MobileIron Docs@Work 2.14.0 for Android Guide

for MobileIron Core and MobileIron Cloud

February 08, 2021

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

Contents

New features summary

This release introduces the following new features and enhancements:

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

Docs@Work app features and enhancements

This release includes following new app features and enhancements.

- **Modern authentication for SharePoint Online**: The Docs@Work app now supports modern authentication for Microsoft SharePoint Online.

NOTE: SharePoint Online sites will be logged out when the app is updated to Docs@Work 2.14.0.

- **Certificate-based authentication for Microsoft Sharepoint Online**: The Docs@Work app now supports certificate-based authentication for Microsoft SharePoint 365.

Docs@Work administrator features and enhancements

This release includes no new administrator features and enhancements.

Overview of Docs@Work for Android

The following provide an overview of the Docs@Work app for Android devices:

About Docs@Work

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 for Android is available in three flavors, **Android AppConnect, and Android enterprise**.

Docs@Work Android AppConnect

Docs@Work is available as an Android AppConnect app.

AppConnect is a MobileIron feature that containerizes apps to protect data on iOS and Android devices. Each AppConnect-wrapped app becomes a secure container whose data 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 data, such as documents. AppConnect apps are managed using policies configured in a MobileIron Enterprise Mobility Management (EMM) platform. The EMM platform is either MobileIron Core or MobileIron Cloud.

As an AppConnect app, all Email+ data is secured. The app interacts with other apps according to the data loss prevention policies that you specify. You can also take advantage of AppConnect features such as app authorization and app configuration.

Docs@Work for Android AppConnect has the following secure features:

- **Secure apps passcode**: A secure apps passcode, if you require one, gives device users access to all secure apps. This is the AppConnect passcode, which you define in the MobileIron EMM platform. 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 Email+ app data, app configurations, and policies. This means app data is secure even if a device is compromised. App data on the device is encrypted using AES-256 encryption. The encryption key is not stored on the device. It is programmatically derived, in part from the device user's AppConnect passcode, if you require an Appconnect passcode.
- **Data loss prevention**: You determine whether device users can take screen captures of protected data. You also determine whether AppConnect apps can access camera photos or gallery images, and whether they can stream media to media players. You can also specify copy/paste restrictions and a web browser policy.
- **Secure apps data deletion**: If a device is retired, or a secure app is retired, the secure app's data is deleted.

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

Docs@Work for Android enterprise

Docs@Work is available as an Android enterprise app. Email+ for Android enterprise has the following secure features:

- **Data loss prevention**: You determine whether device users can take screen captures of protected data as well as specify if users can copy/paste protected data.
- **Data deletion**: App data is removed from a device for any of the following:
  - The device is retired
  - The app is removed from the label or the app catalog (MobileIron Core)
  - Users are removed from app distribution (MobileIron Cloud)
  - The app is uninstalled from the device

Permissions acquired by Docs@Work

Docs@Work for Android needs the following permissions:

Permission	Description
Docs@Work runtime permissions	
Modify Or Delete The Contents Of Your USB Storage	To save and create enterprise documents.
Read The Contents Of Your USB Storage	To read enterprise documents.

Permission	Description
Docs@Work other permission	
Full network access	Internet access for syncing data.
View Network Connections	To determine network connectivity.
View Wi-Fi Connections	To determine if user is on Wi-Fi or not.
Connect and disconnect from Wi-Fi	Used by test suite to modify Wi-Fi connectivity.
Receive Data from Internet	Required to sync files.

Where to find Docs@Work for Android and Android enterprise

Docs@Work for Android is distributed by administrators through MobileIron Core and Cloud.

Docs@Work for Android enterprise can be downloaded using enterprise PlayStore.

About Docs@Work for Android configuration

Device users can download Docs@Work for Android directly from the Google Play. You can also distribute Docs@Work for Android as a recommended app through Apps@Work.

NOTE: 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 Android devices or available through the AppConnect-enabled apps required for Android devices, you must still create new configurations for deploying the Docs@Work app.
- If you are using the Default AppConnect Global Policy, you do 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.
- Use the Docs@Work configuration to specify:
  - AppTunnel rules
  - content sites
  - Docs@Work app behavior

NOTE: Ensure that only one Docs@Work configuration is applied to a device.

What the users see in Docs@Work for Android

When users launch Docs@Work for Android, they can access the following from the main screen:

- Sites
- My Files
- Recent Files
- Starred
- Offline
- Settings
- Search

Docs@Work app and Docs@Work (Original)

- If you have an existing deployment of the Docs@Work functionality embedded in Mobile@Work for Android devices or available through the AppConnect-enabled apps required for Android devices, you will still have to create new configurations for deploying the Docs@Work app.
- See also End of Support Announcement: Original Docs@Work (April 2, 2015) at https://community.mobileiron.com/docs/DOC-1288

Configuring Docs@Work for Android

The Docs@Work app enables Android users to access, store, view, edit, and annotate documents from content repositories, such as Microsoft SharePoint. MobileIron Cloud 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 sections describe how to set up Docs@Work for Android.

Main steps for configuring Docs@Work for Android AppConnect (Core)

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

Set up app distribution

You can set up app distribution as an in-house app. In addition to Docs@Work, the following apps are required for Docs@Work for Android:

- Secure Apps Manager
- Web@Work
- Email+

The apps must be added to the MobileIron app storefront as in-house apps for distribution. You can download the apps from the software download page on support.mobileiron.com.

- For Docs@Work, go to https://support.mobileiron.com/mi/android-docsatwork/current
- For Secure Apps Manager, go to https://support.mobileiron.com/mi/android-sam/current
- For Web@Work, go to https://support.mobileiron.com/mi/android-browser/current
- For Email+, go to https://support.mobileiron.com/mi/android-email+/current

To distribute the apps as in-house apps:

Procedure

1. In the Admin Portal, go to **Apps > App Catalog**.
2. Select **Android** from the **Select Platform list**.
3. Click **Add+** to open app wizard.
4. Click **In-house**.
5. Click **Browse** and navigate to the AppConnect app (.apk) you want to upload.
6. (Optional) Enter a description for the app.
   MobileIron recommends that you add the following app descriptions:
   - Docs@Work: Docs@Work gives you an intuitive way to access, store, and view documents from content repositories, such as Microsoft SharePoint.

- Secure Apps Manager: Secure Apps Manager works with the Mobile@Work app to secure and manage secure apps on your device.
- Email+: Email+ provides native email client experience with easy setup. It also provides other important emailing features.
- Web@Work: Web@Work is a secure browser that allows your device users to easily and securely access your organization's web content.

