MobileIron Docs@Work 2.14.0 for iOS Guide

for MobileIron Core and MobileIron Cloud

August 10, 2020

For complete product documentation see:
MobileIron Docs@Work for iOS Product Documentation

Proprietary and Confidential | Do Not Distribute

Copyright © 2009 - 2020 MobileIron, Inc. All Rights Reserved.

Any reproduction or redistribution of part or all of these materials is strictly prohibited. Information in this publication is subject to change without notice. MobileIron, Inc. does not warrant the use of this publication. For some phone images, a third-party database and image library, Copyright © 2007-2009 Aeleeta's Art and Design Studio, is used. This database and image library cannot be distributed separate from the MobileIron product.

“MobileIron,” the MobileIron logos and other trade names, trademarks or service marks of MobileIron, Inc. appearing in this documentation are the property of MobileIron, Inc. This documentation contains additional trade names, trademarks and service marks of others, which are the property of their respective owners. We do not intend our use or display of other companies’ trade names, trademarks or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.

Contents

New features summary

This guide documents the following new features and enhancements:

- Docs@Work app features and enhancements
- Docs@Work administrator features and enhancements

Docs@Work app features and enhancements

- **Modern auth supports SharePoint Connector**: Modern auth now supports Microsoft SharePoint Online Connector on Docs@Work.

NOTE:

> - For certificate based authentication with Microsoft 365 SharePoint site, MobileIron recommends username AUTOFILL configuration.
> - The key-value pair **ENABLE_WEBVIEW_AUTHENTICATION** should be enabled to log in to webview.
> - SharePoint online sites will be logged out when the app is updated to Docs@Work 2.14 .0.
> - SharePoint Online with smart card authentication is not supported on Docs@Work 2.14 .0.

- **Rebranding**: MobileIron has updated the Docs@Work for iOS icon and user interface color scheme.
- **Enable split tunneling using MobileIron Tunnel**: A new option, **Enable Split Tunneling using MobileIron Tunnel**, is added for configuring Docs@Work. Use this option only if you have AppTunnel rules configured for Docs@Work. Before enabling the option, ensure that MobileIron Tunnel is deployed. Enabling the option allows the AppTunnel rules to be applied to MobileIron Tunnel along with AppTunnel.
  The workaround is available due to the planned deprecation of the UIWebView API by Apple.

  For **MobileIron Core** deployments, the option is available in the Docs@Work configuration on the Admin Portal.
  For **MobileIron Cloud** deployments, the option is available in the AppTunnel configuration for the app.

  The feature requires MobileIron Tunnel 4.1.0 for iOS and MobileIron Go 5.4.0 or Mobile@Work 12.3.0. MobileIron Core 10.7.0.0 or MobileIron Cloud 70 is required to configure the feature.

  For information about the UIWebView API deprecation, see UIWebView Deprecation and AppConnect Compatibility.

  For information about configuring split tunneling with MobileIron Tunnel, see "Configuring split tunneling with MobileIron Tunnel (Core)" or "Configuring split tunneling with MobileIron Tunnel (Cloud)" in the Split Tunneling using MobileIron Tunnel section.

Docs@Work administrator features and enhancements

- **New value added**: New value **password** added to **autofill_credentials** key-value pair. Autofill credentials configuration now supports password parameter for CIFS and WebDAV sites from MobileIron Core. When configured, the user is automatically logged into the site from the Sites screen. See the “Key-value pairs to configure app behavior” section for the description of the key-value pair.

Overview of Docs@Work for iOS

The Docs@Work app gives device users an intuitive and secure way to access, store, view, edit, and annotate documents from content repositories, such as Microsoft SharePoint, and cloud services such as Box and Dropbox. It allows administrators to configure content repositories, which are then automatically available to device users. It also lets administrators establish data loss prevention controls to protect documents from unauthorized distribution. Docs@Work supports AES-256-GCM for encrypting email attachments.

Device users must **have a valid user ID and password to access** content sites.

The Docs@Work consists of the following elements:

TABLE 1. DOCS@WORK ELEMENTS

Section	Description
Sites	The Docs@Work dashboard displays the content sites.
My Files	Save files to My Files for viewing and editing. Unlike other folders, documents in My Files are not connected to any content site and are not updated automatically.
Recents	View the most recently used files.
Starred	Files and folders marked as starred are available here.
Offline	Files marked as offline are available for offline viewing.

Docs@Work features

The device users can use the following Docs@Work features:

- Log in to content repositories and navigate through folders.
- Download documents from content repositories.
- View documents.
- Edit and annotate local files.
- Upload documents to content repositories.
- Download, view, and email encrypted attachments.
- Add content repositories to Docs@Work.

A MobileIron license is required for deploying Docs@Work. Docs@Work uses certain aspects of AppConnect, including passcode access and app tunneling. However, an AppConnect license is not required for Docs@Work.

Docs@Work for iOS is an AppConnect-enabled app. AppConnect is a MobileIron feature that containerizes apps to protect content on iOS and Android devices. Each AppConnect app becomes a secure container whose content is encrypted and protected from unauthorized access. Because each user has multiple business apps, each app container is also connected to other secure app containers. This connection allows the AppConnect apps to share content. AppConnect apps are managed using policies configured in MobileIron Unified Endpoint Management (UEM) platform. The UEM platform is either MobileIron Core or MobileIron Cloud.

As an AppConnect app, all Docs@Work content is secured. The app interacts with other apps according to the data loss prevention policies that you specify. The app has the following secure features:

- **Secure apps passcode**: A secure apps passcode, if you require one, protects access to all secure apps. This is the AppConnect passcode, which you define in MobileIron UEM. The AppConnect passcode provides an additional layer of security for secure apps, beyond the device passcode.
- **Data encryption**: AppConnect encrypts all AppConnect-related data on the device, such as Docs@Work app data, app configurations, and policies. This means app data is secure even if a device is compromised.
- **Data loss prevention**: You determine whether Docs@Work for iOS can use the iOS copy/paste , open-in features. AppConnect data loss prevention policies control if users can copy/paste data out of Docs@Work and control how email attachments can be shared with other apps via open-in.

For information about AppConnect features and configuration beyond Docs@Work for iOS, see the *AppConnect and AppTunnel Guide*.

Enable MobileIron Access for Docs@Work

In a MobileIron Core and MobileIron Access as a service deployment, federated traffic from Docs@Work through Access is only supported with MobileIron Tunnel. However, using Tunnel to CIFs services will fail.

Federated traffic through AppTunnel and Access as a service is not supported for Docs@Work. Selecting **Enable Access** option in the Docs@Work configuration has no impact.

For information about MobileIron Access and how to set up the service with MobileIron Core, see the *MobileIron Access Guide*.

NOTE: If Enable Split Tunneling using MobileIron Tunnel is selected, HTTPS authentication traffic, which would have previously used AppTunnel to Access, goesthrough Tunnel instead.

Where to find Docs@Work for iOS

You can download Docs@Work for iOS from the Apple App Store.

About Docs@Work for iOS configuration

Docs@Work for iOS is configured in MobileIron Unified Endpoint Management (UEM) platform. The UEM platform is either MobileIron Core or MobileIron Cloud.

Device users can download Docs@Work for iOS directly from the Apple AppStore. You can also distribute Docs@Work for iOS as a recommended app through Apps@Work.

Note The Following: Mobile@Work must be available on the device and registered with MobileIron Core, before installing the Docs@Work app.

- If you have an existing deployment of the Docs@Work functionality embedded in Mobile@Work for iOS devices or available through the AppConnect enabled apps required for iOS devices, you will still have to create new configurations for deploying the Docs@Work app.
- If you are using the Default AppConnect Global Policy, you may not need to create a new policy.
- Configuring an AppConnect container policy is required only if you did not **Authorize** for **Apps without an AppConnect container policy** in the AppConnect Global policy. Or, if you want to configure a different set of data loss prevention policies for Docs@Work.
- Standalone Sentry configured for AppTunnel is required if you want to tunnel traffic to content repositories. CIFS traffic must be tunneled through Standalone Sentry.
- Standalone Sentry configured for ActiveSync is required to open encrypted email attachments in Docs@Work.
- Use the Docs@Work configuration to specify:
  - AppTunnel rules
  - Content sites
  - Docs@Work app behavior

For more information on Configurations, Configuring Docs@Work for iOS

Configuring Docs@Work for iOS

The Docs@Work app enables iOS users to access, store, view, edit, and annotate documents from content repositories, such as Microsoft SharePoint. Administrators can set up Docs@Work so that:

- users see all available content repositories
- documents are protected from unauthorized distribution

Users can also configure access to content repositories.

The following describe how to set up Docs@Work for iOS.

Required components for Docs@Work for iOS deployment

The following components are required for Docs@Work for iOS deployment:

- MobileIron Unified Endpoint Management (UEM) platform: MobileIron Core or MobileIron Cloud.
- Sentry, with ActiveSync enabled (required if you want to secure access to the ActiveSync server using Sentry).
- An iOS device that is registered with a MobileIron UEM.
- MobileIron client: Mobile@Work for MobileIron Core deployments; MobileIron Go for MobileIron Cloud deployments.

For supported versions see the MobileIron *Docs@Work for iOS Release Notes*.

NOTE: If a device user has already launched Docs@Work for iOS as a standalone trial app, the device user must uninstall and reinstall Docs@Work for iOS to use it as a secure AppConnect-enabled app.

Main steps for configuring Docs@Work for iOS (Core)

Complete the following basic tasks to set up Docs@Work and distribute content sites:

Before you begin

- Decide which repositories you want to make available. All repositories you configure for Docs@Work are visible to all users. You can provide select users with instructions for accessing restricted repositories.
- Decide whether you want to make each repository a published site. Content on published sites is automatically downloaded and mirrored on devices.
- Collect the following information for each repository:
  - URL for the site
  - type of repository (SharePoint, WebDAV)
  - subtype of repository (Office 365, NetworkDrive, and so on.)

Set up app distribution

- Distributing as a recommended app on page 5

Set up Docs@Work

- Enabling Docs@Work
- Configuring the AppConnect global policy on page 31
- Configuring an AppConnect container policy on page 9
- Configuring content sites in the Docs@Work configuration on page 10

AppTunnel setup

Complete the following additional tasks to set up app tunneling to content repositories.

- Configuring an AppTunnel service

Attachment control setup

Complete the following tasks to set up attachment control

- Configuring attachment control on page 23
- Configuring 256-bit encryption on page 33

Docs@Work app behavior setup

- Additional configurations using key-value pairs

Distributing as a recommended app

Device users can download Docs@Work for iOS directly from the Apple AppStore. You can also distribute Docs@Work for iOS as a recommended app through Apps@Work.

Procedure

1. In the Admin Portal, go to **Apps > App Catalog**.
2. Click **Add+**.
3. Click **iTunes** to import Docs@Work for iOS from the Apple App Store.
4. Enter **MobileIron Docs@Work** in the Application Name text box.
5. Click **Search**.
6. Select the app from the list that is displayed.
7. Click **Next**.
8. (Optional) Select one or more categories if you want to display this app in a specific group of apps on the device. Click **Add New Category** to define new categories.
9. Click **Next**.
10. Use the following guidelines to make the appropriate selections for **App@Work Catalog**:

Item	Description
This is a Free App	Select for free recommended apps. iOS allows Managed App features to be applied to free apps and apps purchased with VPP credits, but not to apps paid for by the user. Specifying whether the app is free ensures successful download of apps that otherwise require user payment.
Hide this App from the Apps@Work catalog	Select to prevent this app from being displayed in Apps@Work. For example, you might want to hide apps that will be installed upon registration anyway. Hiding a mandatory app reduces clutter in Apps@Work, leaving device users with a concise menu of the approved apps they might find useful.
Allow conversion of apps from unmanaged to managed in Apps@Work (iOS 9 or later).	Select if you want to allow the app to be converted from an unmanaged app to a managed app in Apps@Work on devices running iOS 9 through the most recently released version as supported by MobileIron. The unmanaged app will not require uninstallation, as it will be converted directly to a managed app.
Feature this App in the Apps@Work Catalog	Select this option if you want to highlight this app in the Featured apps list. NOTE: The Message feature for iOS apps applies only to featured apps. For more information, see "Informing users of new apps and upgrades for featured apps" in the Apps@Work Guide.

11. Click **Next**.
12. Use the following guidelines to complete the screen:

Item	Description
Per App VPN Settings	
Per App VPN by Label Only	Select the VPN setting you created for per app VPN in the right (all) column, and click the right arrow to move it to the left (selected) column. If the app will use MobileIron Tunnel, select the MobileIron Tunnel VPN setting you created. You can select multiple per app VPN settings. To reorder the per app VPN configurations in the Selected column, use the up and down arrows to sort the names in the list. This feature applies to iOS 7 through the most recently released version as supported by MobileIron. See Managing VPN settings in the *MobileIron Core Device Management Guide* for information on creating a per app VPN or MobileIron Tunnel VPN setting. See “Setting per app VPN priority” in the Apps@Work Guide.
Managed App Settings	
Prevent backup of the app data	Select to ensure that iTunes will not attempt to back up possibly sensitive data associated with the given app.
Remove app when device is quarantined or signed out	Select to enable configured compliance actions to remove the app if a policy violation results in a quarantined device or the device signs out in multi-user mode. To enable this feature, you must also configure a corresponding compliance action, and security policy with that compliance action selected. Once the device is no longer quarantined, the app can be downloaded again. NOTE: If you change the setting after the app is added, the changed setting will not be applied to the app.
Send installation request or send convert unmanaged to managed app request (iOS 9 and later) on device registration or sign-in.	Select this option so that after device registration is complete, or after a user signs in on a multi-user device: • The device user is prompted to install this app. • The app is converted to a managed app, if the app is already installed as an unmanaged app. To allow conversion to a managed app, also select the option **Allow conversion of apps from unmanaged to managed in Apps@Work (iOS 9 or later).** This setting is not selected by default.

