may experience minor issues if you choose to run it in a non-certified browser.
Platform Requirements	iOS 7.2 and later Android 3.2 and later Windows 7 Windows 8 Windows 10 10.9 Mavericks and later
Framework Requirements	.NET 4.0.3 and later .NET 4.5 and later Mono
Visual Studio Requirements	Visual Studio 2010 v10.0.50903 Visual C++ 2008
Other	Link Sharing enabled Microsoft Outlook 2007+ (32-bit or 64-bit)

Component	Requirement & Description
Role Requirements	
Admin Roles	**Select a role that has Content, Content Device Install, and Content Device Remove enabled by default.** Grants access to the content management page and control of content distribution. For more information on creating roles, read the **Roles and Added Resources Guide**.
End-User Roles	**Enable Manage Content and grant Full Access** For more information on creating roles, read the **Roles and Added Resources Guide**.
Repository Requirements	
UEM Managed Content	Configure the category structure before uploading content You cannot add subcategories to categories that have content in them.
Corporate File Server Content	Install Content Gateway Install Content Gateway to establish a connection in instances where the Workspace ONE UEM server domain cannot access a Corporate File Server. To review which Workspace ONE UEM supported repositories require, support, or do not support Content Gateway, see Support for Corporate File Servers. For comprehensive installation instructions, read the **Content Gateway Installation Guide**.
Alternative File Storage Requirements	
Local File Storage	Determine Appropriate Solution for Organization For more information on available options, see Local File Storage for Workspace ONE UEM Managed Content.
Optional Security Component Requirements	
Onboarding	Meet minimum app and OS requirements ■ iOS VMware Workspace ONE Content v2.4+ ■ iOS 7+ device
App Requirements	
Workspace ONE Content	

File Storage

2

Various content types are available for configuration in the Workspace ONE UEM console that can be deployed to the VMware Workspace ONE Content 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 table. Learn about the additional configuration and components requirements for each storage option.

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

This chapter includes the following topics:

Content Management Enterprise Integration Solution

Workspace ONE UEM powered by AirWatch provides the Content Management solution which along with the other enterprise integration components addresses the unique challenge of securing the content on mobile devices. Content Gateway is one such component that facilitates end users to securely access content.

Content Gateway

The Content Gateway, together with the VMware Workspace ONE Content app, 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 the VMware Workspace ONE Content app, 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 the VMware Workspace ONE Content app allows you to provide unmatched levels of access to your corporate content without sacrificing security.

Set Content Storage Capacity

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

Procedure

1 Navigate to **Groups & Settings > All Settings > Admin > Storage** at a Customer or Global organization group level.

Note You must ensure you have the required admin privileges to view and use the storage settings.

2 Select **Content** from the **Storage Type** drop-down menu.

3 Select the **Edit** icon for the appropriate Organization Group. The Storage Management window appears. Complete the settings.

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

4 Select **Save**.

Restrict File Extensions

Specify file type permissions by creating an allowlist or denylist for Corporate File Server and Managed content. This restriction hides blocked file types based on their extension from being visible in the UEM console or within the Workspace ONE Content app and so prevents them from being downloaded or uploaded to Content Repositories.

Procedure

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

2 Set the **Allowed File Extensions**.

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

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

What to do next

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	UEM Managed
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 (throughWorkspace ONE Content app)	Corporate File Server

Corporate File Servers

3

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

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 Workspace ONE Content.

This chapter includes the following topics:

- Configure an Admin Repository
- Enable Users to Sync Corporate File Servers
- Configure Repository Details
- Cache Performance

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.

Procedure

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 Workspace ONE Content 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. Each assigned user receives the same static link to the file repository.

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

Note Irrespective of the number of files present in the repository folders, only 1K files in any folder that are sorted alphabetically gets synced to the device.

Corporate File Server Matrix

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

	Admin	Automatic	Manual
Available Repositories			
Box	✓	✓	✓
CMIS	✓	✓	✓
Google Drive	✓	–	–
Network Share	✓	✓	✓
OneDrive	✓	–	–
OneDrive for Business	✓	–	–
OneDrive for Business ADFS	✓	–	–
OneDrive for Business OAuth	✓	–	–
SharePoint	✓	✓	✓
SharePoint ADFS	✓	✓	✓
SharePoint O365	✓	✓	✓
SharePoint O365 ADFS	✓	✓	✓
SharePoint O365 OAuth	✓	–	–
SharePoint - Personal (My Sites)	✓	–	–
SharePoint WebDAV	✓	–	–
SharePoint Windows Auth	✓	✓	✓
WebDAV	✓	✓	✓

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

	Admin	Automatic	Manual
SharePoint O365	✓**	✓**	✓**
SharePoint O365 ADFS	✓**	✓**	✓**
SharePoint O365 OAuth	✓	–	–
SharePoint - Personal (My Sites)	✓**	–	–
SharePoint WebDAV	✓**	–	–
SharePoint Windows Auth	✓**	✓**	✓**
WebDAV	✓*	✓*	✓*

Legend:

¥ =The VMware Content Gateway on Linux servers supports only SMB v2.0 and SMB v3.0. The default supported version is SMB v2.0.

✓+ = Required

✓ = Supported

– = Not Supported

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

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

PIV-D Certificate Authentication Support

Workspace ONE Content app users are granted access to on-prem SharePoint repositories after the users are authenticated using the PIV-D Derived Credentials. Certificate-based authentication eliminates the requirement of user name and password.

On-prem repositories such as SharePoint can be configured to use the PIV-D Derived Credentials for authentication. Configuring the SharePoint repository to use the PIV-D Derived Credential requires Kerberos configuration in the VMware Content Gateway settings.

The following prerequisites must be considered for setting up the PIV-D Certificate Authentication:

- Kerberos Constrained Delegation (KCD) server must be set up with proper SPNs (Service Principal Names).
- Active Directory must be synced with Workspace ONE UEM, with User Principle Name (UPN) as an attribute.
- Service account must be available to both Workspace ONE UEM and VMware Content Gateway to use as part of the Kerberos authentication workflow.
- Content Gateway must be provided a trusted certificate from the Certificate Authority (CA) issuing the user certificates. These certificates might be only intermediate certificates or the entire certificate chain depending on validation requirements on the CA.

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.

Procedure

1 Navigate to **Content > Repositories > Admin Repositories** in the UEM console.

2 Select **Add**.

3 Configure the settings that appear.

Setting	Description
Name	Label the content directory.
Type	Select a Corporate File Server from the drop-down menu.
Link	Provide the full path to the directory location rather than the root domain. **Example:** http://SharePoint/Corporate/Documents A URL copied directly from a web browser might not have permission to access a server for certain repository types.
Organization Group	Assign Corporate File Server access to a selected group of users.
Use PIV-D Derived Credentials	This setting is available only when SharePoint is selected as the repository type. Select the check box to use the PIV-D certificate authentication to authenticate the users instead of user names and passwords. PIV-D certificate authentication is for authenticating the users who want to access the on-prem SharePoint repositories from their devices. **Note** Enabling use of a PIV-D Derived Credential requires Kerberos configuration in the Content Gateway settings. For information about the certificate authentication settings on Content Gateway, see the *Configure Content Gateway on the UEM Console* topic in the Content Gateway documentation.
Access via Content Gateway	Use the Content Gateway if the Workspace ONE UEM server's domain cannot access the Corporate File Server.
Content Gateway	Identify the unique name of the appropriate Content Gateway node from the drop-down menu.
Allow Inheritance	Permit child organization groups to inherit the same access permissions as their parent organization group.
Allow Write	Permit end users to create and upload files and folders, edit documents, and check in or check out files to external repositories on their devices.