7. (Optional) Select a category if you would like to display the app in a specific group of apps on the device.
8. Click **Next**.
9. (Optional) Enter an Override URL if you are implementing an alternate URL for downloading secure apps. The URL must point to the secure app in its alternate location.
10. Click **Next**.
11. Select **App Installation Settings**.
12. Select the Per App VPN settings you created for the app.
13. Click **Finish**.
    The app is displayed in the **App Catalog** with an icon that identifies the app as an in-house app.
14. Select the app in the app catalog.
15. Click **More Actions > Apply To Label**.
16. Select the labels that you want to apply to the app.
17. Click **Apply**.

Related topics

- For more information on adding secure Android apps to the app catalog, see “Managing Mobile apps for Android” in the *Apps@Work Guide*.

Enabling Docs@Work for Android

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.

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**.

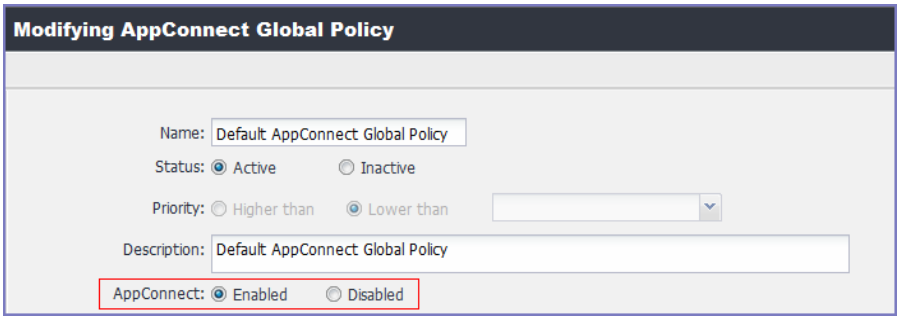
Configuring the AppConnect global policy

Because Docs@Work for (Android or iOS) is an AppConnect app, 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

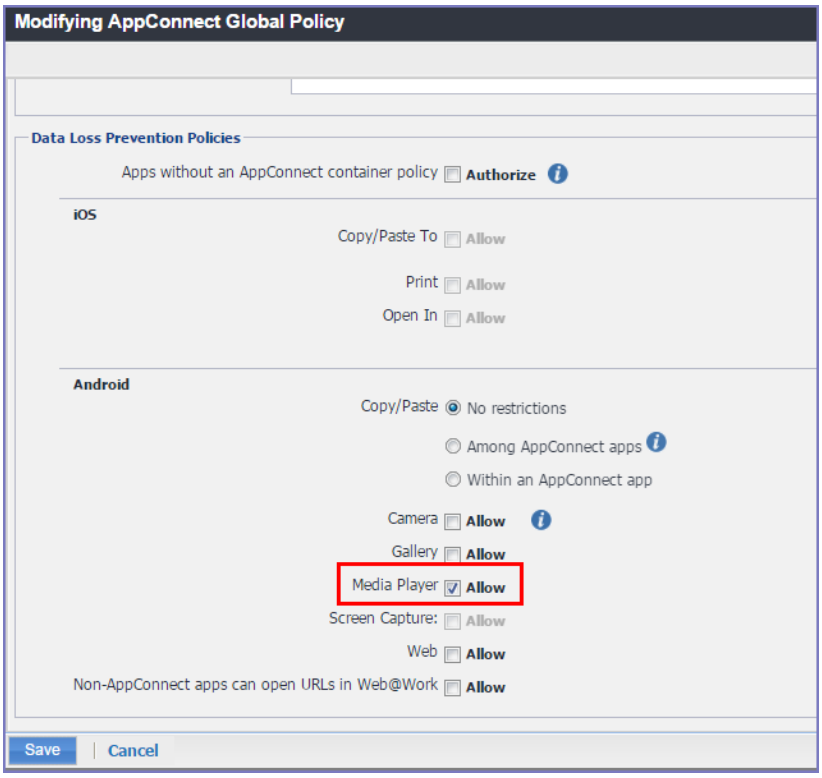
1. In the Admin Portal, go to **Policies & Configs > Policies**.
2. Select **Default AppConnect Global Policy**.



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. Also, ensure that there is a container policy for Web@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 Android.
   If you want to allow device users to play audio and video files in Docs@Work for Android, you must select **Media Player: Allow** checkbox in the **AppConnect Global Policy**.



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.

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 Android.
4. Enter a description for the policy.
5. In the **Application** field, select **Docs@Work**.
6. Select the data loss prevention settings.
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

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 > Docs@Work**.
3. Enter the required information 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**.

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

$EMAIL$
$USERID$
$FIRST_NAME$
$LAST_NAME$
$USER_UPN$
$DISPLAY_NAME$
$USER_CUSTOM1$
$USER_CUSTOM2$
$USER_CUSTOM3$
$USER_CUSTOM4$

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 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*","url":"https://www.box.com","domain":"BoxEnterprise" *Name for the site*: The name is displayed in the Docs@Work app. Example: Acme Company Box

4. Click **Save**.

Device users can also add a Box User site.

NOTE: Android devices support only one Box site. This can either be a Group site or a User site.

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), 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 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*","url":"*valid url for the content repository including port*","domain":"SharePoint", "subDomain":"Federated","priority":"true | false"} NOTE: • Ensure that there are no spaces • Values are case sensitive **Required parameters:** "name", "url", "domain", "subDomain" **Description:** *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. **Example:** {"name":"SharePoint","url":"https:// sharepoint.acme.com","domain":"SharePoint","subDomain":"Federated","priority":"false"}

4. Click **Save**.

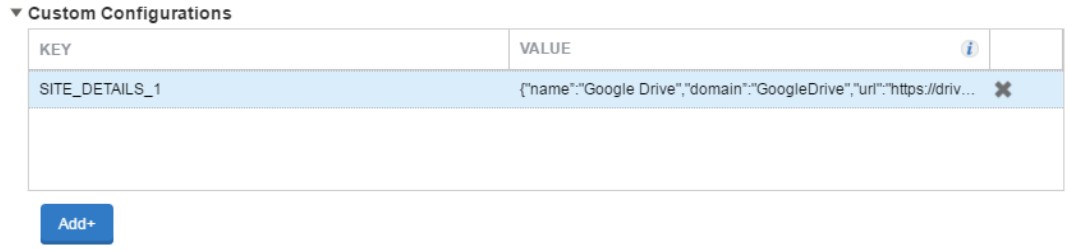
Adding Google Drive as a Group site

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 AUTOFILL_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**.



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**.

While on the subject of tables, the paragraph type p.TableTitleNoNumber allows you to create a table with a title but with not "Table X:". I use this in the Derived Credential Guides to indicate for every task the provider and OS it applies to.

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS <DO NOT USE FOR ANY OTHER BOOK>

Derived credential providers	Entrust
Device platforms	iOS, Android

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.