Item	Description
Send installation or convert unmanaged to managed app request to quarantined devices	Select this option to enable the following on quarantined devices: • Prompt the device user to install the app. • Convert the app to a managed app, if the app is already installed as an unmanaged app. NOTE: These settings are applied even if a compliance action blocks new app downloads for a quarantined device.
Advanced Settings	
Remove app when MDM profile is removed	Select this option to remove this app from the device when the MDM profile is removed from the device.

13. Associate the app with a label to have that app listed on iOS devices.
    a. Go to **Apps > App Catalog**.
    b. Select **iOS** from the **Platform** list.
    c. Select the app you want to work with.
    d. Click **Actions > Apply to Label**.
    e. Select the label that represents the iOS devices for which you want the selected app to be displayed.
    f. Click **Apply**.
14. Make sure that the Apps@Work web clip is also applied to the same labels, so that iOS devices can access your enterprise storefront.
    a. Select **Policies & Configs > Configurations**.
    b. Select the **System - iOS Enterprise AppStore** setting.
    c. Select **More Actions > Apply to Label**.
    d. Select the iOS label and click **Apply**.

Enabling Docs@Work

A Docs@Work license is required on MobileIron Core to enable support. Enabling this setting indicates that you have the required license to deploy Docs@Work. Enabling Docs@Work is also required for AES-256-GCM encryption for email attachments.

Procedure

1. In the Admin Portal, go to **Settings > System Settings**.
2. In the left menu bar, click **Additional Products > Licensed Products**.
3. Select **Docs@Work**.
4. Select Enable merging of configurations option to enable merging multiple configurations for a device.

NOTE: The Enable merging of configurations option is disabled by default.

5. Click **Save**.

Configuring an AppConnect container policy

This task is only required:

- If you did not select **Authorize** for **Apps without an AppConnect container policy**, in the AppConnect Global Policy.
- If you want to configure a different set of data loss prevention policies for Docs@Work.

The AppConnect container policy authorizes an AppConnect app and specifies the data loss prevention settings. The container policy overrides the corresponding settings in the AppConnect Global Policy. Separate AppConnect container policies are required for each operating system (Android or iOS).

NOTE: Ensure that only one Docs@Work AppConnect container policy is applied to a device.

Procedure

1. In the Admin Portal, go to **Policy & Configs > Configurations**.
2. Click **Add New > AppConnect > Container Policy**.
3. Enter a name for the policy. For example, enter Docs@Work container policy for iOS.
4. Enter a description for the policy.
5. In the **Application** field, select **Docs@Work**.
   Select Docs@Work only if the app is available in the app catalog as a recommended app. If not, you must enter the app bundle ID.
6. Select the data loss prevention settings.

Item	Description
Exempt from AppConnect passcode policy	iOS only Select this option if you want to allow the device user to use Docs@Work without entering the AppConnect passcode or Touch ID. NOTE: When you select this option, situations still occur when the device user must enter the AppConnect passcode or Touch ID. For example, when the user first launches Docs@Work, the user is prompted to authenticate.
iOS Data Loss Prevention	
Allow Print	This setting allows an AppConnect app to use print capabilities if the app supports them. However, Docs@Work does not allow users to print documents from within Docs@Work, even if you select this option.
Allow Copy/Paste To	Select **Allow Copy/Paste To** if you want the device user to be able to copy content from Docs@Work to other apps. When you select this option, then select either: • **All apps** Select **All apps** if you want the device user to be able to copy content from

Item	Description
	Docs@Work and paste it into any other app. • **AppConnect apps** Select **AppConnect apps** if you want the device user to be able to copy content from Docs@Work and paste it only into other AppConnect apps.
Allow Open In	Select **Allow Open In** if you want Docs@Work to be allowed to use the Open In (document interaction) feature. Select one of these options: • **All apps** Select **All apps** if you want Docs@Work to be able to send documents to any other app. • **AppConnect apps** Select **AppConnect apps** to allow Docs@Work to send documents to only other AppConnect apps. • **Whitelist** Select **Whitelist** if you want Docs@Work to be able to send documents only to the apps that you specify. Enter the bundle ID of each app, one per line, or in a semi-colon delimited list. For example: com.myAppCo.myApp1 com.myAppCo.myApp2;com.myAppCo.myApp3 The bundle IDs that you enter are case sensitive.

7. Select **Save**.
8. Select the Docs@Work container policy.
9. Click **More Actions > Apply To Label**.
10. Select the appropriate labels to which you want to apply this policy.
11. Click **Apply**.

Related topics

For more information on configuring the AppConnect Container Policy, see the “Configuring AppConnect container policies” section in the *AppConnect and AppTunnel Guide*.

Configuring content sites in the Docs@Work configuration

Content sites configured in the Doc@Work configuration are automatically added to the Docs@Work app. Device user action is not required. These sites are called Group sites. SharePoint (including OneDrive for Business), WebDAV, CIFS, and DFS sites are configured in the **Content Sites** section of the Docs@Work configuration. Box, SharePoint sites that use Federated authentication, and Google Drive sites are configured in the **Custom Configurations** section using key-value pairs.

- Adding SharePoint, WebDAV, CIFS, and DFS sites on page 11
- Support for variables in configuring content sites on page 11
- Verifying the SharePoint URL on page 12

- Adding Box enterprise as a Group site on page 13
- Adding a SharePoint Group site with Federated authentication on page 13
- Adding a SharePoint Group site with derived credentials on page 14
- Configuring DFS content site on page 15

Adding SharePoint, WebDAV, CIFS, and DFS sites

Content sites configured in the Doc@Work configuration are automatically added to the Docs@Work app. Device user action is not required. SharePoint (including OneDrive for Business), WebDAV, CIFS, and DFS sites are configured in the **Content Sites** section of the Docs@Work configuration.

Procedure

1. In the Admin Portal, go to **Policies & Configs > Configurations**.
2. Select **Add New > Docs@Work**.
3. Use the following guidelines to create or edit a Docs@Work setting and add content sites:
4. Click **Save**.
5. Select the Docs@Work configuration.
6. Click **More Actions > Apply To Label**.
7. Select the appropriate labels to which you want to apply the configuration.
8. Click **Apply**.

NOTE: Docs@Work is a document centric application. It relies on an API (in native mode) to query directories and files. If the entity being queried is not a folder or file, the APIs fail. As a result, List support is limited to DocumentLibrary. No other type of List is supported.

Support for variables in configuring content sites

Variables allow you to configure content server access that is specific to the user or group. For example, in Active Directory, you can specify a user’s home directory on a network drive as an attribute. If you include the variable in the URL for the content site, the user's view of the network drive will be their home folder.

Prerequisites for using variables for configuring content sites

- Requires LDAP or AD integration.

Supported Content sites for variables

- SharePoint (including Office 365)
- Network Drives
- Cloud Storage

Variables for Box and Dropbox are not supported.

Supported variables for configuring content sites

$EMAIL$
$USERID$
$FIRST_NAME$

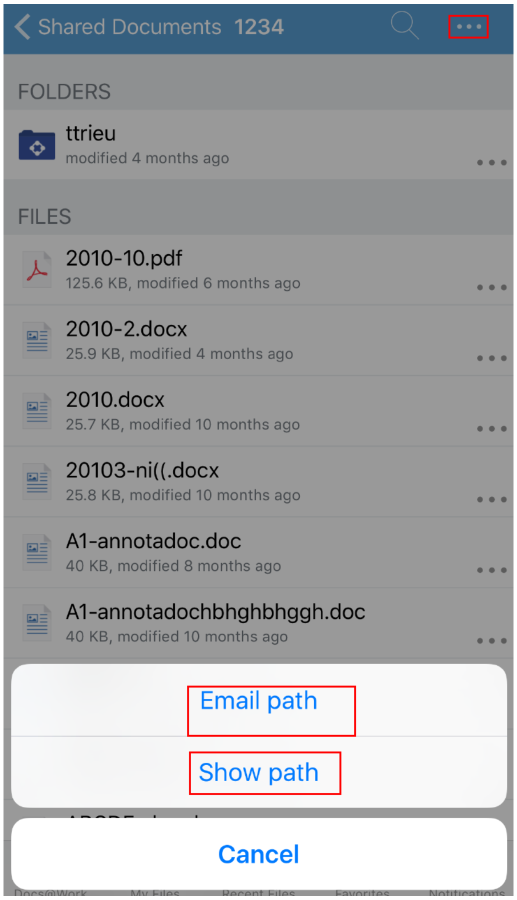
$LAST_NAME$
$USER_UPN$
$DISPLAY_NAME$
$USER_CUSTOM1$
$USER_CUSTOM2$
$USER_CUSTOM3$
$USER_CUSTOM4$

Verifying the SharePoint URL

You can view the SharePoint or WebDAV URL in Docs@Work that you should use when configuring a SharePoint or WebDAV site. This allows you to verify and enter the correct URL in the Docs@Work configuration in MobileIron Core to configure SharePoint and WebDAV group sites.

Procedure

1. Add the SharePoint or WebDAV site as a User site in Docs@Work.
2. In Sites, tap on the SharePoint or WebDAV site.
3. Navigate to the folder you want to configure as a Group site.
4. Tap, hold, and then release the **...** menu.
   The menu items will display.



FOLDERS

ttrieu
modified 4 months ago

FILES

2010-10.pdf
125.6 KB, modified 6 months ago

2010-2.docx
25.9 KB, modified 4 months ago

2010.docx
25.7 KB, modified 10 months ago

20103-ni((.docx
25.8 KB, modified 10 months ago

A1-annotadoc.doc
40 KB, modified 8 months ago

A1-annotadochbhghbhggh.doc
40 KB, modified 10 months ago

5. Select one of the menu items to either view the URL or email the URL.

Item	Description
Email path	A draft email message with the site URL displays. Enter an email address to email the URL path.
Show path	The URL path for the content site displays.

Adding Box enterprise as a Group site

You add a key-value pair in the **Custom Configurations** section to configure Box as a Group site. Group sites are automatically pushed to the Docs@Work app.

Procedure

1. In the Core Admin Portal, go to **Policies & Configs > Configurations > Add New > Docs@Work > Docs@Work**.
2. Scroll down to the **Custom Configurations** section.
3. Add the SITE_DETAILS_N key-value pair. For more information, see "Key-value pairs to configure app behavior" section.
4. Click **Save**.

Device users can also add a Box User site.

NOTE: iOS devices support one Group site and multiple user sites.

Adding a SharePoint Group site with Federated authentication

You add a key-value pair in the **Custom Configurations** section to configure a SharePoint site that uses Federated authentication as a Group site. Group sites are automatically pushed to the Docs@Work app. If authentication to the SharePoint server is done using Active Directory Federation Services (ADFS), the users must enter their enterprise AD or LDAP credentials to authenticate to the server.

Procedure

1. In the MobileIron Core Admin Portal, go to **Policies & Configs > Configurations > Add New > Docs@Work > Docs@Work**.
2. Scroll down to the **Custom Configurations** section.
3. Add the SITE_DETAILS_N key-value pair. For more information, see "Key-value pairs to configure app behavior" section.
4. Click **Save**.

Adding a SharePoint Group site with derived credentials

Derived credentials with Entrust PIV-D certificates and p12 certificates are supported for SharePoint sites with ADFS. See the *MobileIron Derived Credentials with Entrust Guide* for information about how to set up derived credentials with Docs@Work.

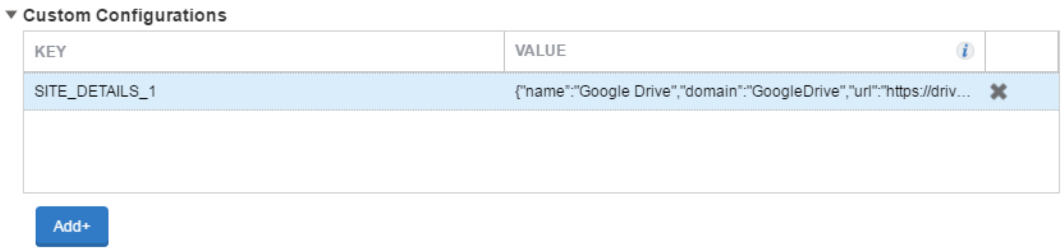
Adding Google Drive as a Group site

You add a key-value pair in the **Custom Configurations** section to configure Google Drive as a Group site. Group sites are automatically pushed to the Docs@Work app.

NOTE: Variables are not supported in the URL for configuring the Google Drive site. For example, you will not be able to specify a user name as part of the JSON value. However, you can configure fAUTOFILL_CREDENTIALS key-value pair to autofill the username for Google Drive.

Procedure

1. In the MobileIron Core Admin Portal, go to **Policies & Configs > Configurations**.
2. Select the Docs@Work configuration to which you want to add Google Drive.
3. Click **Edit**.



▾ Custom Configurations

KEY	VALUE
SITE_DETAILS_1	{"name":"Google Drive","domain":"GoogleDrive","url":"https://driv...

4. Scroll down to the **Custom Configuration** section.
5. Click **Add+** to enter the following key value pair:

Key	Value
SITE_DETAILS_N Where *n* is a number 1-100 Example: SITE_DETAILS_1	Enter parameters for the content site in the following JSON format: {"name":"*name for the site*","domain":"GoogleDrive","url":"https://drive.google.com”} NOTE: • Values are case sensitive. **Description** *name for the site*: Enter a name for the site. Example: Google Drive.