Setting	Description
Allow Delete	Permits remote content delete for the Network Share repository. With this feature, the end user can delete their content permanently from the Network Share repository using the Workspace ONE Content app.
Authentication Type	Select the access level admins have to Corporate File Servers from the UEM console. ■ **None** – Prevent administrators from viewing and downloading Corporate File Server content from the UEM console. ■ **User** – Permit browsing of the repository file structure within the UEM console. Enter credentials into the **Username** and **Password** text boxes that appear. **Note** If the Use PIV-D Derived Credentials check box is selected, then the password text box does not appear. Provide the User Principal Name for the user in the Username text box.

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**.

Configure Link Using Best Practices

Ensure Content Gateway is configured with the correct link. 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.

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, the end users can access the Corporate File Server content from their devices. Using Content Gateway with Corporate File Servers allows the end users to securely add, edit, and upload content to the Corporate File Server.

The steps can vary when configuring an Automatic or Manual Template.

Procedure

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.

Setting	Description
Name	Label the content directory.
User Repository Name (auto template only)	Use look-up values to name the repository after the end user within the VMware Workspace ONE Content.
Type	Select a Corporate File Server from the drop-down menu.
Link	A URL copied directly from a web browser might not have permission to access a server for certain repository types.
Link (auto template only)	Use look-up values to create a repository when an end user accesses the VMware Workspace ONE Content. **Example:** https://sharepoint.acme.com/share/{EnrollmentUser}
Link (manual template only)	Provide the path to the directory location using * as a wildcard for a domain link. **Example:** http://*.sharepoint.com You can add a new link to an existing manual template but cannot edit or delete an existing link. Exercise caution when you add new links that are in the denylist, as you cannot edit or delete the links if there is any error. Any corrections to the links require deleting the entire template.
Denied Link(s)	Specify the values for the wildcard character (*) in the file paths. The values specified for * at the beginning and the end of the file path stops your users from creating manual repositories and sub folders using the manual template.
Organization Group	Assign Corporate File Server access to a specified group of users.
Use Derived Credentials	This setting is available only when SharePoint is selected as the repository type. Select the check box to use the PIV-D certificate authentication to authenticate the users instead of user names and passwords. PIV-D certificate authentication is for authenticating the users who want to access the on-prem SharePoint repositories from their devices. **Note** Enabling use of a PIV-D Derived Credential requires Kerberos configuration in the Content Gateway settings. For information about the certificate authentication settings on Content Gateway, see the *Configure Content Gateway on the UEM Console* topic in the Content Gateway documentation.

Setting	Description
Access via Content Gateway	Use the Content Gateway if the Workspace ONE UEM server's domain cannot access the Corporate File Server.
Allow Inheritance	Allow child organization groups to inherit the same access permissions as their parent organization group.
Allow Write	Allow end users to create and upload files and folders, edit documents, and check in or check out files to external repositories on their devices.

4 Complete the remaining Security, Assignment, and Deployment tabs and select **Save**.

5 If configuring a **Manual Template**, direct end users to the Self Service Portal where they can manually add and access their repository.

Note When repositories are set up, the first time a user navigates to the repository the user's sign-in credentials are used automatically to authenticate. If the sign-in credentials do not match the repository authentication or if the DEP or Web enrollment is used, then the user must manually sign in to the repository. In a DEP or Web enrollment, there are no known credentials to attempt authentication as credentials are never entered into a Workspace ONE application.

Configure Repository Details

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

Procedure

1 On the Security tab, complete the text boxes to control how the end users share and move sensitive documents outside of corporate mediums.

The Force Encryption setting has been removed since Workspace ONE UEM console version 9.5. The VMware Workspace ONE Content app encrypts all the files by default, whether the setting is available or not.

Setting	Description
Document Sharing	Disable the sharing settings for maximum security. You can enable them for configuring end-user collaboration.
Access Control	Set to **Allow Offline Viewing** to give end users the most viewing freedom for their document. Configure **Allow Online Viewing Only** to ensure that all devices accessing content are compliant, as Workspace ONE UEM cannot scan offline devices for compliance.
Allow Open in Email	Allow the content to open in emails. Users cannot open files that are larger than 10 MB. To allow users to open files larger than 10 MB, you must edit such files on the UEM console and enable this option. Files in user repositories cannot be edited.

Setting	Description
Allow Open in Third Party Apps	Give the permission to open this content in other applications. You can set a list of approved apps in the SDK Profile. Disabling this option also disables the end user's permission to print the PDF documents from the iOS VMware Workspace ONE Content.
Allow Saving to Other Repositories	Select to allow your end users to save this file to their Personal Content.
Enable Watermark	Select to add a watermark overlay to the file. Configure the Overlay Text for the watermark as part of an SDK profile.
Allow Printing	Give the end users the permission to print PDF documents from the iOS VMware Workspace ONE Content using AirPrint server. Once printed, content falls out of the control of the Workspace ONE UEM administrator. Printing is supported only if Allow Open in Third Party Apps is enabled.
Allow Edit	This setting only applies to write-enabled repositories.

2 Configure the **Assignment** settings to control which users have access to content.

This function ensures that only authorized employees have access to confidential or sensitive material and allows you to set up a tiered hierarchy of content access.

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

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

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

4 Select **Save**.

Cache Performance

When the entire corporate repository is cached, memory spikes can occur on the Device Services server due to the low internal memory. Each time, the cache must be disabled to overcome the load on the Device Services server.

Note The database script that is used to disable cache is no longer applicable from Workspace ONE UEM 1904 version. The cache can be disabled by switching the ContentCacheFeatureFlag to false in the API, `https://<host>/api/system/featureflag/<FeatureFlagName>/<OG_GUID>/false` .

The just-in-time caching strategy eliminates the low memory issue by caching only those folders and content records that are accessed by the user. The unwanted folders and contents are removed from the cache.

The folders are cached individually using a `folderId` cache key as opposed to caching the entire repository using the `RepoId` cache key.

In a cache miss, the Device Services server loads only the metadata of the current folders from the database and stores it in the cache. In a cache hit, the Device Services server reads only the root level folder structure from the cache.

Workspace ONE UEM Managed Content Repository

4

The UEM Managed Content repository refers to a location where administrators with the appropriate permissions have complete control over the files that are stored within it. Using the VMware Workspace ONE Content app, the end users can access the added content from the repository labeled UEM Managed but cannot edit the content.

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 UEM 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 UEM Managed Content Category Structure.