Adding a SharePoint Group site with certificate-based authentication and derived credentials

Certificate-based authentication with Entrust PIV-D certificates and p12 certificates are supported for SharePoint sites with ADFS.

Note The Following:

- In Android 4.1, 4.2, 4.3 and 4.4 devices, certificate-based authentication related to webview certificate challenge is not supported.
- Certificate-based authentication does not support tunneling.

Procedure

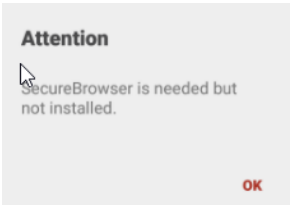
1. In the MobileIron Core Admin Portal, go to **Policies & Configs > Configurations**.
2. Select the Docs@Work configuration to which you want to add a SharePoint.
3. Click **Edit**.
4. Under **Custom Configuration**, click **Add+** to enter the following key-value pair:

Key	Value
IdCertificate_*n* Where *n* is a number 1-100 For example: IdCertificate_1	Select the certificate from the **VALUE** drop-down list. For example: CBACert
IdCertificate_n_host For example: IdCertificate_1_host	Enter the host name for SharePoint site which supports certificate-based authentication. For example: mobileiron.com

5. Click **Save**.

Accessing Google Drive from Docs@Work

With Docs@Work 2.2.0 and later, users might be blocked to access Google Drive sites on Docs@Work. Google does not allow the requests in embedded browsers known as web-views. Docs@Work for Android uses Web@Work as the browser to access Google Drive. If Web@Work is not installed, you might get the following error:

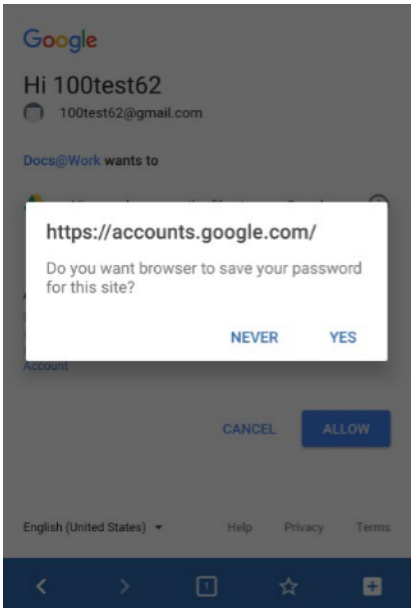


Prerequisites

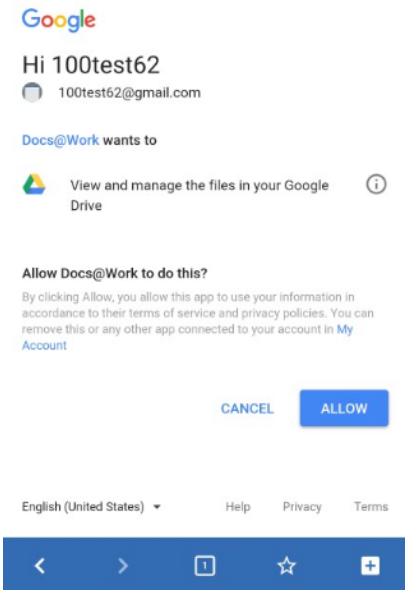
- Verify that you have configured Google Drive as a Group site. See Accessing Google Drive from Docs@Work on page 22.
- Verify that you have installed Web@Work.
- Verify that you have added the custom URL key-value pair for Web@Work.
  Key: custom_url_scheme
  Value: com.mobileiron.orion.android

Procedure

1. Login to Docs@Work on your mobile and click **Sites**.
   Google Drive is available as a group site.
2. Click Google Drive to add or access your account. An alert to allow or deny Web@Work displays.
3. Click **Allow** to continue.
4. Enter your email address to sign in.
5. Click **Next.** An alert to save the password for the site displays.
   You can choose to save the password or click **Never**.



6. Click **Allow** for Docs@Work to access Google Drive.



Docs@Work can now access Google Drive.

Required components for Docs@Work for Android deployment

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

- MobileIron unified endpoint management (UEM) platform: MobileIron Core or MobileIron Cloud.
- Standalone Sentry, with ActiveSync enabled (required if you want to secure access to the ActiveSync server using Standalone Sentry).
- Android devices 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 Android Release Notes*.

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

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.

Prerequisites

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

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

- Verify 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 25.
2. Configure an AppTunnel service for a CIFS repository in Standalone Sentry settings.
   See Configuring an AppTunnel service for DFS on page 25.
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 27.

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. NOTE: MobileIron does not support Kerberos for DFS content servers. Only basic authentication is supported for 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 • if the Service Name is <CIFS_ANY>, you can enter a hostname with wildcards. 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. We recommend 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.

Item	Description
	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, Configuring DFS content site on page 25. 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.

Item	Description
	Web@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 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>.
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

Item	Description
	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 29.

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.

Item	Description
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. 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.

Main steps for configuring Docs@Work for Android AppConnect (Cloud)

Following are the main steps for configuring and deploying Docs@Work for Android AppConnect on MobileIron Cloud:

Adding Docs@Work for Android AppConnect to MobileIron Cloud

You add Docs@Work in the same manner you would add any other Android in-house app. After adding to MobileIron Cloud, you can distribute the app to devices.

Procedure

1. In the MobileIron Cloud, go to **Apps > App Catalog > +Add > In-House**. Add the app just as you would any in-house app.
2. After adding the apps, select the distribution option that includes the users and devices to which you want to make Docs@Work for Android available.
3. Click **Next**. If the app was already in the catalog and you are editing the app, click **Save**.

Next steps

- Configuring Docs@Work for Android AppConnect in MobileIron Cloud on page 35

Related topics

For details on adding in-house apps for Android, see the **MobileIron Cloud Guide** or click on **Help** in MobileIron Cloud.

Configuring Docs@Work for Android AppConnect in MobileIron Cloud

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.)

To configure Docs@Work on MobileIron Cloud follow these steps:

Procedure

1. Edit the Default AppConnect device configuration or create a new one.

NOTE: If the same settings will apply to all user groups and all AppConnect-enabled apps, then you can edit the default configuration. Only one AppConnect device configuration can be applied to a given device and all AppConnect-enabled apps on that device.

2. Add the Docs@Work app to the app catalog.

• Under Advanced Options and App Configuration, provide the following information for each content site you want to display in Docs@Work:

Item	Description
Content Sites	
URL	Enter a URL for the content site. The URL must include http:// or https://. Both domain name and IP address are supported.
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

Item	Description
Authentication	Select if you want the device to authenticate to the server.
Published Site	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 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.

- Provide the following information for the published sites:

Item	Description
Published site	
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.
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.

- Select a device group for app distribution.