6. Click **Save**.

Authentication with an identity provider (IdP)

If your Google Drive setup uses an identity provider (IdP) for authentication, device users are directed to the IdP without having to go through any intermediate screens.

If Google Drive is set up through the Docs@Work configuration in MobileIron Core, you must also configure the AUTOFILL_CREDENTIALS key-value pair to enable this feature.

Configuring DFS content site

Distributed File System (DFS) allows administrators access to group shared folders located on different servers by transparently connecting them to one or more DFS namespaces. DFS uses CIFS protocol.

Requirements

- Standalone Sentry 8.0.1 through the most recently released version as supported by MobileIron.
- Standalone Sentry 8.5.0 through the most recently released version as supported by MobileIron is required for create, upload, and delete (CUD) operations for files and folders.
- MobileIron Core 9.0.0.0 through the most recently released version as supported by MobileIron.

Before you begin

- Ensure that you have Standalone Sentry set up for AppTunnel.
  DFS traffic must be tunneled through Standalone Sentry.

NOTE: Context headers, server-side proxy, and ATC are not supported for tunneling to DFS servers.

- Ensure that the necessary SCEP or Certificate setting is created. You will reference the SCEP or Certificate setting when you create the AppTunnel rule in the Docs@Work configuration.

Configuration tasks summary

The following configuration tasks are required. These tasks are done in the MobileIron Core Admin Portal.

1. Enable DFS in Standalone Sentry settings.
   See Enabling DFS on page 15.
2. Configure an AppTunnel service for a CIFS repository in Standalone Sentry settings.
   See Configuring an AppTunnel service for DFS on page 15.
3. Configure AppTunnel rules and DFS content site in Docs@Work configuration.
   See Configuring AppTunnel rules and DFS site in the Docs@Work setting on page 16.

Enabling DFS

1. In the Admin Portal, go to **Services > Sentry**.
2. Edit the entry for the Standalone Sentry that supports AppTunnel.
3. In the **App Tunneling Configuration** section, select the check box for **Enable DFS**.

Configuring an AppTunnel service for DFS

1. In the Admin Portal, go to **Services > Sentry**.
2. Edit the entry for the Standalone Sentry that supports AppTunnel.
3. In the **App Tunneling Configuration** section, under **Services**, click **+** to add a new service.

4. Use the following guidelines to configure a tunnel service:

Item	Description
Service Name	The Service Name is used in the Docs@Work configuration for setting up tunneling to the content repository. Enter one of the following: • A unique name for the service that Docs@Work accesses. One or more of your internal app servers provide the service. You list the servers in the Server List field. - The service name must begin with CIFS_. - A service name cannot contain these characters: 'space' \ ; * ? < > " |. • <CIFS_ANY> Select <CIFS_ANY> to allow tunneling to any URL for a CIFS-based or DFS content server. Typically, you select <CIFS_ANY> if the URL for a CIFS-based or DFS content server contains wildcards for tunneling, such as *.myCompany.com. Note The Following: • The order of the Service Name entries does not matter. • Do not select <ANY>, <TCP_ANY>, <IP_ANY>, or <IP_ANY_WP8.1> for tunneling to DFS.
Server Auth	Select Pass Through The Sentry passes through the authentication credentials, such as the user ID and password (basic authentication) or NTLM, to DFS.
Server List	NOTE: The Server List field is not applicable when the service name is <CIFS_ ANY>. Enter the DFS server's host name or IP address (usually an internal host name or IP address). Include the port number on the DFS server that Standalone Sentry can access. Example: fs1.companyname.com:445 You can enter multiple servers. Depending on the Global Configuration settings for the Sentry, either round-robin or priority distribution is used to load balance the servers. Separate each server name with a semicolon. Example: fs1.companyname.com:445;fs2.companyname.com:445
TLS Enabled	Not applicable for app tunnel to DFS.
Proxy/ATC	Not applicable for app tunnel to DFS.
Server SPN List	Not applicable for app tunnel to DFS.

5. Click **Save**.

Configuring AppTunnel rules and DFS site in the Docs@Work setting

1. In the Admin Portal, go to **Policies & Configs > Configurations**.
2. Select the Docs@Work configuration and click **Edit**.
3. In the **AppTunnel Rules** section, use the following guidelines to add an AppTunnel rule for CIFS repository:

Item	Description
AppTunnel Rules Configure AppTunnel rules settings for Docs@Work. When Docs@Work tries to connect to the URL configured here, Standalone Sentry creates a tunnel to the content server. To add an AppTunnel entry, click + . To delete an AppTunnel entry, click - .	
Sentry	Select the Standalone Sentry on which you configured the AppTunnel service. The drop-down list contains all Standalone Sentrys that are configured to support AppTunnel.
Service	Select an AppTunnel Service Name from the drop-down list. This service name specifies an AppTunnel service configured in the App Tunneling Configuration section of the specified Sentry.
URL Wildcard	Enter one of the following: • A content server's hostname Example: cifs-windows.yourcompany.com • A hostname with wildcards, if the Service Name is <CIFS_ANY>. The wildcard character is *. Example: *.yourcompanyname.com If you want finer granularity regarding what requests Standalone Sentry tunnels, configure multiple AppTunnel rows. The Sentry and Service fields that you specify in this AppTunnel row determine the target content server. Note The Following: A hostname with wildcards works only with the service <CIFS_ANY>. Unlike services with specific service names, these services do not have associated app servers. The Standalone Sentry tunnels the data to the URL specified in the app. MobileIron recommends that you carefully consider how you use wildcards. For example, do not use just * for the URL. **The order of these AppTunnel rows matters**. If you specify more than one AppTunnel row, the first row that matches the hostname requested is chosen. That row determines the Standalone Sentry and Service to use for tunneling. Do not include a URI scheme, such as http:// or https:/, in this field.
Port	Enter the port number that Docs@Work can request. Typically, the port number is 445.
Identity Certificate	Select the Certificate or the SCEP profile that you created for devices to present to the Standalone Sentry that supports app tunneling.

4. In the **Content Sites** section, enter the following information:

Item	Description
Name	Enter a name for the content site. This name will be displayed on the device.
URL	Enter a valid URL for the DFS. Both domain name and IP address are supported. A valid URL must start with http:// or https://. Format example: https://*resolvablehostname*:445/URL Variables: You can enter a valid URL with variables for the content site. Variables in the protocol or the hostname are not supported. See also, Support for variables in configuring content sites on page 11. Examples with variables: \\$USER_CUSTOM1$ Format of DFS URL with UserId: https://*resolvablehostname*:445/users/$USERID$ Note The Following: LDAP or AD integration is required for using variables. If the Site URL is invalid, it will not be distributed to users.
Domain	Select CIFS from the drop-down list.
Subdomain	Select NetworkDrive from the drop-down list.
Authentication	Select if the device has to authenticate to the server. NOTE: Only basic authentication is supported.
Published Site	Select to designate the site as a Published site.

5. Click **Save**.
6. Select the Docs@Work configuration.
7. Click **More Actions > Apply To Label**.
8. Select the appropriate labels to which you want to apply the configuration.
9. Click **Apply**.

Configuring an AppTunnel service

You create an AppTunnel service in Standalone Sentry as part of the AppTunnel setup required to tunnel traffic to content repositories. CIFS traffic must be tunneled through Standalone Sentry.

Before you begin

Ensure that you have a Standalone Sentry that is set up for AppTunnel and the necessary device authentication is also configured. See “Configuring Standalone Sentry for app tunneling” in the MobileIron Sentry Guide.

Procedure

1. In the Admin Portal, go to **Services > Sentry**.
2. Edit the entry for the Standalone Sentry that supports AppTunnel.
3. In the **App Tunneling Configuration** section, under **Services**, click **+** to add a new service.
4. Use the following guidelines to configure a tunnel service:

Item	Description
Service Name	The Service Name is used in the Docs@Work configuration for setting up tunneling to the content repository. Enter one of the following:
	• A unique name for the service that the AppConnect app on the device accesses. One or more of your internal app servers provide the service. You list the servers in the Server List field. For example, some possible service names are: - SharePoint - Human Resources A service name cannot contain these characters: 'space' \ ; * ? < > " |. Special prefixes: - For app tunnels that point to CIFS-based content servers, the service name must begin with CIFS_.
	• <ANY> Select <ANY> to allow tunneling to any URL that the app requests. Typically, you select <ANY> if an AppConnect app’s app configuration specifies a URL with wildcards for tunneling, such as *.myCompany.com. The Sentry tunnels the data for any URL request that the app makes that matches the URL with wildcards. The Sentry tunnels the data to the app server that has the URL that the app specified. The Server List field is therefore not applicable when the Service Name is <ANY>. For example, consider when the app requests URL myAppServer.mycompany.com, which matches *.mycompany.com in the app configuration. The Sentry tunnels the data to myAppServer.myCompany.com. Docs@Work typically uses the <ANY> service, so that it can browse to any of your internal servers. NOTE: Do not select the <ANY> option for tunneling to CIFS-based content servers, Office 365, Box, and Dropbox. For CIFS-based content servers, select <CIFS_ANY>.
	• <CIFS_ANY> Select <CIFS_ANY> to allow tunneling to any URL for a CIFS-based content

Item	Description
	server. Typically, you select <CIFS_ANY> if the URL for a CIFS-based content server contains wildcards for tunneling, such as *.myCompany.com. NOTE: The order of the Service Name entries does not matter.
Server Auth	Select the authentication scheme for the Standalone Sentry to use to authenticate the user to the app server: • Pass Through The Sentry passes through the authentication credentials, such as the user ID and password (basic authentication) or NTLM, to the app server. • Kerberos The Sentry uses Kerberos constrained delegation (KCD). KCD supports Single Sign On (SSO). SSO means that the device user does not have to enter any credentials when the AppConnect app accesses the app server. The Kerberos option is only available if you selected Identity Certificate for Device Authentication.
Server List	Enter the app server's host name or IP address (usually an internal host name or IP address). Include the port number on the app server that the Sentry can access. Example: sharepoint1.companyname.com:443 Acceptable characters in a host name are letters, digits, and a hyphen. The name must begin with a letter or digit. You can enter multiple servers. The Sentry uses a round-robin distribution to load balance the servers. That is, it sets up the first tunnel with the first app server, the next with the next app server, and so on. Separate each server name with a semicolon. Example: sharepoint1.companyname.com:443;sharepoint2.companyname.com:443 NOTE: The Server List field is not applicable when the service name is <ANY> or <CIFS_ANY>.

Item	Description
TLS Enabled	Select TLS Enabled if the app servers listed in the Server List field require SSL. This option is not applicable when the service name is <ANY> or <CIFS_ANY>. NOTE: Although port 443 is typically used for https and requires SSL, the app server can use other port numbers requiring SSL.
Proxy/ATC	Select if you want to direct the AppTunnel service traffic through the proxy server. You must also have configured Server-side Proxy or Advanced Traffic Control (ATC).
Server SPN List	Enter the Service Principal Name (SPN) for each server, separated by semicolons. For example: sharepoint1.company.com;sharepoint2.company.com. The Server SPN List applies only when the Service Name is not <ANY> and the Server Auth is Kerberos. If each server in the Server List has the same name as its SPN, you can leave the Server SPN List empty. However, if you include a Server SPN List, the number of SPNs listed must equal the number of servers listed in the Server List. The first server in the Server List corresponds to the first SPN in the Server SPN List, the second server in the Server List corresponds to the second server in the Server SPN List, and so on. NOTE: When the Service Name is <ANY> and the Server Auth is Kerberos, the Standalone Sentry assumes that the SPN is the same as the server name received from the device.

5. Click **Save**.

Related topics

For more information on configuring AppTunnel, advanced traffic control, and AppTunnel rules, see “Configuring an AppTunnel service” in the AppConnect and AppTunnel Guide.

Configuring AppTunnel rules

You create AppTunnel rules in the Docs@Work configuration as part of an AppTunnel setup required to tunnel traffic to content repositories. When Docs@Work tries to connect to the URL configured in **AppTunnel Rules**, Standalone Sentry creates an AppTunnel to the content server.

Note The Following:

- MobileIron strongly recommends that you do not configure AppTunnel rules with '*' in the URL. Docs@Work may not be able to activate the license for the embedded editor, impacting viewing and editing functionality.
- Standalone Sentry does not support tunneling traffic to Office 365, Box, and Dropbox. Therefore, if you are configuring access to Office 365, Box, or Dropbox, do not use URL patterns (example: *) to configure the AppTunnel traffic rules.

Before you begin

Ensure the following:

- Standalone Sentry is configured for AppTunnel.
- An AppTunnel service is configured in Standalone Sentry. See Configuring an AppTunnel service on page 18.