This chapter includes the following topics:

- Local File Storage for Workspace ONE UEM Managed Content

Configure the UEM Managed Content Category Structure

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

Procedure

1 Navigate to **Content > Categories** > **Add Category**.

2 Configure the settings that appear and **Save**.

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

3 As needed, add a subcategory to your category structure.

a Select **Add**  from the **Action Menu**.

b Configure the settings that appear and **Save**.

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

Upload Content to the UEM Managed Repository

Add files to the UEM 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 Workspace ONE Content app, delivering content to end users' devices. The end users, however, cannot edit the synced managed content.

Procedure

1 Navigate to **Content > List View**.

2 Select **Add Content** and choose **Select Files**.

3 Select an individual file for the upload from the dialog box.

4 Configure content **Info** settings.

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

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

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

Note Irrespective of the number of files added on the UEM console, the metadata for only the first 10k files that are sorted alphabetically are synced on the user's device.

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.

Procedure

1 Navigate to **Content** > **Batch Status**.

2 Select **Batch Import**.

3 Provide a **Batch Name** and a **Batch Description**.

4 To download a .csv template file, select the information icon ( ).

5 Fill out the CSV file with the file path and other information for content you want to upload.

6 Select **Choose File** and choose the .csv that you created.

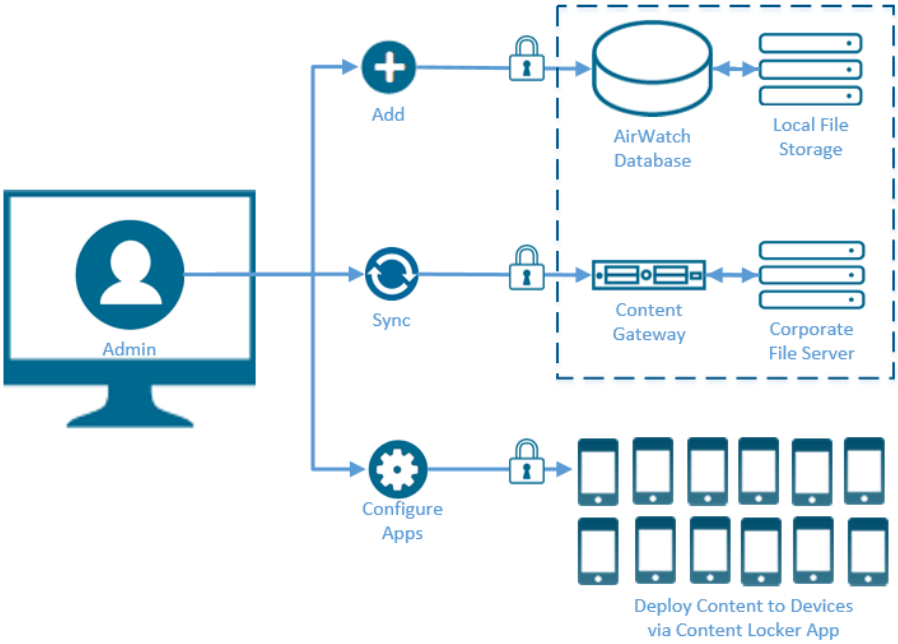
7 Select **Open** to select the .csv.

8 Select **Save** to upload your populated Batch File.

Local File Storage for Workspace ONE UEM Managed Content

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

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



File Storage for your Win32 Applications

Certain functionality in Workspace ONE UEM powered by AirWatch uses a dedicated file storage service to handle processing and downloads, which reduces the overall burden on the database and improves performance. Configuring file storage manually is only applicable to on-premises customers. It is configured automatically for SaaS customers.

It also includes certain 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.

Workspace ONE UEM Reports

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

Internal Applications

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

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

Workspace ONE UEM Managed Content

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

File Storage Requirements for your Win32 Applications

If you have a lot of managed content taking up space in the database, Workspace ONE UEM powered by AirWatch offers you dedicated file storage. To set up file storage, you must determine the location and storage capacity, configure network requirements, and create an impersonation account.

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 Workspace ONE UEM 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 supply the domain when configuring the service account in the format <domain\username>. Domain Trust can also be established to avoid an authentication failure.
- If the file storage and API are hosted outside the Console and Device Services servers then there must be connectivity between the file storage and API for writing/fetching values.

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 can vary depending on how you plan to use file storage. The file storage location must have enough space to accommodate the internal applications, managed content, or reports you intend to use. Take into the account the following considerations.

- If you enable caching for internal applications 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 must publish.
- For storing reports, your storage requirements depend on the number of devices, the daily number of reports, and the frequency with which you purge them. As a starting point, 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 in the domain of the shared storage directory.
- Give the local user read/write/modify permissions to the file share that is being used for the File Storage Path.
- Configure File Storage Impersonation User in Workspace ONE UEM with the domain account in the format <domain\username>.
- If the shared storage directory is not on a domain, create an identical local user and password on the server being used for File Storage, Console, and Device Services server. In this case, supply the local user account in the format <username>.

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 the file storage to store your managed content.

Procedure

1 At the Global organization group level, navigate to **Groups & Settings > All Settings > Installation > File Path** and scroll to the bottom of the page.

2 Select the **File Storage Enabled** slider and configure the settings.

When file storage is enabled, you can configure an external repository in which files are stored. A disabled setting means that files are stored as binary large objects in the database.

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

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

VMware Workspace ONE Content

5

The Content Management solution provides you the VMware Workspace ONE Content app to enable the end users to access the managed content. The Workspace ONE Content 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 Workspace ONE UEM 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 Workspace ONE Content v2.2 and later for iOS uses the NSFileProtectionComplete class to store the content.

This chapter includes the following topics:

Configure VMware Workspace ONE Content

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

Note VMware Workspace ONE has announced the End of General Support (EOGS) for Workspace ONE Content for Windows beginning July 31, 2020 and officially ending on July 31, 2021. For more information about the EOGS, see the knowledge base article, End of General Support for the AirWatch Content Locker for Windows.

Procedure

1 Navigate to **Groups & Settings > All Settings > Content > Applications > Workspace ONE Content app**.

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

Setting	Description
Application Profile	Set to define the security policies and settings used by this application. Leave as **Default** and configure the Recommended Default SDK settings to define app behavior using Workspace ONE UEM recommendations. Alternatively, select **Custom** application settings to override the default SDK settings and configure a unique set off behaviors for the app.
iOS Profile	Select a custom-created SDK profile from the drop-down list.
Android Profile	Select a custom-created SDK profile from the drop-down list.

3 Configure the **General** settings.

Setting	Description
Numbers of Days to Keep Content New	Select the number of days recently added documents will be labeled as new in the Workspace ONE Content.
Block Enrollment via Content, Boxer, and Web	Enable to prevent enrollment through Workspace ONE Content, VMware Workspace ONE Boxer, and VMware Workspace ONE Web. If Workspace ONE Content uses the VMware Workspace ONE SDK for iOS in Objective-C, then MDM enrollment is required for the single-sign on SDK setting to function correctly.
Change Repository Name for Managed Content	Enable to change the repository name in the **Root Repository Name** field that appears.
Root Repository Name	Enter the new repository name you want to use.
Allow Hyperlinks	Enable to allow end users to open hyperlinks located in documents in the **Open Internet Links with** field that appears.
Open Internet Links with	Select the application in which to open hyperlinks.