3. Add the Key and value for **AppConnect Custom Configuration**, for example: **watermark_text** key-value pair.
4. Add the Key and value for **AppConnect Certificate Configuration**, for example: **signing_certificate_ca_n** key-value pair.

Docs@Work configuration field description for Android (Core and Cloud)

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

TABLE 1. DOCS@WORK CONFIGURATION FIELD DESCRIPTION FOR ANDROID 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. A valid URL must start with http:// or https://. Starting with Core 7.5.1.0, if you are using variables, http:// or https: is not required. However, the entry in the URL fieldmust map to a valid URL that starts with a http://, https://, or smb://. UNC is also supported. Examples: $USER_CUSTOM2$ https://$USER_CUSTOME1$ **CIFs sites** For CIFS sites, the URL must also include the CIFS port. A calid 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 variable 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, " Support for variable in configuration content sites". Example with variable: https://networkdrive/users/
Content Sites	
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://. Startig with Core 7.5.1.0, if you are using variable, http:// or https: is not required. However, the entry in the URL field must map to a valid URL that starts with http://, https://, or smb://. UNC is also supported.

TABLE 1. DOCS@WORK CONFIGURATION FIELD DESCRIPTION FOR ANDROID IN MOBILEIRON CORE AND CLOUD (CONT.)

Item	Description
	Example: $USER_CUSTOM2$ https://$USER_CUSTOM1$ CIFs sites For CIFS sites, the URL must also include the CIFS port. Avalid 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, “Support for variables in configuring content sites”. Examples with variabled: https://networkdrive/users/$FIRST_NAME$ https://sharepoint.mycompany.com/personal/$FIRST_NAME$_$LAST_NBAME$_company_com. **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 might not match with the credentials in OneDrive and may result in failure to access to OneDrive for Business and #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

TABLE 1. DOCS@WORK CONFIGURATION FIELD DESCRIPTION FOR ANDROID IN MOBILEIRON CORE AND CLOUD (CONT.)

Item	Description
	• CIFS: Network Drive • DFS: Network Drive
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 applicable to iOS devices. Does not apply to Android devices.*
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.

TABLE 1. DOCS@WORK CONFIGURATION FIELD DESCRIPTION FOR ANDROID IN MOBILEIRON CORE AND CLOUD (CONT.)

Item	Description
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. 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.

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 Constrained Delegation (KCD).
- Docs@Work must use the AppTunnel feature, configured so that the Standalone Sentry uses 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. MobileIron does not support KCD with CIFS-based content repositories.
- 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 union 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 union 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

Docs@Work app behavior

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.
- 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.
- Autofilling username and domain.

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

Configuring Docs@Work app 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 on **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 46.
5. Click **Save**.

Key-value pairs to configure app behavior

TABLE 2. KEY-VALUE PAIRS TO CONFIGURE APP BEHAVIOR

Key	Value: Enter/Select one	Description and Value
Specifies 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.
Disallow adding some document storages		
blocked_storage_domains	Enter one or more of the following: • Box • Dropbox • Microsoft SharePoint • WebDAV • CIFS	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.
Disallow adding user sites		
disable_user_sites	• true • false	Prevents device users from adding sites to Docs@Work. User added sites will be removed. Documents from User 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	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

Key	Value: Enter/Select one	Description and Value
	are allowed. For example: SharePoint:2, Box:1	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. Example: SharePoint:2; Box:1 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.
Allows sending analytics from Docs@Work to Mixpanel		
allow_ analytics	• true • false	Use the following values to set the key-value pair: • True: Enables sending analytics from Docs@Work to Mixpanel. • False: Disables sending analytics from Docs@Work to Mixpanel. The default value is set to True.
Disables editing, importing, and uploading files		
disable_ editing	• true • false	Disables the following in My Files and all content sites in Docs@Work: • Editing. • Importing images from photo gallery. • Uploading to and deleting files in the backend resource.
Automatically populates the user name for the content site.		
AUTOFIL L_ CREDEN TIALS	Enter parameters for the content site in the following JSON format: {"*URL*": {"domainTyp e":" *DomainType*	*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 directly logged in to the Site from the Sites screen. This feature is applicable for CIFS and WebDAV sites only on MobileIron Core. NOTE: $PASSWORD$ value will be available only when admin enables "Save User Password" in device registration settings on Core and

Key	Value: Enter/Select one	Description and Value
	","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 registered Mobile@Work client after that. Refer to MobileIron Core documentation for its usage. **Examples:** • {"https://sharepoint.miacme.com": {"domainType":"SharePoint","userName":"miacme/$USERID$"},"default":"miacme.com/$USERID$"} • {"https://sharepoint.miacme.com": {"domainType":"SharePoint","userName":"miacme\\$USERID$"},"default":"miacme.com\\$USERID$"} • {"default": "domain/$USERID$"} • {"domainType": "CIFS","userName": "$USERID$","password":"$PASSWORD$"}}

Key	Value: Enter/Select one	Description and Value
	user name can be preceded by either a single forward slash or two back slashes: *Domain*/$USERID$ or *Domain*\\$USERID$ TIP: - Copying and pasting JSON strings may result in invalid JSON. - Validate the JSON	

Key	Value: Enter/Select one	Description and Value
	string. There are many sites, example: jsonlint.com, that will validate the JSON string.	
Displays watermark text on the fies and folders		
watermark_text	Use a user identifying variables as 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.
Displays the title of files and folders in SharePoint		
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.
Sets box metadata cache expiry		
box_metadata_timeout	Default value: 15 minutes	Box metadata for a particular folder is cached whenever response is received from server. This cached metadata expires after timeout and if a new request for metadata

Key	Value: Enter/Select one	Description and Value
		comes for the same folder, it is sent to BOX server. Duration in minutes after which box metadata cache expires.
Allow digital signature for PDF		
signing_ certificate	Certificate	This key allows the admin to add signing certificate which is used for digital signature for PDF forms for Android AppConnect. To enable digital signature add configure signing certificate, add signing_ certificate key and select the signing certificate from drop-down menu. NOTE: Only one signing certificate is supported and it should be in .p12 format. It needs to be added as certificate enrollment configuration.
signing_ certificate_ ca_n	Certificate	This key allows the admin to add multiple Certificate Authorities to trusted CA's. The certificate must be DER-encoded. Where, the value of n can be from 0 to 9. For example: signing_certificate_ca_0, signing_certificate_ca_1
Default viewer for PDF files		
enable_ pspdfkit	True False	This key allows the admin to change default viewer for PDF files. If set to true, this enhances user interface experience and also supports digital signature feature.
Grouping of Offline files		
group_ offline_ files	True False	This key allows files under offline section to be grouped under folder path header. The default value is set to False.
Miscellaneous		
ENABLE_ CIFS_ RETRY_ ON_ SHARIN G_ VIOLATIO N	True False	This key allows the admin to resolve an issue where CIFS would cause a sharing violation error, when you try to open a file which was already opened/updated on desktop.