Procedure

1. In the MobileIron Core Admin Portal, go to **Policies & Configs > Configurations**.
2. Select for the Docs@Work configuration you want to add AppTunnel rules.
3. Click on **Edit.**
4. In the **AppTunnel Rules** section click on **Add+**.
5. Use the following guidelines to create an AppTunnel rule:

Item	Description
AppTunnel Rules	
Sentry	Select the Standalone Sentry that you want to tunnel the URLs listed in this AppTunnel entry. The drop-down list contains all Standalone Sentrys that are configured to support AppTunnel.
Service	Select a Service Name from the drop-down list. This service name specifies an AppTunnel service configured in the App Tunneling Configuration section of the specified Sentry.
URL Wildcard	Enter one of the following: • A content server's hostname Example: finance.yourcompany.com • A hostname with wildcards. The wildcard character is *. Example: *.yourcompanyname.com If you want finer granularity regarding what requests the Standalone Sentry tunnels, configure multiple AppTunnel rows.
URL Wildcard	The Sentry and Service fields that you specify in the AppTunnel row determine the target content server. Note The Following: • A hostname with wildcards works only with the service <ANY> or <CIFS_ANY>. Unlike services with specific service names, these services do not have associated app servers. The Standalone Sentry tunnels the data to the app server that has the URL that the app specified. • **The order of these AppTunnel rows matters**. If you specify more than one AppTunnel row, the first row that matches the hostname requested is chosen. That row determines the Standalone Sentry and Service to use for tunneling. • Do not include a URI scheme, such as http:// or https:/, in this field. • If you are directing Office 365, Box, or Dropbox traffic through an AppTunnel, do not use URLs with wildcards.

Item	Description
	NOTE: Tunneling traffic through Standalone Sentry is not supported for Box and Dropbox. • Docs@Work data is tunneled only if the Docs@Work request matches the hostname in the URL Wildcard field and the port number specified in the Port field.
Port	Enter the port number that Docs@Work requests to access. App data is tunneled only if the app's request matches the hostname in the URL Wildcard field and this port number. NOTE: If a port number is not configured, for http and https traffic, the default port is used. The default port used for http is 80 and the default port used for https is 443.
Identity Certificate	Select the Certificate or the SCEP profile that you created for devices to present to the Standalone Sentry that supports app tunneling.

Configuring attachment control

Configuring email attachments to open in Docs@Work and encrypt, protects corporate data from being leaked.

Before you begin

A Standalone Sentry set up for ActiveSync is required to enable device users to open encrypted email attachments in Docs@Work.

See "Configuring Standalone Sentry for ActiveSync" in the MobileIron Sentry Guide for information about how to set up a Standalone Sentry for ActiveSync.

Procedure

1. In the Admin Portal, go to **Services > Sentry**.
2. Select the Standalone Sentry that handles email for the devices.
3. Click the edit icon.
4. In the section **Attachment Control Configuration**, select **Enable Attachment Control**.
5. For **iOS using native Email**, select **Open with Docs@Work and protect with encryption**.
6. Click **Save**.

For information on setting up Standalone Sentry and configuring attachment control, see "*Email attachment control with Standalone Sentry*" in the *MobileIron Sentry Guide*.

What users see

When the device user opens an email attachment,

- the attachment is automatically downloaded to the Imported Files folder in My Files. An Imported Files folder is automatically created if one did not already exist.
- if the document type is supported, the attachment is automatically opened for viewing.

Main steps for configuring Docs@Work for iOS (Cloud)

Configuration for Docs@Work is done in MobileIron Cloud. Following are the main steps for configuring Docs@Work for iOS on MobileIron Cloud:

1. Adding Docs@Work for iOS on MobileIron Cloud
2. Configuring Docs@Work for iOS on MobileIron Cloud
3. (Optional) Configuring AppTunnel for Docs@Work

Adding Docs@Work for iOS on MobileIron Cloud

Docs@Work for iOS is available in the app catalog in MobileIron Cloud.

Procedure

1. In MobileIron Cloud, go to **Apps > App Catalog > +Add**.
2. In **Business Apps**, click **Docs@Work (iOS)**.
3. Make any updates as necessary and click **Next**. You can change the category and add a description.
4. Choose a distribution option for the app and click **Next**.
5. Update the default install settings or add install settings as necessary.
6. Update the promotion settings or add promotion settings as necessary.
7. For **Docs@Work configuration**, click **+** icon to add Docs@Work configuration.

Next steps

Configuring Docs@Work for iOS on MobileIron Cloud

Configuring Docs@Work for iOS on MobileIron Cloud

After adding Docs@Work to MobileIron Cloud, configure Docs@Work on MobileIron Cloud.

Procedure

1. In the MobileIron Docs@Work configuration, enter a name for the configuration.
2. Configure the Docs@Work settings as needed.
3. Add any custom configurations for the app in **AppConnect Custom Configuration**.
4. Add any certificates that are required.
5. Choose a distribution option for the configuration and click **Done**.
   The configuration is distributed to the subset of the devices to which the app is distributed

Content sites configured in the Doc@Work configuration are automatically added to the Docs@Work app. Device user action is not required.

(Optional) Configuring AppTunnel for Docs@Work

You create an AppTunnel service in Standalone Sentry as part of the AppTunnel setup required to tunnel traffic to content repositories. CIFS traffic must be tunneled through Standalone Sentry.

Before you begin

Ensure that you have a Standalone Sentry that is set up for AppTunnel and the necessary device authentication is also configured. See “Configuring Standalone Sentry for app tunneling” in the MobileIron Sentry Guide.

Procedure

1. In the MobileIron Docs@Work **App Configuration > AppTunnel**, click **+** icon.
2. Enter a name for the configuration.
3. Optionally add a description for this configuration.
4. Enter the domain wildcards for the App Tunnel.
5. Choose a distribution level for this Configuration.

Related topics

For more information on configuring AppTunnel, advanced traffic control, and AppTunnel rules, see “Configuring an AppTunnel service” in the AppConnect and AppTunnel Guide.

Default iOS AppConnect Configuration

The Default iOS AppConnect Configuration is enabled by default and applied to all iOS devices. The iOS AppConnect Configuration specifies AppConnect app settings such as AppConnect passcode and data loss prevention requirements.

You may edit the Default iOS AppConnect Configuration (**Configurations > Default iOS AppConnect Configuration**) if needed. The changes will be applied to all iOS devices. If you want the setting to be applied to only some iOS devices, create a new AppConnect Device configuration (**Configurations > AppConnect Device**) for iOS and distribute the new configuration to a subset of iOS devices.

User-added sites

Users can add the following types of sites:

- Box
- Cloud Storage
- Dropbox
- Network Drive
- SharePoint

To add corporate sites, the user will need the following information:

- The site’s URL. The URL must include http:// or https://. Both domain name and IP address are supported.

- Type of Authentication for Network drives. The authentication setting is labeled No Authentication.
- Device users should enable this setting, if the site does not require authentication.
- Type of authentication for SharePoint servers:

Authentication type	Description
Corporate	User authenticates with on-premise SharePoint using either Windows NTLM or Forms-based authentication with corporate credentials. User credentials can be domain\username or just username, depending on how SharePoint is set up with Windows domain authentication.
Office 365	User authenticates with Office 365 SharePoint using the authentication mechanism supported by Office 365. User credentials map to the user’s account on Office 365, or to the user’s AD credentials. If Office 365 has been integrated with corporate AD, then user’s SharePoint credentials map to AD credentials.
NoAuthn	User doesn’t need to provide credentials for authentication. The SharePoint server supports anonymous access..

- Web View. For SharePoint sites, the user can turn on Web View to be able to view and navigate SharePoint folders in browser view.

Related topics

For more information about topics such as app delegation, see the *MobileIron Cloud Administrator Guide*.

Docs@Work installation on an iOS device (Core and Cloud)

Device users can install Docs@Work from a notification they receive on their iOS device, or from the MobileIron app catalog on their device.

- **Docs@Work** for iOS installation from notification: After you send an installation request for Docs@Work for iOS, users receive a notification that prompts them to install the new or updated app. By tapping Install, Docs@Work for iOS is installed to the device.
- **Docs@Work** for iOS installation from the MobileIron app catalog: When a featured app or an update to an installed app is published to device users, those users see a badge that appears on the corresponding tab in the MobileIron app catalog.
  The number on the badge indicates the number of apps or updates available. The availability of an update is determined by comparing the version number for the installed app to that of the newly-published app.

  After importing Docs@Work for iOS into the app distribution library, the app appears in Apps@Work on the device. Tap the entry for Docs@Work and follow the prompts to install the app.

Docs@Work configuration field description (Core and Cloud).

The following table provides a description of the configuration fields for Docs@Work for iOS on MobileIron Core and Cloud.

TABLE 2. DOCS@WORK CONFIGURATION FIELD DESCRIPTION IN MOBILEIRON CORE AND CLOUD

Item	Description
Name	Enter brief text that identifies this setting.
Description	Enter additional text that clarifies the purpose of this Docs@Work setting.
Client TLS	If the app is using certificate pinning, select **Enable Client TLS Configuration** and choose the appropriate Client TLS configuration from the dropdown.
AppTunnel Rules	Configure AppTunnel rules settings for this app. First, configure the Standalone Sentry to support AppTunnel.
	Enable MobileIron Access: The setting is available only if MobileIron Access is configured in the Admin Portal in **Services > Access**. Otherwise, the setting is grayed out. If the option is selected, MobileIron Access trusts the HTTPS traffic via AppTunnel. Tunnel is not needed in this setup. NOTE: If **Enable Split Tunneling using MobileIron Tunnel** is selected, HTTPS authentication traffic, which would have previously used AppTunnel to Access, goes through Tunnel instead.
	Enable Split Tunneling using MobileIron Tunnel: iOS only. Requires Mobile@Work 12.3.0 and MobileIron Tunnel 4.1.0 for iOS. Before enabling the option, ensure that MobileIron Tunnel is deployed and a Tunnel VPN configuration is applied to the AppConnect app. For information about deploying MobileIron Tunnel for iOS, see the *MobileIron Tunnel for iOS Guide for Administrators*. Select the option if the AppConnect app will transition to using WKWebView or the app currently uses WKWebView and any of the following is also true: • AppTunnel rules are configured to tunnel app data. • Enable MobileIron Access is selected. Enabling the option allows the configured AppTunnel rules to be managed through MobileIron Tunnel rather than through AppTunnel. For more information about configuring **Enable Split Tunneling using MobileIron Tunnel** for Docs@Work, see Split Tunneling using MobileIron Tunnel.
Content Sites	

Item	Description
Name	Enter a name for the content site.
URL	Enter a valid URL for the content site. A valid URL must start with http:// or https://. Starting with MobileIron Core 7.5.1.0, if you are using variables, http:// or https: is not required. However, the entry in the URL field must map to a valid URL that starts with a http://, https://, or smb://. UNC is also supported. Examples: $USER_CUSTOM2$ https://$USER_CUSTOM1$ **CIFS sites** For CIFS sites, the URL must also include the CIFS port. A valid URL can start with smb:// or \\. UNC is supported. Both domain name and IP address are supported. Examples for CIFS: https://server.name:445/path/to/share/folder smb://server.name:445/path/to/share/folder \\server.name:445\path\to\share\folder **Variables** You can also specify variables in the URL. You can specify a single variable, or a combination of variables. LDAP or AD integration is required for using variables. See also, Docs@Work configuration field description (Core and Cloud). on page 27. Examples with variables: https://networkdrive/users/$FIRST_NAME$ https://sharepoint.mycompany.com/personal/$FIRST_NAME$_$LAST_NAME$_company_com/ **SharePoint URL's limitation with Docs@Work** The SharePoint URL is case sensitive. You need to enter the URL path with the exact case as it is configured in SharePoint Servers. This is applicable for both SharePoint Online (O365) and SharePoint OnPrem. For example: If SharePoint URL in SharePoint Server is configured as **https://<FQDN>/personal/Documents** and if MobileIron Core or Cloud has configured the SharePoint URL as **https://<FQDN>/Personal/documents** then Docs@Work will fail to load the Documents page in non Web View mode. Admin has to configure the SharePoint URL in MobileIron Core or Cloud as **https://<FQDN>/personal/Documents** with exact case.

Item	Description
	OneDrive for Business The credentials for OneDrive for Business are always in lower case. If the credentials in LDAP or AD are mixed case, they may not match with the credentials in OneDrive and may result in failure to access the OneDrive for Business site from Docs@Work. To ensure that device users can successfully access OneDrive for Business add #LOWER to the variable in the URL. Example for OneDrive for Business: https://company.sharepoint.com/personal/#LOWER($USERID$)#_company_com/documents
Domain	Select the type of content site you are configuring: • SharePoint Select SharePoint for OneDrive for Business. • WebDAV • CIFS
Subdomain	Select the subdomain type for the content site: • SharePoint: Office 365, Corporate Select Office 365 if you are configuring OneDrive for Business. • WebDAV: NetworkDrive, CloudStorage • CIFS: NetworkDrive • DFS: NetworkDrive
Authentication	Select if the device has to authenticate to the server. Do not select if you are using Single Sign On using Kerberos Constrained Delegation. See also “Supported authentication to content repositories” in the MobileIron Docs@Work Release Notes.
Published	Select to designate the site as a Published site. All content in a Published site is automatically downloaded and mirrored locally on the device when the device syncs. If the option is not selected, the device user must manually download the content. Documents in a Published site cannot be edited. Devices users cannot upload or create files or folders in published site. A Web View site cannot be configured as a Published site, and a Published site cannot be configured as a Web View site. NOTE: Published sites for SharePoint are not supported at root, site, and subsite levels. Published sites are supported at document library and folder levels. MobileIron recommends that Published sites be set for publishing 50-100 documents.
Web View	Only for SharePoint domains. Only applicable to iOS devices. Does not apply to Android devices.