Setting	Description
Local Storage	Enable to provide a storage alternative for user content.
Upload on Wi-Fi Only	Enable to restrict uploads from Workspace ONE Content to Wi-Fi connections only.

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

5 Assign **Notifications** to Workspace ONE Content applications for the specified platform.

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

6 Select **Save**.

Configure Document Extensions

Document extensions enable end users to interact with the VMware Workspace ONE Content files on iOS devices 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 Workspace ONE Content v3.1 and later by completing the required configurations in the UEM console.

- Disable Authentication Type
- Disable Application Allowlisting
- Enable Allow Open In Third Party Apps

Disable Authentication Type

Applications with the authentication type enabled restrict the users from uploading files from Workspace ONE Content app using document extensions. To allow the user to upload files into the third-party applications, the authentication type must be disabled.

Procedure

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

2 Select **Disabled** from the Authentication Type drop-down menu.

3 Select **Save**.

Disable Application Allowlisting

Allowlisting of applications must be disabled to permit users to open documents from third-party apps into Workspace ONE Content.

Procedure

1 Navigate to **Apps > Settings and Policies > Security Policies**.

2 Set **Limit Documents to Open Only in Approved Apps** to **No**.

3 Select **Save**.

Enable Allow Open In Third Party Apps

Allow Open In Third Party Apps option must be enabled for the end users to use the export functionality within third-party apps.

Procedure

1 Navigate to **Content > Repositories > Admin Repositories**.

2 Select the **Edit** icon next to the Corporate File Server that syncs to end-user devices.

3 On the **Security** tab, select **Allow Open In Third Party Apps** and then **Save**.

Enable Storage Access

End users can access the files and storage from third-party applications only when the file and storage access is enabled for the Workspace ONE Content on Android devices.

To enable the storage access for Workspace ONE Content on Android, complete the required configurations on the console.

- Enable Allow Open In Third Party Apps
- Enable Storage Access from Third-Party Apps using Android SDK Default Settings
- Enable Storage Access from Third-Party Apps using Android SDK Custom Profile

Enable Storage Access from Third-Party Apps using Android SDK Default Settings

Add a configuration key in the default SDK profile to enable the content file and storage access from third-party applications.

For more information about limitations, see Limitation of Storage Access from Third-Party Apps (Android Only).

Procedure

1 Navigate to **Apps > Settings and Policies > Settings > Custom Settings**.

2 Select **Enable Custom Settings** and paste {"PolicyEnableFileProvider": "true"}.

3 Select **Save**.

Enable Storage Access from Third-Party Apps using Android SDK Custom Profile

Add a configuration key in the custom SDK profile to enable the content file and storage access from third-party applications.

For more information about limitations, see Limitation of Storage Access from Third-Party Apps (Android Only).

You can use a custom SDK profile for Workspace ONE Content.

Procedure

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**.

   a If you have multiple custom settings, append the PolicyEnableFileProvider key after your existing custom key within { }.

   { "CustomSetting Default": "true", "PolicyEnableFileProvider": "true" }

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

- 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 Workspace ONE Content authentication is enabled, you must have Workspace ONE Content unlocked to access it through a third-party app (displays message).

- If your admin has configured an app allowlist and the third-party app is not in the allowlist, then you cannot open or create files through Workspace ONE Content.
- 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 Workspace ONE Content.

VMware Workspace ONE Content Capabilities by Platform

The following matrix applies to the platform version of VMware Workspace ONE Content available in the app store.

Note VMware Workspace ONE has announced the End of General Support (EOGS) period for Workspace ONE Content for Windows beginning July 31, 2020 and officially ending on July 31, 2021. For more information about the EOGS, see the knowledge base article End of General Support for the AirWatch Content Locker for Windows.

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

Features	iOS	Android	Win 10
Wipe content at Maximum number of failed login attempts	✓	✓	✓
Prevent deleting mandatory content	✓	✓	✓
DLP			
Prevent Copy/Paste	✓	✓	✓
Enable/Disable Print	✓		
Enable/Disable Open in Third Party Application(s)	✓	✓	✓
Enable/Disable Sharing via Email	✓	✓	
Enable/Disable Document Level Encryption	✓	✓	✓
Enable/Disable Document Watermarking	✓*	✓*	
*The watermark feature is available for only admin repositories, user repositories, and Workspace ONE UEM managed content. It is not available for email attachments opened in Workspace ONE Content			
Enable/Disable Screen Capture		✓**	
** For Workspace ONE Content, 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 Workspace ONE Content home screen and folders. Screen Mirroring is also disabled.			
Data Collection			
Install Content	✓	✓	✓
Open/Close Content	✓	✓	✓
Uninstall/Delete Content	✓	✓	✓
Session Status	✓	✓	✓
Mobile Experience			
Access			
Keep Me Signed In	✓	✓	✓
Authenticate with back-end credentials (Active Directory)	✓	✓	✓
Integrate with Workspace ONE UEM Single-Sign-On	✓	✓	
Workspace ONE UEM Single-Sign-On with Hub as Broker App	✓	✓	
Allow Offline Access	✓	✓	✓
Standalone MCM	✓	✓	✓
Customize Terms of Use	✓	✓	✓

Features	iOS	Android	Win 10
Content Views			
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	✓		
File Management			
Sort Content (alphabetically, chronologically, importance)	✓	✓	✓
Filter Content (File Type, download status)	✓	✓	✓
Delete On-Demand documents	✓	✓	✓
Import and Upload new documents/new versions	✓	✓	✓
2-way sync for WebDav, network shares	✓	✓	
2- way sync for Google Drive, One Drive	✓	✓	
Check-In/Check-Out to SharePoint	✓	✓	
Add comments to files at SharePoint Check-in		✓	
User Generated Content- Capture Pictures or Video in VMware Workspace ONE Content	✓	✓	
Add, Copy, Multi-Select files or folders	✓	✓	✓
User Generated Content - Add Audio Files	✓		
User Generated Content - Add Office Files	✓	✓	
User Generated Content - Add Text Files	✓	✓	
Queue Multiple Document Downloads Simultaneously	✓	✓	✓
Manage Downloads (Pause/Resume/Cancel/Re-order)	✓		✓
Manage Uploads (Pause/Resume/Cancel/Re-order)	✓		
Usability			

Features	iOS	Android	Win 10
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)	✓	✓	✓
User Managed Content (Local Storage)			
File Management			
Add/Remove Files(s)	✓	✓	✓
Add new version	✓	✓	✓
Move File(s)/Folder(s)	✓	✓	✓
Add/Remove Folder(s)	✓	✓	✓
Removed files goes to Trash	✓	✓	✓
Automatically Upload document upon opening in VMware Workspace ONE Content	✓	✓	
Collaboration			
Add and Save PDF Annotations	✓	✓	✓
Edit and Save Office Documents (Word, Excel, PPT)	✓	✓	
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	✓		