What users see

Device user experience can be defined based on the key-value pairs the administrator configures.

NOTE: For Android enterprise devices, these features are enabled via configurations in the Docs@Work for Android enterprise app configuration. Key-value pairs are not applicable to Android enterprise devices.

If you configure BLOCKED_STORAGE_DOMAINS:

- If a site type is blocked, any sites of that type will be deleted from Docs@Work. This includes both Group and User sites. Blocked sites can be configured in the Docs@Work configuration on Core; however, the site type will not be pushed to Docs@Work. Device users will not be able to add that site type to Docs@Work.
- 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.

If you configure DISABLE_USER_SITES:

- Device users will not see the option to add sites to Docs@Work.
- User added sites will be removed.
- Documents from User sites marked as Starred, Offline, or in Recents will be removed.

If you configure SUPPORT_EMAIL_ID:

The email address is automatically populated when the device user emails the device logs.

If you configure RESTRICT_NUMBER_OF_USER_SITES:

- If the device user has already added more than the configured number, the latest sites will be deleted. Only the oldest sites up to the number configured will remain.
- If the user tries to add more than the number specified for the site type, an error message is presented.

If you configure DISABLE_EDITING:

Disables editing in My Files and all content sites in Docs@Work.

If you configure AUTOFILL_CREDENTIALS:

The user name is automatically populated for that content site. The device user can replace the auto-filled user name with a different user name and sign in to the content site. For Google Drive sites, however, the device user can only sign in with the auto-filled user name.

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:

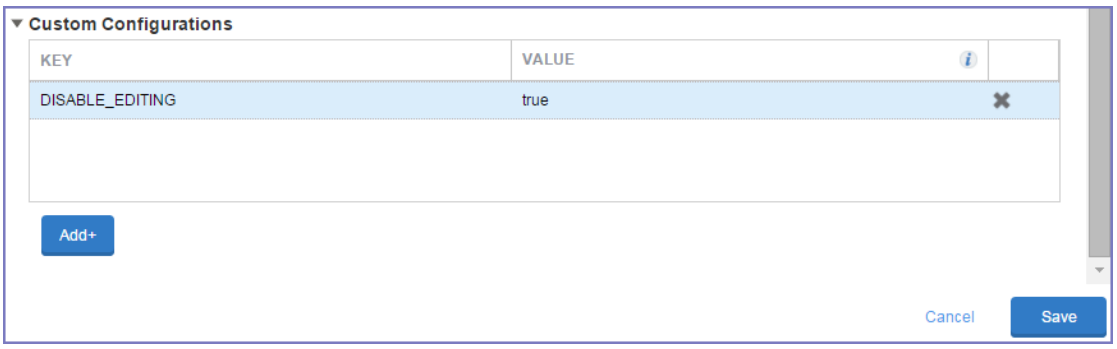
- Editing.
- Importing images from photo gallery.
- Uploading to and deleting files in the backend resource.

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 the **Edit** button.



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.**

Configuring Docs@Work for Android enterprise

The following sections describe how to configure Docs@Work for Android enterprise:

- Overview of configuration tasks on MobileIron Core
- Configuring CIFS content site for Android enterprise mode with Core
- Configuring CIFS content site for Android enterprise mode with Cloud
- Docs@Work configuration field description for Android enterprise (Core and Cloud)

Before you begin

- MobileIron Core should be set up for Android enterprise. For more information, see the *MobileIron Core Device Management Guide for Android and Android enterprise Devices*.
- Tunnel for Android enterprise should be set up and devices should be enrolled with Android enterprise with Tunnel. For more information, see How to Set Up App VPN with MobileIron Tunnel for Android Guide for Administrators.
- CIFS site access requires AppTunnel rule to be configured in Android enterprise mode. For all other sites, device users must enable MobileIron Tunnel before using Docs@Work to access corporate resources.

Limitations

The following are limitations of Docs@Work for Android enterprise:

- Only one Docs@Work app configuration for Android enterprise can be configured per MobileIron Core. You cannot have multiple Docs@Work configurations assigned to different labels.
- Access to DFS repositories is not supported.
- Access through Standalone Sentry is supported for CIFS sites with Docs@Work 2.3.
- Cert-based auth for SharePoint is not supported.

Overview of configuration tasks on MobileIron Core

These configuration tasks are performed in the MobileIron Core Admin Portal:

- Adding and configuring Docs@Work for Android enterprise on page 57
- Generating Group and Published site configuration on page 57

Adding and configuring Docs@Work for Android enterprise

Upload the MobileIron Docs@Work for Android enterprise app to MobileIron Core from Google Play and configure content sites to make it available to Android enterprise devices.

To add and configure Docs@Work for Android enterprise:

1. In the MobileIron Core Admin Portal, go to **Apps > App Catalog**.
2. Click **Add+**.
3. Click **Google Play**.
4. For **Application Name**, enter Docs@Work for Android enterprise.
5. Click **Search**.
6. Select the line for Docs@Work for Android enterprise.
   Do not select the Docs@Work for Android enterprise preview app.
7. Click **Next**.
8. Select "5.0" for **Min. OS Version.**
9. Click **Next**.
10. Select **Install this app for Android enterprise**.
    You may need to scroll down to see the option. Additional fields are then displayed.
11. Use the following table to set up the **Configurations** section:

12. Click **Finish**.
13. Apply the Docs@Work for Android enterprise app to the appropriate labels to distribute the app to Android enterprise devices.

Generating Group and Published site configuration

MobileIron recommends generating a valid JSON with the Configuration Tool. This ensures that a valid JSON is configured in the Docs@Work for Android enterprise app configuration.

To generate valid JSON configuration for a content site:

1. Complete the Docs@Work for Android enterprise configuration without Group Site and Published Site configuration and apply to an Android enterprise device.
2. In Docs@Work for Android enterprise, go to Settings > Configuration Tool.
3. Click on the "+" icon to configure a content site.
4. Configure the Site Name, URL, including type of site (SharePoint or WebDAV), Sub domain, Authentication, Published Site, and Web View.
5. Add additional sites as needed.
6. Click on the upload icon at top of the screen to export the file.
7. Email the file to an email account from where it can be copied and pasted into the **Groups Sites** and **Published Site Config** fields.