Item	Description
	Select to allow device users to view and navigate SharePoint folders in browser view.
Published Site Configurations These settings only apply to Published sites.	
Update Interval (Minutes)	Specify the update interval for Published sites. The Default setting is every 60 minutes.
Max auto download size (MB)	Specify the maximum file size for automatic download. Files greater than this size will not be automatically downloaded. The default setting is 500 MB.
Max documents per update	Specify the maximum number of documents to update for each site. Only the number of files specified will be updated. The default setting is 100 files.
Update Mode	Specify the method devices can use to update Published sites. Select either Wi-Fi Only or Wi-Fi and Cellular. MobileIron recommends using Wi-Fi only if you support large number of documents.
App Configuration	
URL	Enter a URL for the content site. The URL must include http:// or https://. Both domain name and IP address are supported. To use the following CIFS URL *smb://server.name:445/path/to/share/folder* Convert it to a Content Site URL *https://server.name:445/path/to/share/folder*
Domain	Select the type of content site you are configuring: • SharePoint (Select SharePoint for One Drive for Business) • WebDAV
Subdomain	Select the subdomain type for the content site: • SharePoint: Office 365, Corporate Select Office 365 if you are configuring OneDrive for Business. • WebDAV: NetworkDrive, CloudStorage
Authentication	Select if you want the device to authenticate to the server.
Published Site	Select to designate the site as a published site.

Item	Description
	All content in a published site is automatically downloaded and mirrored locally on the device when the device syncs. If the option is not selected, the user must manually download the content. A Web View site cannot be configured as a published site, and a published site cannot be configured as a Web View site. NOTE: Published sites for SharePoint are not supported at root, site, and subsite levels. Published sites are supported at document library and folder levels. MobileIron recommends that published sites be set for publishing 50-100 documents.
Web View	Only for SharePoint domains. Select to allow users to view and navigate SharePoint folders in browser view.
Published site	
Update Interval (Minutes)	Specify the updated interval for published sites. The Default setting is every 60 minutes.
Max auto download size (MB)	Specify the maximum file size for automatic download. Files above this size will not be automatically downloaded. The default setting is 500 MB.
Max documents per update	Specify the maximum number of documents to update for each updated site. Only the number of files specified will be updated. The default setting is 100 files.
Update Mode	Specify the method devices can use to update published sites. Select either Wi-Fi Only or Wi-Fi and Cellular. MobileIron recommends using Wi-Fi Only if you support large number of documents.
Custom Configurations	To configure custom app behavior, add key-value pairs to manage and control the device user experience. For more information about configurable key-value pairs, see Additional configurations using key-value pairs.

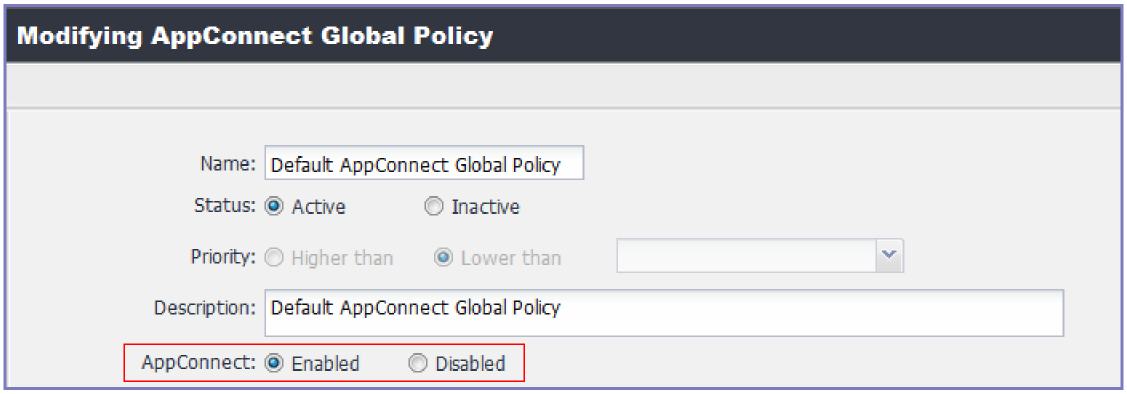
Configuring the AppConnect global policy

Docs@Work for iOS is an AppConnect app, so AppConnect must be enabled in the AppConnect global policy if it has not yet been configured. The AppConnect global policy specifies AppConnect app settings such as AppConnect passcode and data loss prevention requirements. You can use the Default AppConnect Global Policy.

You may decide to create a new AppConnect Global Policy (**Add New > AppConnect**). If you create a new AppConnect Global Policy, you must apply it to the appropriate labels. You do not need to apply the Default AppConnect Global Policy to a label.

Procedure

1. In the Admin Portal, go to **Policies & Configs > Policies**.
2. Select **Default AppConnect Global Policy**.



Modifying AppConnect Global Policy

Name: Default AppConnect Global Policy

Status: ● Active ○ Inactive

Priority: ○ Higher than ● Lower than

Description: Default AppConnect Global Policy

AppConnect: ● Enabled ○ Disabled

3. For **AppConnect**, select **Enabled**.
4. (Optional) Scroll down to the **Security Policies** section.
5. (Optional) For **Apps without an AppConnect container policy**, select **Authorize**.

NOTE: If you do not select **Authorize**, then you must create an AppConnect container policy for Docs@Work

6. (Optional) If you select **Authorize** for **Apps without an AppConnect container policy**, also select the data loss preventions options you want to enable for iOS.
7. Click **Save**.

Applying to a label

Applying a policy or configuration to a label makes the policy or configuration available to all the devices that are associated with that label. Perform these steps only if you created a new AppConnect Global Policy. You do not need to apply a default AppConnect Global Policy to a label.

Procedure

1. Select the AppConnect global policy.
2. Click **More Actions > Apply To Label**.
3. Select the appropriate labels to which you want to apply the policy.
4. Click **Apply**.

Related topics

For more information about the AppConnect Global policy, see the “Configuring the AppConnect global policy” section in the AppConnect and AppTunnel Guide.

AES-256-GCM encryption for email attachments

You can configure Docs@Work to use 256-bit encryption. If you already have Docs@Work (original) enabled and are now enabling Docs@Work, the system continues to use 128-bit encryption for email attachments. To use 256-bit encryption with Docs@Work, you must first disable Docs@Work (Original) and then regenerate the attachment encryption key. A 256-bit key is only generated if Docs@Work (Original) is disabled and all Standalone Sentrys are at least at version 6.1.0.

Docs@Work (Original)	Docs@Work	Sentry Version	Encryption key generated
Enabled	Enabled	-	AES-128-ECB
Disabled	Enabled	Some Standalone Sentrys are at least at version 6.1.0.	AES-128-ECB
Disabled	Enabled	All Sentrys are at least at version 6.1.0.	AES-256-GCM

Note The Following:

- Key regeneration causes a restart for all Standalone Sentrys that use encryption for attachment control. A restart can cause a brief interruption in email service to device users.
- After regenerating the encryption key, iOS device users who use the iOS native email client cannot read previously received attachments. If device users need to read previously received attachments, re-push the Exchange setting to the devices. MobileIron advises caution when re-pushing the Exchange setting. Re-pushing the Exchange setting increases the load on the Exchange server.

TIP: After you upgrade Standalone Sentry, in the Core Admin Portal, go to **Services > Overview**, and click **Verify** for the Standalone Sentry. This action immediately updates the Standalone Sentry version in Core. Otherwise, the Standalone Sentry version in Core is updated at the next sync. All Standalone Sentry versions in Core must be at least at Sentry 6.1.0 release to generate a 256-bit key.

Configuring 256-bit encryption

You will need to enable 256-bit encryption, if you previously had Docs@Work (Original) enabled.

Procedure

1. Ensure that all Sentrys configured on Core are at least at Sentry 6.1.0.
2. In the Admin Portal, go to **Settings > System Settings**.
3. Scroll down to the **Additional Products** section.
4. Click on **Licensed Products**.
5. De-select **Enable Docs@Work (Original)**.
6. Ensure that **Enable Docs@Work** is enabled.
7. Click on **Save**.
8. Go to **Settings > Sentry**, and click **Preferences**.
9. In the **Standalone Sentry** section, click **Regenerate Key**.

Related topics

For information about regenerating the encryption key, see “Regenerating the encryption key” in the MobileIron Sentry Guide.

Configuring certificate pinning

To use Certificate Pinning, in Docs@Work configuration enable Client TLS option and select the configured Client TLS configuration listed to provide more security between Docs@Work and enterprise server communication. For more information to configure Client TLS see, *Creating a Client TLS configuration* section in the *MobileIron Core AppConnect and AppTunnel Guide*.

Split Tunneling using MobileIron Tunnel

Due to Apple deprecation of support for **UIWebView** and the impact that has on AppConnect AppTunnel on iOS, there is a new option, **Enable Split Tunneling using MobileIron Tunnel** in the AppTunnel configuration for Docs@Work on MobileIron unified endpoint management (UEM) platform.The MobileIron UEM platforms are MobileIron Cloud or MobileIron Core.

Before enabling the option in MobileIron UEM, ensure that MobileIron Tunnel is deployed and the Tunnel VPN configuration is applied to the Docs@Work for which you are enabling the split tunneling option.

Enabling the option allows the AppTunnel rules to be applied to MobileIron Tunnel along with AppTunnel. The workaround is available due to the planned deprecation of the UIWebView API by Apple.

NOTE: This feature is not applicable if you are already using the split tunneling configuration on MobileIron Access for your native iOS apps.

In addition to MobileIron Tunnel 4.1.0, the feature requires either one of the following:

- Mobile@Work 12.3.0 and MobileIron Core 10.7.0.0.
- MobileIron Go 5.4.0 and MobileIron Cloud 70.

For information about configuring AppConnect App Configuration and AppTunnel configuration on MobileIron Cloud, see "Configuring AppConnect Apps" and "Configuring AppTunnel traffic rules" sections in the MobileIron Cloud Administrator Guide.

For information about configuring AppConnect App Configuration on MobileIron Core, see "AppConnect app configuration" in the *MobileIron Core AppConnect* and *AppTunnel Guide*.

The feature requires **Mobile@Work 12.3.0** and **MobileIron Tunnel 4.1.0 for iOS**. For information about the UIWebView API deprecation, see UIWebView Deprecation and AppConnect Compatibility.

Configuring split tunneling with MobileIron Tunnel (Core)

This section describes the steps to configure split tunnel on Docs@Work.

Before you begin

- Ensure that MobileIron Sentry service is active. For more information, see Enabling split tunneling section in the *MobileIronAccess Guide*.
- Ensure that MobileIron Tunnel is deployed and a Tunnel VPN configuration is applied to the AppConnect app. For information about deploying MobileIron Tunnel for iOS, see the *MobileIron Tunnel for iOS Guide for Administrators*.

Adding Per App VPN to Docs@Work app

The following steps describe how to add Per App VPN to Docs@Work configuration. Ensure that Per App VPN profile is already created.

Procedure

1. In the Admin Portal, go to **Apps > App Catalog**.
2. Click Docs@Work, click **Edit**.
3. Under the **Per App VPN Settings**, select **Per App VPN by Label Only** checkbox.
4. Select the VPN available in the list and click the right arrow.
5. Click **Save**.

Editing Docs@Work Configuration

The following steps describe how to edit Docs@Work configuration to enable Split Tunneling on MobileIron Core.

Procedure

1. In the **Admin Portal**, go to **Policies & Configs > Configurations**.
2. Select the check box for Docs@Work configuration.
3. Click **Edit**, in the **Edit Docs@Work Setting** page, go to AppTunnel Rules.
4. Under the **AppTunnel Rules** section, select the **Enable Split Tunneling using MobileIron Tunnel** option.
5. Click **Save**.

For information about configuring AppConnect App Configuration, see "AppConnect app configuration" in the *MobileIron Core AppConnect and AppTunnel Guide*.

For more information Creating Per App VPN or MobileIron Tunnel VPN setting, see VPN settings in the *MobileIron Core Device Management Guide for iOS and macOS Devices*.

Configuring split tunneling with MobileIron Tunnel (Cloud)

This section describes the steps to configure split tunnel on Docs@Work for MobieIron Cloud.

Before you begin

- Add and configure MobileIron Tunnel app. For more information, see Main tasks for configuring MobileIron Tunnel for iOS (Cloud) section in the *MobileIron Tunnel for iOS Guide for Administrators* guide.

- Ensure that you have a Standalone Sentry set up for AppTunnel and the necessary device authentication is also configured. See “Configuring Standalone Sentry for app tunneling” in the *MobileIron Sentry Guide*.
- Ensure Per App VPN is created.

Editing Docs@Work configuration

The following steps describe how to edit Docs@Work configuration to enable Split Tunneling on MobileIron Cloud.

Procedure

1. In the MobileIron Docs@Work **App Configuration > AppTunnel**, click **+ icon**.
2. Enter the **Name** of the configuration.
3. In the **App Tunnel** section, edit the following fields:
   a. Sentry Profile
   b. Turn **ON** the **Enable Split Tunneling using MobileIron Tunnel** option.
4. Add App Tunnel rules.
5. Choose a distribution option for the configuration.
6. Click **Save**.
7. In **App Configuration > Per App VPN** and click **+ icon**.
8. Enter the **Name** of VPN configuration.
9. Select the **Enable Per-App VPN for this app** check-box to select MI Tunnel configuration from the drop-down list.
10. Choose a distribution option for the configuration and click **Done**.
11. Click **Save**.

After configuring split tunneling, ensure that the configurations are pushed to the device.

For more information, see https://help.mobileiron.com/s/article-detail-page?Id=kA12T000000TTetSAG.

Additional configurations using key-value pairs

Key-value pairs allow you to manage and control the device user experience in the following ways:

- Making it easier for the device user to email you logs for the app.
- Controlling the detail in the device logs to help troubleshoot issues.
- Controlling which types of sites device users can add to Docs@Work.
- Restricting the number of User sites device users can add.
- Disabling editing in Docs@Work
- Enabling the embedded viewer in Docs@Work
- Autofilling username and domain

Unless otherwise noted, key-value pairs are not case sensitive.