Features	iOS	Android	Win 10
Notify User when update is available for document	✓	✓	✓
Customization and Integration			
External File Repository Integration			
Share Point 2007	✓	✓	✓
Share Point 2010	✓	✓	✓
Share Point 2013	✓	✓	✓
Share Point Online (Office 365)	✓	✓	✓
Network File Share	✓	✓	✓
WebDAV	✓	✓	
FileServer (HTTP)	✓	✓	
Google Drive	✓	✓	✓
OneDrive	✓	✓	✓
CMIS	✓	✓	
User Added Repository Support	✓	✓	✓
One Drive for Business	✓	✓	
Box	✓	✓	✓
External File Repository Folder Actions			
Allow sharing of Google Drive folders through email	✓		
Allow sharing of OneDrive folders through email	✓		
Allow marking a folder as favorite	✓		
Google Drive and OneDrive folders cannot be deleted as the delete permissions are not provided to these repositories			
Localization			
Arabic	✓	✓	✓
Chinese - Simplified	✓	✓	✓
Chinese - Traditional	✓	✓	✓
Czech	✓	✓	✓
Danish	✓	✓	✓
Dutch	✓	✓	✓

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

QR Code Scan to access Custom URLs (Android Only)

Use custom URLs to provide end users the direct access to the files in the Workspace ONE Content application. Upon scanning, the QR code, which contains the custom URLs allow the end user to search or view the file if the file is downloaded.

You must use either a search query or a specific content ID as the custom URL. The content IDs are automatically generated for every file that you upload to the Workspace ONE UEM console. When you point to the filename, the file path displays the Content IDs.

The custom URLs are:

- awscl://search/?query=text
- awscl://search?query=text
- awscl://search/?query="text"
- awscl://search?query="text"
- awscl://contentid={content ID}
- awscl://contentid="{content ID}"

The search query searches for the specified text string and the specific Content ID directly opens the specified document.

Matrix of Supported File Type by Platform

The file types supported by the Workspace ONE Content app on different platforms are listed in the matrix.

The matrix applies to the version of VMware Workspace ONE Content available in the app store.

Note VMware Workspace ONE has announced the End of General Support (EOGS) for Workspace ONE Content for Windows beginning July 31, 2020 and officially ending on July 31, 2021. For more information about the EOGS, see the knowledge base article End of General Support for the AirWatch Content Locker for Windows.

Supported File Types	iOS		Android		Windows 10		Notes
	Edit	View	Edit	View	Edit	View	
AD/Azure RMS	✓	✓	✓ Content app v3.5+	✓ Content app v3.5+			
AAC (audio/aac)		✓		✓			You cannot edit the audio and the video files. You can only add the files from the Content iOS and Android app.
ALAC (audio/m4a)		✓		✓			
WAV (audio/wav)		✓		✓			
MP3 (audio/mpeg)		✓		✓			
MOV (video/quicktime)		✓		✓			

Supported File Types	iOS		Android		Windows 10		Notes
MP4 (video/mp4)		✓		✓			Among the audio files, you can add only the .m4a files.
M4B, M4R,		✓					
M4V		✓		✓			
CSV (.csv)		✓		✓		✓	
ePub (.epub)		✓					
iBooks							
iWorks - Keynote (.key) application/vnd.apple.keynote		✓					
iWorks - Numbers (.numbers) application/vnd.apple.numbers		✓					
iWorks - Pages (.pages) application/vnd.apple.pages		✓					
MS Office - Excel (.xls/.xlsx) application/vnd.ms-excel	✓		✓	✓		✓	
XLSM		✓		✓			
MS Office - PowerPoint (.ppt/.pptx) application/vnd.ms-powerpoint	✓		✓	✓		✓	
PPTM		✓		✓			

Supported File Types	iOS		Android		Windows 10		Notes
MS Office - Word (.docx) application/ msword	✓	✓	✓	✓		✓	Editing is not supported for .doc files
DOCM		✓		✓			
MS Office - Password Protected (.docx, .pptx , .xlsx MS Office 2007 or later)	✓	✓	✓	✓			Editing is not supported for .doc files
MS Office - Documents with pivot tables		✓		✓		✓	
HTML (.html) text/ html		✓		✓		✓	HTML viewer does not support JavaScript
PDF (.pdf) application/ pdf	✓	✓	✓	✓	✓	✓	
Rich Text Format (.rtf) application/r tf		✓		✓			
Rich Text Format Directory (.rtfd) application/ octet-stream		✓		✓			
XML (.xml) application/ xml		✓		✓		✓	
PNG (.png) image/png		✓		✓		✓	You can add the images but cannot edit the files.
JPG (.jpg) image/jpeg		✓		✓		✓	
TIF (.tif, .tiff) image/tif		✓		✓		✓	

Supported File Types	iOS		Android		Windows 10	Notes
Bitmap (.bmp) image/bmp		✓		✓	✓	
GIF (.gif) image/gif		✓		✓	✓	
Zip (.zip) application/zip	✓	✓	✓	✓	✓	
Password Protected Zip	✓	✓	✓	✓	✓	
RAR (.rar) application/rar	✓	✓				
Password Protected RAR						
GZIP (.gzip) application/zip						
BZIP (.bzip) application/zip						
BZIP2 (.bzip2) application/zip						
TAR (.tar) application/zip						
TXT	✓	✓	✓	✓	✓	
MSG		✓				

Behavior Changes for Content on iOS using Swift SDK

Workspace ONE Content 5.0 for iOS is the first version of Content to use the Workspace ONE Swift SDK. Previous versions of Content used the Objective C version of the Workspace ONE SDK. With this architectural change comes few changes that might impact the Content app behavior that end users are accustomed to.

The following list describes the behavioral changes:

- Workspace ONE SDK does not support the logout function in standalone mode.

  Note Users must use the Intelligent Hub in registered mode on their devices. Users must not try logging in to the Content app in Standalone mode with devices that are not MDM managed or does not have Workspace ONE Intelligent Hub.

- Work offline option on the username/password screen is no longer supported. The user can work offline by navigating to App Settings and enabling Work Offline. Network calls can still be made, and offline work is honored by Content specific interactions only.
- SDK authentication screens are updated to a new user experience.
- If the SDK fails to fetch the Content settings after launch, the user is presented with a failure message.
- Experience update for user change without Check-in Check Out (CICO) during the forgot passcode scenario.

For more information about Content app behavioral changes, see https://ikb.vmware.com/s/article/78206

Workspace ONE Smartfolio

6

Smartfolio is a robust and a secure app that helps your organization manage and share the corporate content with ease. It provides a tailored content publishing and compliance experience for the common Line of Business use cases.

Currenly, Smartfolio is supported only on iOS devices.

Features

- Remotely manage, organize, and deliver critical files to the end users.
- Provide end users offline access to the documents.
- Prioritize the documents based on the relevance.
- Manage security on a per document level to meet the document-oriented regulatory requirements.
- Configure the documents for auto or manual download and collect read receipts as part of the organizational compliance policies.
- Use default SDK settings when configured as part of the Workspace ONE UEM app suite.