Configuring CIFS content site for Android enterprise mode with Core

Common Internet File System (CIFS) allows administrators to access group shared folders located on different servers by transparently connecting them to one or more CIFS name spaces. New Components in the JSON file:

- Sentry hostname
- Sentry port
- Domain pattern
- Sentry service

Configuring AppTunnel Rules in Sentry on MobileIron Core

Before you configure CIFS in Android enterprise mode, you need to configure AppTunnel rule in Sentry:

1. In the Admin Portal, go to Services > Sentry.
2. Edit the entry for the Standalone Sentry that supports AppTunnel.
3. Select the Enable AppTunnel option in the edit Standalone Sentry window.
4. In the AppTunnel Configuration section:
   - Select **CIFS_ANY** in the service name.
   - Select pass through and Kerberos from the drop-down menu.

Configuring CIFS content site on MobileIron Core

1. In the MobileIron Core Admin Portal, go to **Apps > Add +**.
2. Select Google Play and import the Docs@Work app from Google Play store.

NOTE: After completing the import in the docs@work, configure the app restrictions.

3. Select **App catalog> edit> configuration choices**:
   - Enter the **Device UUID** value as $DEVICE_UUID$.
   - Enter the **User ID** value as $USERID$.
   - Enter **Group Site Configuration**, for example CIFS group site configuration:

Configuration	JSON
For **Basic Authentication**	[{"auth":"","domain":"CIFS","name":"CIFS-Site","priority":"false","subDomain":"NetworkDrive","url":"https://cifs.company.com:445","webView":"false"}]
For **Kerberos Authentication**	[{"auth":"NoAuthn","domain":"CIFS","name":"CIFS-Site","priority":"false","subDomain":"NetworkDrive","url":"https://cifs.company.com:445","webView":"false"}]

   - Enter **AppTunnel rules** in JSON array format, for example: [{"sentryHostName":"https://sentry.company.com", "sentryPort":"443",

"sentryService":"CIFS_1", "domainPattern":["cifs.company.com"]},
{"sentryHostName":"https://sentry.company.com", "sentryPort":"443",
"sentryService":"SERV_2", "domainPattern":["sharepoint.company.com"]}]
where;
sentryHostName: Standalone Sentry URL that you want to tunnel the sites URL listed in group site.
sentryPort: Sentry Tunnel port. Use port 443.
domainPattern:Content server's hostname. For example: finance.yourcomany.com or hostname with wildcards. The wildcard character is *. For example: ***.yourcompany.com**.
sentryService: The service name is used in the Docs@Work configuration for setting up tunnelling to the content repository.
.

4. Click **Save**.

Configuring digital signatures for PDF files in MobileIron Core

1. In the MobileIron Core Admin Portal, go to **Apps > Add +**.
2. Select **Google Play** and import the Docs@Work app from Google Play store.After completing the import in the docs@work, configure the app restrictions.
3. In app restrictions options, for signing certificate:
   - Enter Signing Certificate alias, for example: $CERT_ALIAS:LOCAL$ This is the certificate alias set up in the MobileIron Core.
   Where;
   $CERT_ALIAS:$; Is the **Certificate Enrollment** setting configured in the MobileIron Core user interface for the devices. For example: $CERT_ALIAS:scepIdentityCert$, where;
   scepIdentityCert is the name of the SCEP configured in Core.
4. Click **Save**.

Configuring CIFS content site for Android enterprise mode with Cloud

Common Internet File System (CIFS) allows administrators to access group shared folders located on different servers by transparently connecting them to one or more CIFS name spaces on MobileIron Cloud.

Configuring SCEP Identity Certificate and Sentry Profile

To configure SCEP Identity Certificate and Sentry Profile on MobileIron Cloud perform the following steps:

1. In MobileIron Cloud, go to **Admin> Infrastructure > Add Certificate Authority**. See*, Configuring authentication using SCEP Identity (MobileIron Cloud only)* section in the *MobileIron Sentry Guide for MobileIron Cloud* guide.
2. Go to **Admin> Infrastructure >** Create a Sentry Profile for ActiveSync. See, *Configuring Standalone Sentry for ActiveSync* section in the *MobileIron Sentry Guide for MobileIron Cloud* guide

Configuring CIFS content site on MobileIron Cloud

1. In the MobileIron Cloud Admin Portal, go to **Apps > App Catalog.> Add +**.
2. Select **Google Play**, search and import the Docs@Work app.

NOTE: After completing the import in the docs@work, configure the app restrictions.

3. Add Docs@Work app to App Catalog as Enterprise app.
4. Delegate the app to the targeted audience.
5. Select **Apps >App Catalog > Docs@Work** app.
6. Click **App Configuration** tab, select **Managed Configuration for Android** and edit configuration choice.

Configuration	Value
User ID	${userUID}
Group Sites	[{"auth":"","domain":"CIFS","name":"CIFSSite"," priority":"false","subDomain":"NetworkDrive","url":"https:// cifs.company.com:445","webView":"false"}]
AppTunnel Rule	Enter **AppTunnel rules** in JSON array format, for example: [{"sentryHostName":"https://sentry.company.com", "sentryPort":"443", "sentryService":"CIFS_1", "domainPattern":["cifs.company.com"]}, {"sentryHostName":"https://sentry.company.com", "sentryPort":"443", "sentryService":"SERV_2", "domainPattern": ["sharepoint.company.com"]}]

Configuration	Value
	Where: **sentryHostName**: Standalone Sentry URL that you want to tunnel the sites URL listed in group site. **sentryPort**: Sentry Tunnel port. Use port 443. **domainPattern**: Content server's hostname. For example finance.yourcompany.com or hostname with wildcards. The wildcard character is *. For example: *.yourcompanyname.com. **sentryService**: The Service name is used in the Docs@Work configuration for setting up tunnelling to the content repository.
Identity Certificate	Drop - down which is auto populated with SCEP Identity Created while configuring sentry profile.

7. Click **Update**.

Configuring digital signatures for PDF files in MobileIron Cloud

1. In the MobileIron Cloud Admin Portal, go to Apps > App Catalog > Add +.
2. Select Google Play, search and import the Docs@Work app

NOTE: After completing the import in the docs@work, configure the app restrictions.

3. Add Docs@Work app to App Catalog as Enterprise app.
4. Delegate the app to the targeted audience.
5. Select Apps > App Catalog > Docs@Work app.
6. Click App Configuration tab, select Managed Configuration for Android and edit configuration choice.

Configuring	Value
Signing Certificate	Drop down which is auto populated with certificate aliases after certificate enrollment is done.