Configuring Docs@Work application behavior

To configure app behavior, you add key-value pairs in the Custom Configurations section of the Docs@Work configuration.

Procedure

1. In the MobileIron Core Admin Portal, go to **Policies & Configs > Configurations**.
2. Select for the Docs@Work configuration you want to edit.
3. Click **Edit.**
4. In the **Custom Configurations** section click on **Add+** to add a key-value pair.
   See Key-value pairs to configure app behavior on page 37.
5. Click **Save**.

Key-value pairs to configure app behavior

TABLE 3. KEY-VALUE PAIRS TO CONFIGURE APP BEHAVIOR

Key	Value	Description
Specify the level of detail for logs		
log_level	• DEBUG • INFO • WARNING • ERROR	Select one of the following: • DEBUG: Includes debug level information for application flow and request, response messages for target repositories. This is the highest level and verbose, so choose this level only when needed. • INFO: Includes only information related to specific flows and requests. • WARNING: Includes only warnings about runtime errors and target repositories. • ERROR: Includes only runtime errors, and error and status codes from requests to target repositories.
Email logs		
support_email_id	Enter a valid email address.	Automatically populates the email address when the device user emails the device logs.
Block adding content		
blocked_storage_domains	• Box • WebDav • CIFS • SharePoint	Blocks device users from adding the content site to Docs@Work: Enter the values as a semicolon (;) separated list. Example: Box;Dropbox;CIFS Microsoft SharePoint includes Office 365 SharePoint sites. • If SharePoint, Box, or Dropbox is blocked, the option will not be available when the device user tries to add a site. • If WebDAV is blocked, both Network Drive and Cloud storage options will not be available. All WebDAV and CIFS sites will be removed from Docs@Work. • If CIFS is blocked, the device user is presented with an error message when trying to add a CIFS site. Existing CIFS sites will be removed. WebDAV sites will not be removed. Network Drive and Cloud storage options will continue to be available when the device user tries to add a site. • Documents from the blocked sites marked as Starred, Offline, or in Recents will be removed. Documents in My Files are not removed.
Block adding user sites		
disable_user_sites	true false	Blocks device users from adding sites to Docs@Work. User added sites will be removed. Documents from user

Key	Value	Description
		sites marked as Starred, Offline, or in Recents will be removed.
Restrict number of allowed user sites		
restrict_number_of_user_sites	Connector type: Number of sites that are allowed. For example: SharePoint:2, Box:1	Restricts the number of User sites that a device user can add. If a site type is not configured, there are no restrictions on the number of User sites for that site type. Restricting number of User sites has no impact on blocked sites. This key-value pair only applies to allowed sites. The configuration is ignored if DISABLE_USER_SITES is true. Enter the following value: • site type and number in the following format: Site type1:number; Site type2:number. Valid entries for site type are: SharePoint, Box, Dropbox, WebDAV, CIFS. Number is a positive integer greater than 0. In this example, the device user will be able to add up to two SharePoint sites, and only one Box site. There are no restrictions on any other type site.
Disable editing		
disable_editing	true false	Disables the following in My Files and all content sites in Docs@Work: • Editing. • Creating new files and folders. • Importing images from photo gallery. • Uploading to and deleting files in the backend resource.
Add group sites using key-value pairs		
SITE_DETAILS_N	Where *n* is a number 1-100 Example: SITE_DETAILS_1 Enter parameters for the content site in the following JSON format: {"name":"*name for the site*","url":"*valid url for the content repository including port*","domain":"SharePoint", "subDomain":"Federated","priority":“true | false”, "webView":“true | false”} Example to add a Google drive:	Adding a SharePoint Group site with Federated authentication *name for the site*: The name is displayed in the Docs@Work app. *valid url for the content repository including port*: The URL must start with http:// or https://. Both domain name and IP address are supported. If priority is not defined, the default setting is false. "priority":"false" identifies the content site as a Group site. Configuring “priority”:“true” identifies the site as a Published site. You can configure a site as a Published site only if “subDomain” is also configured.

Key	Value	Description
	{"name":"Google Group","domain":"GoogleDrive","url":"https://drive.google.com"} Example to add a Box Site: {"name":"Box1","domain":"BoxEnterprise","url":"https://www.box.com"} NOTE: • Ensure that there are no spaces • Values are case sensitive **Required parameters:** “name”, “url”, “domain”, “subDomain”	If "webView":"true", the SharePoint documents can be opened in Microsoft’s online web viewer and editor. The site is automatically a Group site. It cannot be configured as a Published site. Pushing Google Drive from Core. Pushing Enterprise Box Site from Core. **Example:** {"name":"SharePoint","url":"https://sharepoint.acme.com","domain":"SharePoint","subDomain":"Federated","priority":"false"}
Autofill Credentials		
autofill_credentials	Automatically populates the user name for the content site. Enter parameters for the content site in the following JSON format: {"URL":{"domainType":"*DomainType*","userName":"*$USERID$*","password":"*$PASSWORD$*"},"default":"Domain/$USERID$"} NOTE: For JSON format: - Ensure that there are no spaces. - Values are case sensitive. - Ensure that the JSON format is valid. - The variable for user name can be preceded by either a single forward slash or two back slashes: *Domain*/$USERID$ or *Domain*\\$USERID$	*URL*: Enter the URL for the content site. Include the protocol. Example: http, https. *Domain Type*: Enter one of the following: SharePoint, WebDAV, Box, BoxEnterprise, GoogleDrive, CIFS. *Domain*: Enter the domain name to which the username defaults if the username for the URL cannot be resolved. Variables are not supported. *password*: The user is logged in automatically when the user navigates to the site from the Sites screen. This feature is applicable for CIFS and WebDAV sites only on MobileIron Core. NOTE: $PASSWORD$ value is available only when admin enables "Save User Password" option on the device registration settings on MobileIron Core and user is registered to Mobile@Work Client. For more information, *MobileIron Core documentation* for its usage. The $PASSWORD$ option is not available for MobileIron Cloud. **Examples:** • {"https://sharepoint.miacme.com":{"domainType":"SharePoint","userName":"miacme/$USERID$"},"default":"miacme.com/$USERID$"} • {"https://sharepoint.miacme.com":{"domainType":"SharePoint","userName":"miacme\\$

Key	Value	Description
		USERID$"},"default":"miacme.com\\$USERID$"} • {"default": "domain/$USERID$"} {"https://cifs.company.com:445": {"domainType": "CIFS","userName": "$USERID$","password":"$PASSWORD$"}} NOTE: Copying and pasting JSON strings might result in invalid JSON. MobileIron recommends that you validate the JSON string before using it. There are validator tools such as JSONLint (jsonlint.com) that will help validate the JSON string.
Custom browser applications rather than default Safari browser		
http_ prefix	• mibrowser URLs starting with http:// are opened in Web@Work. • http URLs starting with http:// are opened in Safari. • googlechrome URLs starting with http:// are opened in Google Chrome.	Allows users to tap on a URL starting with http:// and view the site in a browser. If the key-value pair is not configured, users will not be able to view an http link in a browser. If the key-value pair is not configured, http:// links are not opened in any browser. MobileIron recommends that both HTTP_PREFIX and HTTPS_PREFIX are configured. If only one URL scheme is configured, the unconfigured URL scheme will not be opened in any browser, thus impacting user experience.
https_ prefix	• mibrowsers URLs starting with https:// are opened in Web@Work. • https URLs starting with https:// are opened in Safari. • googlechrome URLs starting with http:// are opened in Google Chrome.	Allows users to tap on a URL starting with https:// and view the site in a browser. If the key-value pair is not configured, users will not be able to view an https link in a browser. If the key-value pair is not configured, https:// links are not opened in any browser. MobileIron recommends that both HTTP_PREFIX and HTTPS_PREFIX are configured. If only one URL scheme is configured, the unconfigured URL scheme will not be opened in any browser, thus impacting user experience.
Apply SSO label to add SharePoint site flow		
apply_ sso_ label	• true • false	Changes the **NoAuthn** label to **Corporate single sign-on (SSO)** in Docs@Work. The **NoAuthn** option is seen in the **Authentication** settings for SharePoint sites in Docs@Work. There is no functional change.
Share PDF documents		
ENABL E_PDF_ DOCUM	• true • false	Makes the Share option available for PDF documents.

Key	Value	Description
ENT_DEFINE		
Default to Polaris Viewer instead of iOS Native Viewer		
enable_polaris_viewer	• true • false	Use this key-value pair to set the Docs@Work embedded viewer as default instead of iOS Native viewer.
Enable Polaris document content share		
ENABLE_POLARIS_DOCUMENT_CONTENT_SHARE	• true • false	Makes the **Share** option available for Microsoft Office documents in Polaris editor, regardless of whether Copy/Paste is enabled in AppConnect policy. This key-value pair is case sensitive.
Load/Authentication SharePoint for WebView		
ENABLE_WEBVIEW_AUTHENTICATION	• true • false	Use this key-value pair if the SharePoint server is not set up to use persistent authentication cookies and users encounter issues with opening WebView for SharePoint sites. This key-value pair is case sensitive.
Custom email app such as Email+ client		
mailto_prefix	**To open Email+, use** email+launcher://docsatwork?url=mailto: **To open IBM verse, use** ibmverse://com.ibm.lotus.traveler/mailto?to= **To open SecurePIM, use** spmailto:	Brings up the email client for which the schema is configured in mailto_prefix. Use this key-value pair to open the email client for which the schema is configured in mailto_prefix. Support for third party email client enabled.
Enable Certificate Based Authentication (CBA)		
IdCertificate_1_host	IdCertificate_1_host IdCertificate_1	Use this key-value pair to enable the certificate-based authentiation (CBA). For example: cert_hostname such as (defender.stutz.qa.domain.com) SharePoint

Key	Value	Description
		client-scep using authentication type. This key-value pair is case sensitive.
Display SharePoint title for files and folders		
show_ title	• true • false	Displays user friendly title for files and folders in SharePoint. Use the following values to set the key-value pair: • true: Enables title display. • false: Disables title display. The default value is set to false.
Allow sending analytics from Docs@Work to Mixpanel and Crashlytics		
allow_ analytic s	• true • false	Use the following values to set the key-value pair: • true: Enables sending analytics from Docs@Work to Mixpane and Crashlyticsl. • false: Disables sending analytics from Docs@Work to Mixpanel and Crahlytics. If the key-value pair is not defined in the configuration, allow_analytics is set to true by default.
Enable watermarks when viewing documents		
waterm ark_ text	Use a user identifying variables a values such as, $USERID$ and $EMAIL$.	Displays a diagonal watermark text (provided by the administrator) over all the documents viewed or edited using Docs@Work.
Allow document sharing from Docs@Work		
mi_ enable_ doc_ sharing	• true • false	Use this key-value pair to enable the Docs@Work document sharing feature. The default value is set to false, and must be set to true to enable document sharing.
Allow document sharing from Docs@Work for AppConnect apps		
MI_ SHARE D_ GROU P_ID	A unique, sufficiently complex alphanumeric string	This key manages the decryption of documents from Docs@Work extension. Once this key is set in Docs@Work configuration, only the apps having the identical key value in their configuration would be able to decrypt the documents from Docs@Work Extension. This is an optional key. The key is case sensitive. Enter the key in uppercase. IMPORTANT: Configure mi_enable_doc_sharing with value true to enable document sharing.
MI_AC_	A unique, sufficiently complex	This key manages the access control between the apps.

Key	Value	Description
ACCESS_CONTROL_ID	alphanumeric string	Once this key is set in Docs@Work configuration, only the apps having the identical key value in their configuration would be able to access the documents from Docs@Work Extension. Ensure that the key-value pair is configured in the Email+ configuration as well and that the value is identical (including case) in both Docs@Work and Email+ configurations. The key is case sensitive. Enter the key in uppercase. IMPORTANT: Configure mi_enable_doc_sharing with value true to enable document sharing.
Allow document sharing from Docs@Work for non AppConnect apps		
MI_AC_DOCUMENT_EXTENSION_DLP	• Sentry • All	This key allows the admin to add attachements when you compose mail using Email+ or anyother email client. This key is applicable while sharing documents from Docs@Work with non AppConnect apps.: **Sentry**: The documents are encrypted using Sentru attachement control key. **All**: The attachements are not encryptyed and are sent as plain text. The key is case sensitive. Enter the key in uppercase.
block_unmanaged_extension	• true • false	Allows the admin to block or unblock unmanaged versions of Docs@Work from exposing the document extension to all the apps. Default is set to false. If an admin wants to restrict the document sharing extension to only managed apps, then the block_unmanaged_extension key should be set to true. In addition to this, a separate configuration parameter IS_MANAGED should be set to true via the iOS MDM managed configuration. A sample of sample of managed app configuration is as follows: <?xml version=“1.0” encoding=“ UTF-8"?> <!DOCTYPE plist PUBLIC “-// Apple//DTD PLIST 1.0//EN” “http://www.apple.com/ DTDs/PropertyList-1.0.dtd“> <plist version=“1.0”> <dict>

Key	Value	Description
		<key>IS_MANAGED</key> <true/> </dict> </plist>
IS_MANAGED	• true • false	Set this key to true if you want to restrict extension only to managed apps . A sample.contents of managed app is as follow: <?xml version=“1.0” encoding=“UTF-8"?> <!DOCTYPE plist PUBLIC “-//Apple//DTD PLIST 1.0//EN” “http://www.apple.com/DTDs/PropertyList-1.0.dtd“> <plist version=“1.0”> <dict> <key>IS_MANAGED</key> <true/> </dict> </plist> The default values is set to False.
Custom keyboards		
MI_AC_IOS_ALLOW_KEYBOARDS	• true • false	This key allows the admin to enable or disable the use of custom keyboards. This key is enabled for AppConnect. This is case sensitive. true: Email+ allows the use of custom keyboards false: Email+ does not allow the use of custom keyboards. Default if key-value is not configured: true. This key-value pair is case sensitive. .
AppConnect logs		
MI_AC_LOG_LEVEL	• Error • Info • Verbose • Debug	Specifies the level of logging from the least to the most verbose. Default if key-value is not configured: true.