Note Workspace ONE Smartfolio app collects the data such as crash reports, log data, and other information required for various analytic purposes. This data helps VMware to improve the product functionality. For information about how VMware handles the collected data, see https://www.vmware.com/help/privacy.html.

This chapter includes the following topics:

Smartfolio and Content Comparison Matrix

The features supported by Smartfolio in comparison with the features supported by Workspace ONE Content are listed in the matrix. Use the matrix to help determine which application better suits your use case.

Table 6-1.

	Workspace ONE Content	**Workspace ONE Smart folio**
App Platform Support	Supports iOS, Android, and Windows 10	Supports only iOS
Repository support	Supports all repository types (OneDrive, SharePoint, NFS)	Supports only UEM Managed Content repository
File Management	Allows creating, viewing, and editing documents	Allows only viewing of documents Supports annotations only on PDF
App Size	Install size of approximately 200 MB	Lighter app with an install size less than 100 MB
Purpose of the app	Enhances the content aggregations and employee productivity workflows	Enhances the admin's content publishing experience
User Experience	Simple and easy to understand UI with more advanced functionalities. Allow users to create, view, edit, and perform many more actions on the documents.	Simple and easy to understand UI with basic functionality. Limits users to only view and annotate (PDF only) the documents.

Workspace ONE Smartfolio Deployment

Easily deploy Smartfolio as a managed application using the Workspace UEM Mobile Application Management functionality. Deploying the Smartfolio application to the end-user devices requires completing few steps on the Workspace ONE UEM console. After the deployment, end users can download the app on their enrolled devices.

The end users' devices that are enrolled through Workspace ONE Intelligent Hub are MDM Managed by default. These devices can also be enrolled without the MDM management by enabling the unmanaged mode for a smart group. Smartfolio app can be accessed on devices that are enrolled either in the managed mode or the unmanaged mode.

For more detailed information about deploying public applications, see the *Workspace ONE UEM Mobile Application Management* documentation.

For information about enabling the unmanaged mode for the devices, see the *Enable Unmanaged Enrollment for iOS Devices* in the *Workspace ONE Hub Services* documentation.

Add Smartfolio to Workspace ONE UEM console

To apply an SDK profile to the Smartfolio app, you must first add it as a public application to the Workspace ONE UEM console. The applied SDK profile gives additional features to the app.

Procedure

1 Navigate to **Apps & Books > Applications > Native > List View**.

2 Select **Public** and then select **Add Application**.

3 Configure the text boxes that display and select **Next**.

Setting	Description
Managed By	Select the organization group where the app is uploaded.
Platform	Select the appropriate platform. Currently only iOS devices are supported.
Source	Search for the application in the App Store either by using the app name or the URL.
Name	Enter Workspace ONE Smarfolio.

4 Locate and select Smartfolio app from the **Search** results page.

5 Review the information that automatically populates in the **Details** tab.

6 Assign **Terms of Use** which displays when the users first access the application from the App Catalog.

7 Select the **SDK** tab and then assign an SDK profile to the Smartfolio application.

8 Select **Save & Assign**.

What to do next

To assign and deploy the Smartfolio app, see Add Assignment to Smartfolio.

Add Assignment to Smartfolio

To deploy the Smartfolio app to your end users, you can add single assignment groups or multiple assignment groups.

Prerequisites

You must upload the Smartfolio as a public application to the Workspace ONE UEM console.

Procedure

1 Navigate to **Apps & books > Applications > Native > List View > Public**.

2 Select the **Assign** link under the Install Status column for the Smartfolio application. Alternatively, you can also select the edit icon and then select **Save & Assign**.

3 On the **Assignment** page, select **Add Assignment** and complete the options.

a In the **Distribution** tab, enter the following information.

Setting	Description
Name	Enter the assignment name.
Description	Enter the description for the assignment.
Assignment Groups	Enter the smart group name to which you want to assign the application. As you enter the smart group name, options are displayed and you can select the appropriate smart group from the list. If necessary, you can add more assignment groups.
App Delivery Method	■ **On Demand** – Deploys content to a catalog or other deployment agent. The device user can decide if and when to install the content. This option is the best choice for content that is not critical to the organization. Allowing users to download the content when they want helps conserve bandwidth and limits unnecessary traffic. ■ **Automatic** – Deploys content to a catalog or other deployment Hub on a device upon enrollment. After the device enrolls, the system prompts users to install the content on their devices. This option is the best choice for content that is critical to your organization and its mobile users.

b In the **Restrictions** tab, enter the following information.

Settings	Description
Remove on Unenroll	Set the application to be removed from a device when the device unenrolls from Workspace ONE UEM. Workspace ONE UEM enables this setting by default. If you enable this setting, supervised devices are restricted from silent app installation. This is because the device is locked and the provisioning profile installation is in the command queue which requires a device to be unlocked to complete the installation. If you disable this setting, provisioning profiles are not pushed with the installed application. That is, if the provisioning profile is updated, the new provisioning profile is not automatically deployed to devices. In such cases, a new version of the application with the new provisioning profile is required.
Prevent Application Backup	Disallow backing up the application data to iCloud. However, the application can still back up to iCloud.
Make App MDM Managed if User Installed	Assume management of applications previously installed by users on their devices, whether applications are supervised or unsupervised. Enable this feature so that users do not have to delete the application version installed on the device. Workspace ONE UEM manages the application without having to install the AirWatch Catalog version on the device.

c In the **Tunnel & Other Attributes** tab, enter the following information.

Settings	Description
Per App VPN Profile	Select a VPN profile that you want to use for the application. Users access the application using a VPN, which helps ensure that application access and use is trusted and secure.
Other Attributes	App attributes provide device-specific details for applications to use. For example, when you want to set a list of domains that are associated to a distinct organization.

d In the **Application Configuration** tab, enter the following information

Settings	Description
UPLOAD XML	You can upload an XML file that contains the key value pairs supported by the application for the app configuration.

4 Select **Create**.

5 Select **Add Assignment** to add more assignments for your publication.

6 Configure the flexible deployment settings by setting the priority for your app assignments.

Settings	Description
Priority	Select the value from the drop-down menu to set the precedence for the assignments. Devices receive applications from the assignment groups based on the priority set for the assignment groups. Adjusting the priority for a single assignment automatically reprioritizes other assignments.
Copy	From the more options menu, select copy to duplicate the selected assignment.
Delete	From the more options menu, select delete to remove the selected assignment.

For more detailed information about adding assignments, see *Add Assignments and Exclusions to Applications* in the *Workspace ONE UEM Mobile Application Management* documentation.

Content Assignment to Smartfolio

The UEM Managed repository is the location where you can store the files that you want to assign to the Smartfolio app on your end users' devices.

To store the files, you must first configure the category structure for the UEM Managed content on the Workspace ONE UEM console. Based on the configured structure, the files appear in an organized manner within the Smartfolio app.

Note A single category can have subcategories or files assigned. A category with subcategories cannot be assigned to the published content.