Docs@Work configuration field description for Android enterprise (Core and Cloud)

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

TABLE 3. DOCS@WORK CONFIGURATION FIELD DESCRIPTION FOR ANDROID ENTERPRISE IN MOBILEIRON CORE AND CLOUD

Item	Description
Silently Install	Select to automatically install the app when the device checks in.
Auto Update this App	Select to automatically update the app when a new version is available.
Configurations	
Device UUID	Enter $DEVICE_UUID$ for the MobileIron Core.
User ID	Enter $USERID$ for MobileIron Core. Enter ${userUIDLocalPart} for MobileIron Cloud.
Group Sites	Enter content site configuration in JSON format. See Generating Group and Published site configuration on page 57 to generate and copy and paste the configuration. Example: [{"name":"averailserver02","url":"https://averailserver02.corp.averail.com","domain":"SharePoint","subDomain":"Corporate","webView":"false","priority":"false"}, {"name":"webdav06 ", "url": "http://averailserver06.corp.averail.com","domain":"WebDAV", "subDomain":"CloudStorage"}] Not applicable for Content Security Service mode.
Published Sites Config	Enter content site configuration in JSON format: See Generating Group and Published site configuration on page 57 to generate and copy and paste the configuration. Example: {"interval";180, "wifi";true, "skipFiles"; 500,"maxDocs";50}

Item	Description
	Not applicable for Content Security Service mode.
Log Level	Select one of the following options to specify the level of detail for logs: • DEBUG: Includes debug level information for application flow and to 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. Not applicable for Content Security Service mode.
Support Email Id	Enter a valid email address. The email address is automatically populated when the device user emails the device logs.
Blocked Storage Domains	Enter one or more of the following to block device users from adding the content site to Docs@Work: • Box • Dropbox • Microsoft SharePoint • WebDAV Enter the values as a semicolon (;) separated list. Example: Box;Dropbox Microsoft SharePoint includes Office 365 SharePoint sites. Not applicable for Content Security Service mode.
User Sites Restrictions	Enter the site type and number in the following format to restrict the number of User sites that a device user can add: Site type1:number; Site type2:number. Valid entries for site type are: SharePoint, Box, Dropbox, WebDAV. Number is a positive integer greater than 0. Example: SharePoint:2; Box:1 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. 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 configuration is ignored if **Disable User Sites** is true. Not applicable for Content Security Service mode.
Disable User	Enter **true** to prevent device users from adding sites to Docs@Work. Not applicable for Content Security Service mode.

Item	Description
Sites	
Disable Editing	Enter **true** to disable editing of documents in Docs@Work. 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.
Auto-fill Credentials Config	Enter parameters for the content site in the following JSON format: {"*URL*":{"domainType": "*DomainType*","userName":"$USERID$"}, "default":"*Domain*/$USERID$"} **Note the following 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$ **Tips** - Copying and pasting JSON strings may result in invalid JSON. - Validate the JSON string. There are many sites, example: jsonlint.com, that will validate the JSON string. **Description:** *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. *Domain*: Enter the domain name to which the username defaults if the username for the URL cannot be resolved. Variables are not supported. **Examples:** • {"https://sharepoint.miacme.com": {"domainType":"SharePoint","userName":"miacme/$USERID$"},"default":"miacme.com/$USERID$"} • {"https://sharepoint.miacme.com": {"domainType":"SharePoint","userName":"miacme\\$USERID$"},"default":"miacme.com\\$USERID$"} • {"default": "domain/$USERID$"}
Allow usage statistics	Allows sending analytics from Docs@Work to Mixpanel. Use the following values to set the key-value pair: • True: Enables sending analytics from Docs@Work to Mixpanel. • False: Disables sending analytics from Docs@Work to Mixpanel. The default value is True.
Show title	Displays user friendly title for files and folders in Sharepoint. To enable SHOW_TITLE, select the check box. The check box is unchecked by default.

Item	Description
Watermark	Displays a diagonal watermark text (provided by the administrator).
Box Metadata Cache Expiry	Sets box metadata cache expiry in minutes. Default value is 15 minutes. Enter the desired integer value to be configured for this timeout.
AppTunnel rule	When Docs@Work app tries to connect to a CIFS, WebDAV or SharePoint site configured in Group sites, the Sentry creates a tunnel to the server. AppTunnel Rule indicates which requests should be tunnelled.
Identity certificate	Select the Certificate or the SCEP profile that you created for devices to present to the Standalone Sentry that supports app tunneling.
Enable PSPDFKit	Enables the use of PSPDFKit for viewing and annotating PDF documents. This check box is checked by default.
Signing certificate	Enter the signing certificate alias like $CERT_ALIAS:<cert_name>$ for Core and choose the certificate from drop-down menu for Cloud
Group Offline file	Allows files under offline section to be grouped under folder path header. The check box is unchecked by default.
Allow non-media files	Allow non-media file types to be viewed using other apps. It takes a wildcard character (*) or a comma separated list of extensions. For example: dwg, svg file extensions.

What users see

The Docs@Work app for Android behaves similarly to the Docs@Work app for Android enterprise. For information on how to use the Docs@Work app, see Working with Docs@Work on page 67.

Working with Docs@Work

This section describes how to use the following features with Docs@Work app.

Content sites

Content sites configured by the administrator are automatically available in Docs@Work 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. 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 tap the sync button.
  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. Sites that a user adds are identified as User sites.

Site details are available by tapping the three vertical dots next to the site.

Offline

When you mark a document as offline, the document is downloaded and available for offline. If changes are made to the document on the content site, the updated version of the document becomes available only when the device user launches the content site containing the document. 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.

Starred

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

User added sites

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

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

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

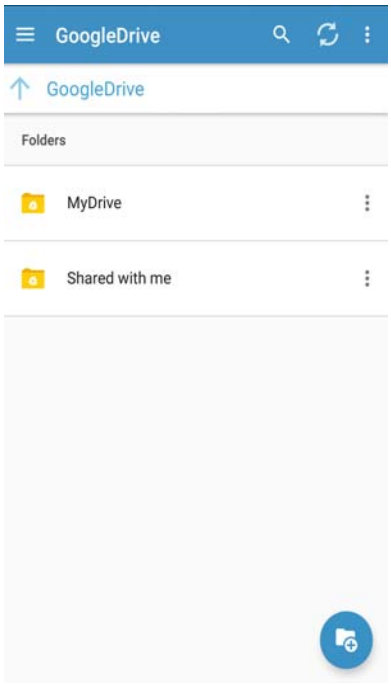
- **The site's URL.** The URL must include http:// or https://. Both domain name and IP address are supported.
- **Type of Authentication for Network drives.** The authentication setting is labeled **No Authentication**. Device users should enable this setting, if the site does not require authentication 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 setup 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).

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, favorite, edit, and annotate 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 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. For Android, the feature is supported with Email+.

The **Email a link** option is available in the listing pages.

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	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 Android, a secure email client. Example: Email+.

Sharing documents from Docs@Work for Android

The Share option is available in the listing pages.

Procedure

1. Tap the three vertical dots next to the document.
2. Tap Share. The document is downloaded and attached to a new email message in a secure email client.

- The recipient does not need Docs@Work to open the document.
- The attached document can only be opened in another secure app, such as Docs@Work.
- The Email option in Docs@Work for Android cannot be turned off.