Key	Value	Description
MI_AC_LOG_LEVEL_CODE	Any string	Underspecification prompted in Mobile@Work to activate AppConnect logs
MI_AC_ENABLE_LOGGING_TO_FILE	• Yes • No	Enables collecting AppConnect logs to a file in Docs@Work.
Allow digital signature for PDF		
signing_certificate	Certificate	This key allows the admin to enable or disable the use of digital signature for PDF forms in Docs@Work added. To enable digital signature add signing_certificate to Docs@Work configuration to provide the certificate in **.p12** format used for PDF signing.
signing_certificate_ca_(n)	Certificate	This key allows the admin to add multiple Certificate Authorities to trusted CA's. If the signing_certificate is not issued by the CA which is not publicly trusted. The certificate must be DER-encoded. Where, the value of **n** can be 0 to 9. For example: signing_certificate_ca_0, signing_certificate_ca_1.
Miscelleneous		
document_menu_restricted_items	• define • lookup	This key allows the admin to fix the text data leak from Docs@Work document view or edit when you perform the Define and LookUp functions. For example: document_menu_restricted_items = define|lookup
disable_slideshow_autolock	• yes • no	This key prevents the device screen from getting locked during Microsoft PowerPoint presentation after Auto Lock timeout.

Key	Value	Description
group_offline_files	• true • false	Grouping offline files based on file path feature is added. To enabled this key set the "group_offline_files" key value to true in Docs@Work key-value pairs. The default value of this KVP is false. Offline file grouping is only for the Docs@Work and not for the file shown in the extension. After upgrade, if KVP is set to true, all offline files appear grouped.
filepass_key_identifier	A unique, sufficiently complex alphanumeric string.	This key allows admin to enable sharing documents securely between MobileIron Docs@Work and Microsoft IntuneMAM protected Office365 apps through FilePass. The value for this key-value pair needs to be same for the all the supported MobileIron Apps (Docs@Work, Email+, and FilePass) participating in File Sharing with Microsoft Office 365 apps.
disable_download_upload_autolock	• true • false	This key allows admin to disable device auto-lock during download or upload. The default values is set to False.
allow_filename_special_characters	• true • false	This key allows admin to enable special characters in the file name for a new folder or file created in Docs@Work. The following special characters are allowed in the file names: ~`#%^+;={}[],.' NOTE: Uploading files with special characters may not work for all the sites.

Edit functionality in Docs@Work

The editing feature is available by default. If you want to restrict mobile device users to read-only access to enterprise content, you can turn off editing in Docs@Work. Enter the DISABLE_EDITING key-value pair in the Custom Configurations section of the Docs@Work configuration. The key-value pair disables the following in My Files and all content sites in Docs@Work:

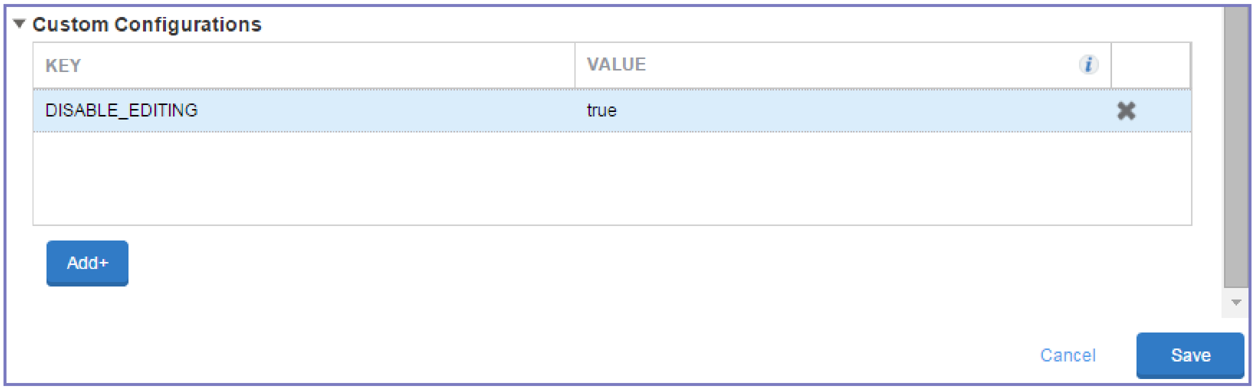
- Editing
- Creating new files and folders
- Importing images from photo gallery
- Uploading to and deleting files in the backend resource

Disabling the edit functionality in Docs@Work

You disable the edit functionality in Docs@Work using key-value pairs. If editing is disabled, device users will no longer see the edit options in Docs@Work. Users will also not be able to switch to edit mode while viewing a document.

Procedure

1. In the MobileIron Core Admin Portal, go to **Policies & Configs > Configurations**.
2. Select the Docs@Work configuration for which you want to disable editing.
3. Click **Edit**.



KEY	VALUE
DISABLE_EDITING	true

4. Scroll down to the **Custom Configuration** section.
5. Click **Add+** to enter the following key value pair:

Key	Value
DISABLE_EDITING	true

6. Click **Save.**

Working with Docs@Work features

Touch ID

If Touch ID is enabled for accessing secure apps, Docs@Work users can use Touch ID as an alternative to using their secure apps passcode. For information about enabling Touch ID for secure apps, see the *AppConnect and AppTunnel Guide*.

Sorting content sites

Device users can sort content sites by site name, creation date, or last opened. In addition, they can order the sites in ascending or descending order.

Procedure

1. Go to **Settings** in Docs@Work.
2. Tap the **Site Order** option.
3. Tap one of the following options to **Sort**:
   - Alphabetical Names: to sort by content site name.
   - Creation Date: to sort by the date the content site was added to Docs@Work.
   - Last Opened: to sort by when a content site was last opened.
4. Tap one of the following options to order the content sites:
   - Ascending: to order alphabetically from A to Z or from the most recent to the oldest date and time.
   - Descending: to order alphabetically from Z to A or from the oldest to the most recent date and time.

Content sites

Content sites configured by the administrator are automatically available in Sites in the Docs@Work app on the device. If a content site is configured as a Published site, the content is automatically downloaded to the device.

Content sites in Docs@Work fall into three types:

- **Group sites**
  Group sites are configured by the administrator and automatically pushed to Docs@Work app under Sites. Group sites cannot be deleted by the device user.
- **Published sites**
  Published sites are Group sites that update automatically and are available for offline use. If there are any changes, content is updated to the latest version at the configured update interval. Published sites can also be

manually updated when you pull to refresh. An update notification is also sent, and the Notifications icon is badged.
Published sites cannot be deleted by the device user. Documents in Published sites cannot be edited. Editing for documents in Published sites can only be enabled in Content Security Service.

- **User sites**
  Device users can also add sites to Docs@Work app under Sites. Sites that a user adds are identified as User sites.

You can check the available details about Group sites, Published sites, and User sites by tapping the Info icon.

Starred

When a file or folder is marked as Starred, a shortcut to the file or folder is available in Starred tab.

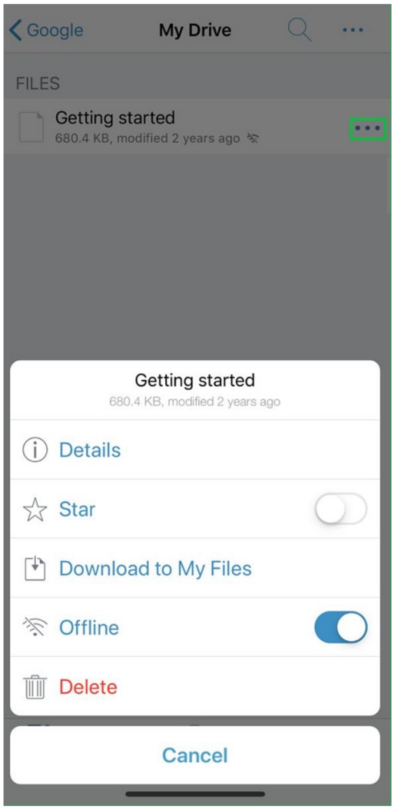
Offline

Docs@Work checks for any updates to the Offline documents on application launch or on a regular interval based on the Docs@Work configurations from the server. All the offline files can be grouped under one header using the **group_offline_files = true/false** key-value pair.

The files marked as offline are available for offline viewing. The files also remain in the source site folder. They are automatically updated to the latest version when you reconnect.

Procedure

1. In Docs@Work iOS app, under the **Sites** tab select a site for example Box, Dropbox, or SharePoint and so on.
2. Open the folder and tap on more option (...) menu to mark the files you want to view in offline mode. The following options are displayed:



3. Enable the Offline option. You can view the offline files under the Offline tab.
4. Click Cancel to stop the file download.

User added sites

Apart from the configured content sites pushed to Sites, device users can add both corporate and personal sites. Device users can add the following types of sites:

- Box
- Cloud Storage
- Dropbox
- Network Drive
- SharePoint

To add corporate sites, the device user will need the following information:

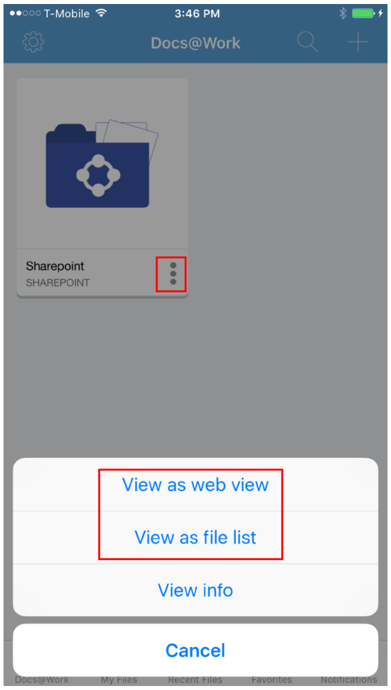
- **The site's URL.** The URL must include http:// or https://. Both domain name and IP address are supported.
- **Type of Authentication for Network drives.** The authentication setting is labeled **No Authentication**. Device users should enable this setting, if the site does not require authentication or you have set up Kerberos Single Sign On using MobileIron.
- **Type of authentication for SharePoint servers.** This can be Corporate, Office 365, NoAuthn, or Federated.

Authentication type	Description
Corporate	User authenticates with on-premise SharePoint using either Windows NTLM or Forms-based authentication with corporate credentials. User credentials can be domain\username or just username, depending on how SharePoint is set up with Windows domain authentication.
Office 365	User authenticates with Office 365 SharePoint using the authentication mechanism supported by Office 365. User credentials map to the user's account on Office 365, or to the user's AD credentials. If Office 365 has been integrated with corporate AD, then user's SharePoint credentials map to AD credentials.
NoAuthn	User does not need to provide any credentials for authentication. Access to on-premise SharePoint is set up with Kerberos Constrained Delegation (using Standalone Sentry), or the SharePoint server supports anonymous access.
Federated	User enters the enterprise AD or LDAP credentials to authenticate to the SharePoint server. The SharePoint server must be set up to use Active Directory Federation Services (ADFS).

- **Web View.** For SharePoint sites, the device user can turn on Web View to be able to view and navigate SharePoint folders in browser view.

View options for SharePoint sites in Sites

Device users have the ability to choose between **web view** and **file view** for SharePoint sites already added to Sites. This feature does not require any configuration changes by the device user or the administrator. To choose how the SharePoint site is viewed, tap the more information icon on the SharePoint tile in Docs@Work, then select either **View as web view** or **View as file list**.



Google Drive group site

Device users can do the following in a Google Drive content site in Docs@Work:

- Access documents in **My Drive** and **Shared with me**.
- Download and upload documents to and from **My Files** in Docs@Work.
- View, edit, annotate, star, and offline documents.
- View and edit Google document formats (docs, slides, sheets, and drawings) in Docs@Work. Google document formats will display the following icon:

  When you edit a Google document format, the changed document is saved in the corresponding Microsoft document format to **My Files**. The original Google document is not changed.
  Example: If you edit a Google Slides file, the changed Slides file is saved as a PowerPoint file to **My Files**. The original Google Slides file remains unchanged.
- Delete files and folders in My Drive.

If document encryption is enabled for Google Drive content site, documents uploaded from Docs@Work to Google Drive will be encrypted. Documents in the Google Drive site that are edited using Docs@Work will also be encrypted. These documents will have the .midx suffix. Example: myfile.doc.midx.

Email document links from Docs@Work

Device users can now email or copy a link to a document from within Docs@Work. The recipient of the email must have the correct permissions to view the document. However, the recipient does not need Docs@Work to open the document.

A secure email client is required on the device. If mailto_prefix key is set, the corresponding email client is used; otherwise, native email client is used to email document links.

The **Email a Link** and **Copy Link to Clipboard** options are available when you open the document.