You can also prioritize the files based on the importance of the content and these files appear in the Smartfolio app as per the order of relevance.

For information about configuring the UEM Managed category structure and adding content, see Configure the UEM Managed Content Category Structure and Upload Content to the UEM Managed Repository.

Acknowledgment in Smartfolio

Smartfolio users can now acknowledge the documents that you assign to them as required content. On the Workspace ONE UEM console, you can view these acknowledgments in the Content List View and the Device Details pages.

On selecting View under the Installed Status column of the Content List View page, a pop-up box appears to show the exact number of users who have viewed and acknowledged the content.

The following list describes the supported document acknowledgment features:

- When the user opens a document, the Acknowledged button appears disabled and is enabled after a default delay of five seconds. The default value can be changed to be in the range of 0-600 seconds by applying the value `AcknowledgementTimeInterval` as a custom SDK Setting on the UEM console.
- The user is not prompted to acknowledge a document which has been already acknowledged.
- User is prompted to acknowledge a new version of the already acknowledged document if you mark the new version as Required.
- The Device Details page shows the acknowledged status and the date on which the document was acknowledged.
- Content Details by Device report contains the acknowledged status on a per device basis.

App Suite SDK Configurations 7

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

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

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

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

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

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

This chapter includes the following topics:

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.

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

Prerequisites

The recommendations provided apply to an app suite that includes:

- VMware Workspace ONE Web
- VMware Workspace ONE Content
- Enrolled devices
- Workspace ONE UEM or wrapped apps
- SDK settings

Procedure

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

2 Configure **Security Policies**.

Action	Description	Rec
Authentication Type		
Passcode	Prompt end users to authenticate with a user-generate passcode when the app first launches, and after an app session timeout. Enabling or disabling SSO determines the number of app sessions that get established. If a wipe is performed, that is, user has reached max number of passcode attempts, then the app will no longer flip to Hub. Instead it will kick off the standalone login flow.	–
Username and Password	Prompt end user to authenticate by re-entering their enrollment credentials when the app first launches, and after an app session timeout. Enabling or disabling SSO determines the number of app sessions that get established.	–
Disabled	Allow end user to open apps without entering credentials.	√
SSO		
Enabled	Establish a single app session across all Workspace ONE UEM and Workspace ONE UEM wrapped apps.	√
Disabled	Establish app sessions on a per app basis.	–
Offlibe Access		
Enabled	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 Maximum Period Allowed Offline to set limits on offline access.	√
Disabled	Remove access to Workspace ONE UEM and wrapped apps on offline devices.	–

Compromised Protection		
Enabled	Override MDM protection. App level Compromised Protection blocks compromised devices from enrolling, and enterprise wipes enrolled devices that report a compromised status.	√
Disabled	Rely solely on the MDM compliance engine for compromised device protection.	–
Data Loss Prevention		
Enabled	Access and configure settings intended to reduce data leaks.	√
	Enable Copy and Paste Into	
	Allows copying and pasting content from external applications into Workspace ONE UEM applications when set to **Yes**.	
	Enable Copy and Paste Out	
	Allows copying and pasting content from the Workspace ONE UEM applications into external applications when set to **Yes**. With Workspace ONE Swift SDK, restrictions are enforced on link generation and copying of logs which were not earlier impacted by clipboard restrictions. Copy and Paste action is independent of other DLP restrictions and does not adhere to allowlisting of apps. For example, if allowed, copy and paste action can take place on any external app and is not restricted to only the allowlisted apps.	
	Enable Printing	
	Allows an application to print from devices when set to **Yes**.	
	Enable Camera	
	Allows applications to access the device camera when set to **Yes**.	
	Enable Composing Email	
	Allows an application to use the native email client to send emails when set to **Yes**.	
	Enable Data Backup	
	Allows wrapped applications to sync data with a storage service like iCloud when set to **Yes**.	
	Enable Location Services	
	Allows wrapped applications to receive the latitude and longitude of the device when set to **Yes**.	
	Enable Bluetooth	
	Allows applications to access Bluetooth functionality on devices when set to **Yes**.	
	Enable Screenshot	
	Allows applications to access screenshot functionality on devices when set to **Yes**.	

	Enable Watermark	
	Displays text in a watermark in documents in the VMware Workspace ONE Content when set to Yes. Enter the text to display in the Overlay Text field or use lookup values. You cannot change the design of a watermark from the UEM console.	
	Limit Documents to Open Only in Approved Apps	
	Enter options to control the applications used to open resources on devices. (iOS only) You can use Workspace ONE UEM Configuration values to restrict users from importing files from third-party applications into Workspace ONE Content. For more information, see **Configure Import Restriction in Workspace ONE Content** section.	
	Allowed Applications List	
	Enter the applications that you allow to open documents.	
Disabled	Allow end user access to all device functions.	–

3 **Save**.

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

5 Configure **Settings**.

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

Analytics		
Enabled	Collect and view useful statistics about apps in the SDK suite.	√
Disabled	Do not collect useful statistics.	–
Custom Settings		
Enabled	Apply custom XML code to the app suite.	–
Disabled	Do not apply custom XML code to the app suite.	√

6 **Save**.

Import Restriction in Workspace ONE Content (iOS Only)

You can restrict or allow the import of content from third-party applications into the Workspace ONE Content by using certain configuration keys in UEM console. These configuration keys allow the content import from only the approved list of native applications.

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

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

The ContentImportRestriction and ContentImportAllowNativeApps configuration values can be used in combination to configure the import restriction as per your requirement. If you want to allow import of content from all native apps, enable the ContentImportAllowNativeApps key. The ContentImportAllowNativeApps key is enabled by default and allows import from all native apps such as iOS native Email, Files, Safari, AirDrop, and such. When enabled, the device users can open and import content from apps that are not in the allowlist into Workspace ONE Content using the web versions of the non-whitelisted applications (using Safari).

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

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

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

PDF Autosave in Workspace ONE Content (iOS Only)

From Workspace ONE Content v4.13.2, the device users can enable or disable the PDF Autosave functionality by using the Enable PDF Autosave setting in the Workspace ONE Content app.

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

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

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

Privacy Settings for Workspace ONE Content (iOS and Android Only)

Additional privacy disclosure and data collection practices can be performed by using certain configuration keys in the UEM console.

End users who are upgrading or are starting to use the latest version of Workspace ONE Content are presented with new privacy dialog screen upon the application launch.

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

- Data collected by the app – Provides a summary of data that is collected and processed by the application. Some of this data is visible to administrators of the Workspace ONE UEM administration console.

- Device Permissions – Provides a summary of device permissions requested for the app to enable product features and functionality, such as push notifications to the device.
- Company's privacy policy – By default, a message is displayed to the user to contact their employer for more information. You can configure the privacy policy URL in the UEM console. Once configured, the user can access the employer's privacy policy from the app.

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

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

Screen Timeout Restriction for Workspace ONE Content (iOS Only)

You can restrict the device users from disabling the screen timeout in Workspace ONE Content app by using certain configuration keys in the Workspace ONE UEM console.

Configuration Keys	Value Type	Supported Values	Description
{ "PolicyAllowScreenTimeoutToggle"}	Boolean	True (default) = Enabled False = Disabled	Set to True or False to control the timeout setting in Content app. If a value is not set, the default setting is applied and users can switch the timeout setting.When set to false, users are not allowed to toggle the timeout setting.

Auto Sync Control for Repositories (Android Only)

Add a configuration key in the default or the custom SDK profile to control the auto sync and authentication check for repositories that are not of managed content repository type.

Configuration Key	Value Type	Supported Values	Description
{ "AutoSyncEnabled"}	Boolean	TRUE (default) = Enabled FALSE = Disabled	When set to False, auto sync and authentication check for repository occurs only when the user navigates into the repository. When the default value is applied, sync and authentication check takes place when an automatic or manual sync is performed.

Workspace ONE Send Support for Content

By integrating Workspace ONE Send with Workspace ONE Content, you can restrict the files in Workspace ONE Content to open only through Workspace ONE Send. To force open the files through Send app, add a configuration key in the UEM console.

Use the following configuration key to restrict files to open through Workspace ONE Send.

Table 7-1.

Configuration Key	Value Type	Supported Values	Description
{ "PolicyAllowAIPFilesToOpenInOffice" }	Boolean	True = Enabled False = Disabled	When set to True, the files open through Workspace ONE Send.

Staged Content Support for Smartfolio

The content that is staged on the multi-user devices is cleared when the end user checks out the device. In such scenarios, on the next login, the user has to redownload the content. To make any managed content available on the end user's device, you must enable the staging mode for the content. On enabling the staging mode, the staged content is retained on the end user's device even after the end user checks in or checks out the device.

The content is available to a new user who checks out the device only if the user is assigned the content. If the content is not assigned to the new user, then the content is cleared.

To enable the staging mode for the content, add the following configuration key on the Workspace ONE UEM console.

Table 7-2.

Configuration Key	Value Type	Supported Values	Description
{ "RetainContentBetweenCheckoutSessions": true }	Boolean	True = Enabled False (default) = Disabled	When set to true, the downloaded content is retained and not cleared during the device check-in and checkout sessions. When set to false, the downloaded content is cleared and not retained during the device check-in and checkout sessions.

Default Tab Change Setting for Smartfolio

On logging in to the Smartfolio app, the end user first lands on the default Home tab. To help the user easily access necessary content without unnecessary navigation within the app, you can set the tab that is most accessed by the user as the default landing tab. You can change the default Home tab to the other available tabs by using a custom setting on the Workspace ONE UEM console.

To change the default tab from Home to the other available tabs, add the following configuration key in the UEM console.

Table 7-3.

Configuration Key	Value Type	Supported Values	Description
{DefaultBottomBarTab: 0}	Integer	Home - 0 All Files - 1 Recent - 2 Favorites - 3 Downloads - 4	The default tab for the Smartfolio app is set based on the chosen supported values.

Expected Behavior for SDK Authentication

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

Authentication Type	SSO	Sessions	Credentials	Expected Behavior
Disabled	Enabled	Single	Enrollment Credentials	Open apps without prompting end users to enter credentials.

Passcode	Enabled	Single	Passcode	Prompts at first launch of first app, establishing a single app session. The next authentication prompt occurs after the session times out.
Username and Password	Enabled	Single	Enrollment Credentials	Prompts at first launch of first app, establishing a single app session. The next authentication prompt occurs after the session times out.
Passcode	Disabled	Per App	Passcode	Prompts on a per app basis, establishing individual app sessions. Note that each app may have a unique passcode. The next authentication prompt occurs when launching a new app, or an individual app session times out.
Username and Password	Disabled	Per App	Enrollment Credentials	Prompts on a per app basis, establishing individual app sessions. The next authentication prompt occurs when launching a new app, or an individual app session times out.

Workspace ONE UEM Application Deployment

8

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 Workspace ONE Content application is available in the public app store, your organization needs to purchase licenses per device to take advantage of the Workspace ONE UEM MCM solution. Please see http://www.air-watch.com/pricing or contact Workspace ONE Support for more information.

This chapter includes the following topics:

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.

Procedure

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

Setting	Description
Managed By	View the organization group the application uploads in.
Platform	Choose the appropriate platform.

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

4 Review the information that automatically populates in the **Info** tab.

5 Add smart groups from the **Assignment** tab.

6 Use the **Deployment** tab to determine how your end users receive the app.

End users find and download recommended apps in the app store. To make finding and deploying it easier, you can recommend it through Workspace ONE UEM or automatically push it to your devices.

7 Assign **Terms of Use**, if desired.

8 **Save and Publish**.

Overview for Onboarding VMware Workspace ONE Content

Onboarding requires end users to review and acknowledge training materials and videos before gaining full access to VMware Workspace ONE Content 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 Workspace ONE Content until they view the required content, but they can still use their device.

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

User Experience

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

Also, consider the impact of deploying Workspace ONE Content in single app mode, as it restricts device functionality to a single app, in this case, Workspace ONE Content. 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 Workspace ONE Content

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

Procedure

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

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

5. Select **Save**.

Content Management using Workspace ONE Console

9

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 and Settings for Content Management.

This chapter includes the following topics:

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 UEM Managed and the 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.
Categories	Add categories and subcategories. Added categories are displayed on the screen in a list view with an action menu.
Featured Content	Manage the featured content you added from the List View or the Categories List View on this screen. Featured content is displayed prominently within the VMware Workspace ONE Content, providing easy access to high volume content. Use this screen to control the order in which featured content is displayed in the Workspace ONE Content using drag or deleting irrelevant content.
Batch Status	Perform a Batch Import and review the details of your uploaded batch from this screen.
Settings	Select to access content specific settings.

Mobile Content Management Dashboard

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

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

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

Content Management List View

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

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	UEM Managed	Corporate File Servers	Automatic Template	Manual Template	User-Added Repository	Category
Edit						
Manage file settings on an individual basis. Edited settings only affect the individual file, not the entire repository's settings.	✓	✓	✓	✓	✓	
Download a local copy of a previous file version.	✓					

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

Settings for Content Management

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

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

Setting	Description
Applications	Access the configuration screens for VMware Workspace ONE Content and VMware Content Locker Sync.
Content Gateway	Configure Content Gateway and download the installer. From Workspace ONE UEM console version 9.6 onwards, Unified Access Gateway (UAG) is the recommended installation type when configuring a Content Gateway node. You can use this option to configure a new Content Gateway on Unified Access Gateway or to migrate your existing Content Gateway to Unified Access Gateway. For more information about configuring Content Gateway on Unified Access Gateway, see Workspace ONE UEM Components on Unified Access Gateway in the UAG documentation. For information about migration, see Migrating Content Gateway to Unified Access Gateway documentation.
User Storage	Configure storage quota exceptions for individual users. These exceptions provide the most granular level of storage assignment, and override organization or user group configurations set in Personal Content.
Advanced	Configure file type restrictions, on-boarding and requiring content for on-boarding, and integrating with a third-party e-Signature vendor.