Content site	Description
SharePoint, Office 365	The recipient must have the correct permissions to view the document. Docs@Work does not check if the recipient has the correct permissions when the device user shares the link. The URL is of the form: https://sharepoint1.companyname.com/ Shared Documents/Architecture/document.docx
Dropbox	Uses Dropbox APIs to create a public shareable link to the document. The URL is of the form: https://www.dropbox.com/folder/5lg6dgrv7m2c862/Getting%20Started.pdf?dl=0
Box	Uses Box APIs to create a public shareable link to the document. The URL is of the form: https://app.box.com/folder/50rvf49stdhqsywoj8lx
WebDAV network drive or cloud storage	The URL of the document corresponds to the WebDAV http or https URL. The URL is of the form: https://webdavserver.documents.mydoc.docx.
CIFS network drive	Not supported.

Email documents from Docs@Work

Docs@Work users can email documents from Docs@Work on their device. This provides users a true mobile experience and the flexibility to securely share documents directly from Docs@Work.

Requirement for emailing documents

- For iOS, **Open In** must be enabled in the AppConnect Global Policy or the AppConnect Container Policy.

- Open In must be enabled in the AppConnect Global Policy or the AppConnect Container Policy
- If mailto_prefix key is set, the Open In tray is used to email document; otherwise, native email client is used.

Emailing documents from Docs@Work for iOS

The **Email** option is available in an opened document.

Procedure

1. Tap to open a document.
2. Tap ⍐ in the opened document.
3. Tap **Email**.
   The document is downloaded and attached to a new email message.

NOTE: If attachment control is enabled to **Open only with Docs@Work and protect with encryption**, then the attachment will have **.secure** or the **.attachctrl** suffix.

Email Docs@Work logs

Occasionally it is necessary for you, the administrator, to obtain the Docs@Work logs from the user's device. You may need the Docs@Work logs to troubleshoot an issue. Device users can send the logs by tapping on **Email logs** under **Settings > Help**. By default, the native email client is used to email the Docs@Work logs.

Add attachments from Docs@Work in Email+

Docs@Work supports adding attachments to a mail using Email+ app. This capability will later be extended toother AppConnect-enabled applications including third-party email clients.

Email+ allows only a single file attachment and the file is attached to the email when you select the file.

Add attachments from Docs@Work in Native mail

Docs@Work supports adding attachments to a mail using native mail.

Email documents from Docs@Work through third-party email clients

The mailto_prefix key-value pair lets you choose a preferred email client within Docs@Work to send an email. The following options are available to email from Docs@Work:

- **Email a document:** Email a document option is supported for Email+ and native clients and third-party email clients
- **Email a link:** Email a link option works entirely dependent on the value of *mailto_prefix*, and is not dependent on different AppConnect data loss prevention (DLP) policy options.

The email client must be AppConnect enabled. For example: Email+, IBM Verse, SecurePIM and so on.

Edit documents in Docs@Work

When the device user first tries to edit a document, the device must have access to the Internet. The editor embedded in Docs@Work requires a license to activate. When it is first launched, the embedded editor tries to contact a license activation server to get a license. If the device is offline, an error message is displayed to the device user.

If a user tries to view an unsupported file, an error message is displayed.

Editing and annotating documents

To edit or annotate, users must download the document to My Files. If the file type is not supported for editing, the edit option will not be available. Online editing is only available with Office Web Apps.

Since Office Web Apps are only supported with SharePoint, Docs@Work supports online editing only with SharePoint folders. Office Web Apps must be enabled on the SharePoint server. If Office Web Apps are not enabled, the edit icon will not be available when you tap to view documents.

To edit or annotate a document:

1. Tap on the document.
2. Tap the ✎ edit icon.
3. If you are editing a document directly from a content repository, tap the doc icon.
4. Tap one of the options presented.

Option	Description
Save	Tap to save the edited file with the same file name. A local copy is created.
Save as	Tap to specify a different file name for the edited file. A local copy is created with the new file name.
Export	Tap to create a PDF. You have the option to change the file name. A local copy of the PDF is created.
Exit	Exits edit mode. Any changes to the file are not saved.

5. Tap one of the options presented when you exit edit mode.
   These options are only presented if you tapped on **Save as** or **Export**.

Option	Description
Save this File	Tap to save the edited file to the same location in the content repository.
Save a Copy	Tap to specify a different location to save the edited file. The location could be in the same content repository or different content repository. The file in the original location is not changed.
Download to My Files	Tap to download the edited file to **My Files**. The file in the original location is not changed. If a file with the same name is available a new file is added.
Cancel	Changes to the file are not saved.

- If saving to a different location fails, you will be presented with the option to download the document to **My Files**.
- To save an edited document, you must also tap **Exit**. If you do not **Exit** from edit mode, changes to the edited document will not be saved. If users try to open an email attachment while another document is open in edit mode, they are provided with the option to discard changes to the opened document before viewing the attachment.

Edit Online

On iPad devices, Docs@Work users may see an additional Edit Online option. The Edit Online option is available only for .docx, .pptx, and .xlsx files on SharePoint sites that have Office Web Apps enabled. Tapping on the Edit Online option takes the user to SharePoint Office Web Apps. The user can then edit the documents using Office Web Apps.

Extracting files from .zip files

Only .zip compressed files and password protected .zip files are supported. Other types of compressed files, such as gzip, .tar files, are not supported.

Note that .key, .numbers., and .pages files are displayed with a .zip extension in Docs@Work. Also, .key, .numbers, and .pages files with .zip extensions are not supported and cannot be extracted.

Procedure

1. Tap on the .zip file.
   If the .zip file is in a content repository, the My Files pop-up window displays. If necessary, you can tap an existing folder or tap **Create Folder.** Depending on your selection, the files are extracted into **My Files**, the selected folder, or the newly created folder.
   If the .zip file was already in **My Files**, a pop-up is not displayed. The file is automatically extracted to the same location as the .zip file
2. Tap **Extract Here**. (This step is only for a .zip file in a content repository.)
3. If a password is required, enter the password, then tap **Extract**.
   The .zip file and the extracted files are downloaded directly to **My Files** or to the folder in **My Files** that you specified. The files are extracted into a folder with the same name as the .zip file.

NOTE: If the .zip file contains a single file, a folder is not created for the extracted file.

File and folder management

Device users can create, move, and rename files in **My Files**. This allows users to manage files and folders on their mobile devices and upload the newly created files to content repositories. Device users can create text files (.txt) and the following Microsoft Office file types:

- .docx
- .pptx
- .xlsx

Devices users cannot upload or create files or folders in Published sites.

Creating files and folders in My Files

Device users can create files and folders in My Files.

Procedure

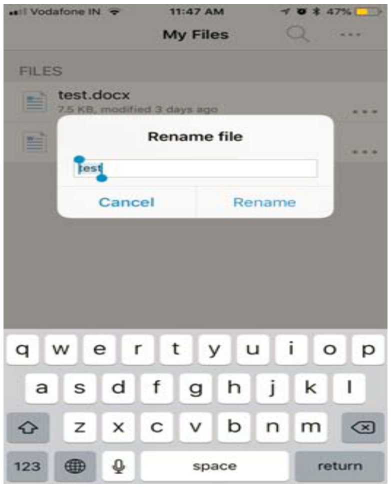
1. In Docs@Work, tap **My Files**.
2. Tap ... at the top of the screen.
3. Tap Create new **... .**
4. Tap Folder to create a new folder or tap one of the document types to create a new file.

Renaming files and folders in My Files

Device users can rename files and folders in My Files.

Procedure

1. In Docs@Work, tap **My Files**.
2. Tap ... next to the file or folder.
3. Tap the rename icon.
4. Enter a new name for the file or folder and tap **Rename**.



Moving files and folders in My Files

Device users can move files and folders in My Files.

Procedure

To move files or folders in **My Files**:

1. In Docs@Work, tap **My Files**.
2. Tap ... at the top of the screen.
3. Tap **Manage**.
4. Select the file and folders to move, then tap the move icon. Device users can select multiple files or folders to move.
5. Tap a folder, or tap **Create Folder**, or tap **Move Here** to move the selected files and folders to a different location.

Locating file or folder

The **Locate** function displays temporarily when the device user creates, moves, uploads, or downloads a file or folder.

The function does not display if the device user is in the same folder or location on Sites to which the document is moved. If the device user is in the same folder or location, the affected file is highlighted.

The **Locate** function allows the device user to quickly and easily navigate to the actual location of the file or folder.

Procedure

To locate a file or folder after you downloaded, uploaded, or moved:

1. Download, upload, or move the file or folder.
2. Tap **Locate** at the bottom of the screen.
   The actual location of the file or folder appears. If **Locate** points to a file, the file is temporarily highlighted.

Sorting files and folders

Device users can sort files and folder by the following methods:

- Name
- Date Created
- Last modified
- Last opened

Click on **Sort Files** in the menu, then select the method to sort.

Background notifications for Published sites

Background notifications alert device users to new content or updated content in Published sites even when Docs@Work is not running in the foreground. However, the user must be signed into Sites. Notifications allow users to always be aware of any changes in documents and have the latest versions of a document on their device.

Docs@Work checks for updates at the update interval set for the Published site and provides background notification if there are any changes. If other processes are running on the device at the update interval, the check by Docs@Work for updates might be delayed. Internet connectivity is required for Docs@Work to check for Published site updates.

TABLE 4. BACKGROUND NOTIFICATION TYPES FOR PUBLISHED SITES

Notification type	Description	If device user taps on the notification
Single document updates	Only one new or updated file is available in any Published site	Docs@Work will be launched into the foreground and start downloading the new or updated file
Grouped document updates	Multiple files were added or modified in any Published sites	Docs@Work will be launched into the foreground and start downloading the new or updated files.
Please sign / published sites	One of the Published sites requires the user to enter their credentials	Docs@Work will be launched into the foreground, start downloading files and prompt the user for authentication
Published site updates	A new Published site is added by the administrator	Docs@Work will be launched into the foreground, start downloading files for the newly added Published site as well as any newly added or updated files from other Published sites

Changing notification settings

Device users can change the notification settings in Docs@Work.

Procedure

1. Launch Docs@Work.
2. Tap the settings icon.
3. Tap **Notifications**.
4. Use the switch for the notification to either enable or disable the notification.

Importing images and video

Device users can add images and video to Docs@Work from the device. This allows users to upload new images and video to content repositories.

Procedure

1. In **My Files**, tap on **...**.
2. Tap on **Add Media**.
3. From Photos, select the photo you want to add.
4. In the **Add Media** text box, enter a name for the image.
5. Tap on **Add**.
6. The new image is added to **My Files**.
   The user can now Star, Upload, and Rename the image.

Browse and add SharePoint site

Device users can add SharePoint sites by browsing for a SharePoint site in Sites. This reduces the chance for error when a SharePoint site URL is copied and pasted.

Adding a SharePoint site by browsing in Docs@Work

You can add a SharePoint site to Sites.

Before you begin

- You must have the SharePoint site URL.
- If authentication is required, your credentials to access the SharePoint site.

Procedure

1. In Sites, tap to add a site.
2. Enter the SharePoint URL in the browse search box, and tap **Go**.
   The URL should include the http:// or https:// prefix.
   Depending on the authentication requirements, you might be asked to enter your corporate credentials.
3. Tap **Add Site**.
4. Enter a name for the site to appear in Sites.
5. Tap **File View** or **Web View** to set the default view and add the SharePoint site to Sites.
6. Tap **Done** to close the browser.

Single Sign On

Single Sign On (SSO) for Docs@Work is supported. The device user registers with MobileIron Core using Mobile@Work. Then, the device user can use Docs@Work to access content servers without having to enter any further credentials.

To use SSO:

- The content server must support authentication using Kerberos.
- Docs@Work must use the AppTunnel feature, configured so that the Standalone Sentry uses Kerberos Constrained Delegation (KCD) to authenticate the user to the content server.
- The content server must be either a Microsoft SharePoint server or IIS-based WebDAV content repository or Apache-based content repository.
- When you configure the content site in the Docs@Work configuration setting, Authentication must be unchecked.

Support for multiple configurations

Merging of multiple configurations for Docs@Work are supported. You can select Enable merging of configurations option on Core to push multiple configurations to a device as a single configuration. Multiple configurations are merged as follows:

- Content site: The combination of all sites is pushed to the device.
- AppTunnel Rules: The latest modified AppTunnel rule is pushed to the device.
- Custom Configurations: The key-value pairs listed in Custom Configurations get merged and combination of all is pushed to device. If there are different values for same key in different configurations then the last modified configuration gets pushed to the device. For example:

Configuration-1: DISABLE_EDITING=true

Configuration-2: DISABLE_EDITING=false

Allow Drag and Drop from Docs@Work for iOS

You can drag content from Docs@Work for iOS to other AppConnect or third party apps. The drag functionality will work if you have configured data loss prevention (DLP) policies for Docs@Work for iOS. The content can be dragged from Docs@Work to the other apps only when the DLP policy for copy and paste option is set to All apps. For other DLP policy settings for copy and paste, the data cannot be dragged from Docs@Work.

Watermark text

The files and documents that are viewed or edited using Docs@Work are marked with a customized watermark. Any string can be used to create the watermark. Use a user identifying variables as values such as, $USERID$ and $EMAIL$. These values will create watermark strings that are unique to each user.

Other features

Device users can do the following:

- Track changes in .doc and .docx files.

The native Docs@Work editor allows device users to do the following:

- View outline in a PDF.
- View a PDF in full-screen mode in an iPhone.
  The top navigation bar and the bottom tool bar are hidden in full screen mode. Tap the top of the page to turn full-screen mode on and off.
- Search within a PDF.

Using Docs@Work app on a non - compliant device

Using a Docs@Work app on a device that is out of compliance or AppConnect policy is not enabled, then the Docs@Work app should be uninstalled and then reinstalled from MobileIron Apps@Work.