Users can view and edit document attachments directly from a secure email app, without having to first save the attachment to My Files.

For Email+ clients, users have to first tap Save. They can then tap View to view and edit the file directly from Email+.

Emailing documents from Docs@Work for Android

The **Email** option is available in the listing pages.

To email a document:

1. Tap the three vertical dots next to the document.
2. Tap **Email**.
   The document is downloaded and attached to a new email message in a secure email client.

NOTE:

- The recipient does not need Docs@Work to open the document.
- The attached document can only be opened in another secure app, such as Docs@Work.
- The **Email** option in Docs@Work for Android cannot be turned off.

Users can view and edit document attachments directly from a secure email app, without having to first save the attachment to **My Files**.

For Email+ clients, users have to first tap **Save**. They can then tap **View** to view and edit the file directly from Email+.

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 an Email

Docs@Work can add attachments when you compose an email from Email+ or any other email client. The number and size of files that you attach to an email is at the discretion of the email client - for example, AppConnect

Android AppConnect Email+ and Android enterprise Email+ allows multiple file attachments. You can select multiple files to add as attachments.

Accessing Google Drive from Docs@Work

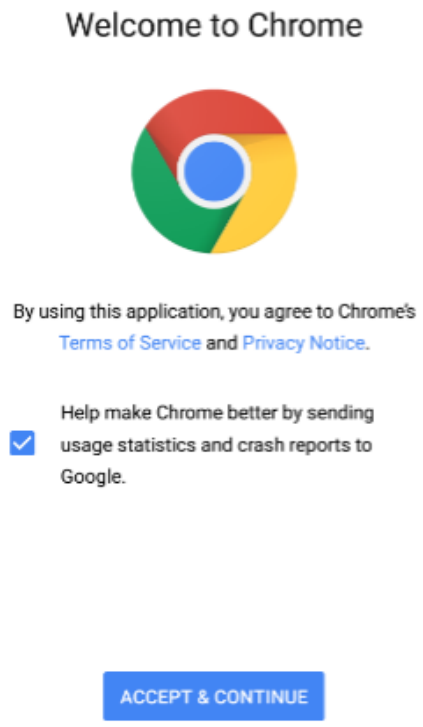
With Docs@Work 2.2.0 and later, users might be blocked to access new Google Drive sites on Docs@Work. Google does not allow the requests in embedded browsers known as web-views. Docs@Work for Android enterprise uses Google Chrome as the browser to access Google Drive.

Prerequisites

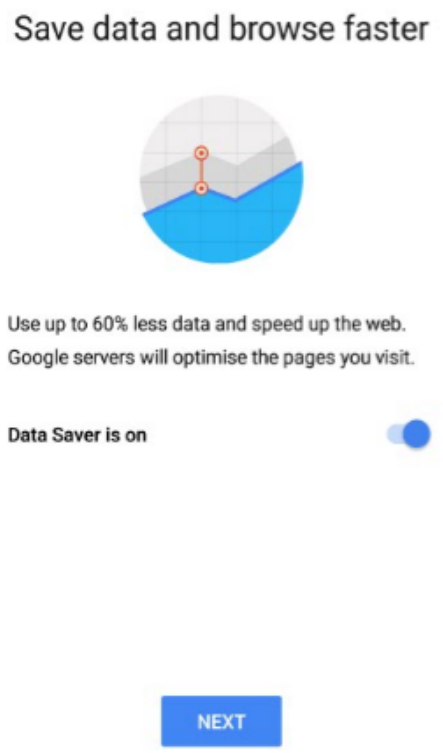
- Verify that you have installed Google Chrome.

Procedure

1. Login to Docs@Work on your mobile and click **Sites**.
   Google Drive is available as a group site.
2. Click **Google Drive** to add or access your account. The Chrome welcome screen displays.

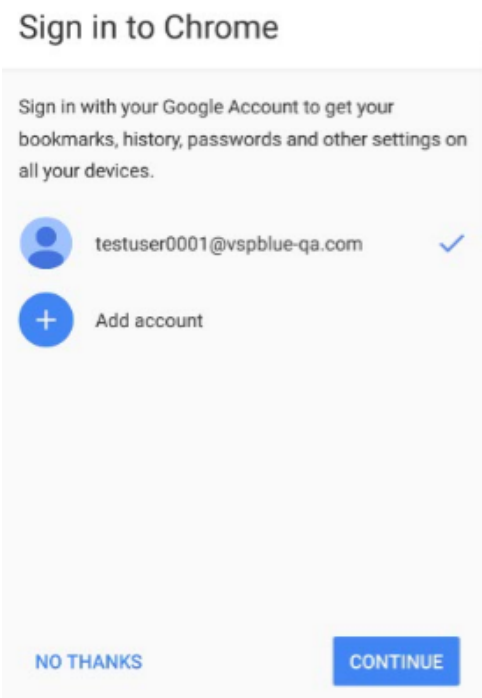


3. Click **Accept & Continue**. The data save screen displays. Click the toggle button to turn on the data saver.

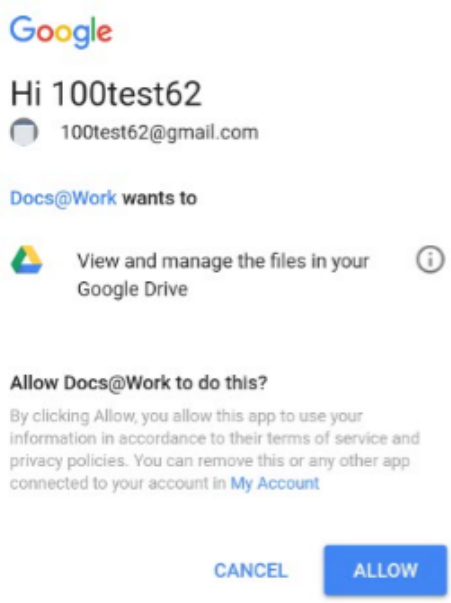


4. On the Sign in to Chrome window, select **NO THANKS** to open the Google screen. OR
   To add another account, click **Add Account**.

NOTE: If you have signed into Google Chrome with different account and choose to sign-in with another account, you must sign-out from the first account. Else, the authentication flow is broken and Docs@Work might not be able to access Google Drive.



5. On the Google account screen, click **Allow** to let Docs@Work access Google Drive.



6. Docs@Work can now access Google Drive.

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. 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.

Editing and annotating documents in Docs@Work for Android

To edit a document:

1. Tap the three vertical dots adjacent to the file.
2. Tap **Edit and Save** or **Edit and Save As**.
   The edit options are only available if you can edit the document type.
   The **Edit and Save As** option is available only if you are editing the document directly from a content repository.
   If you selected **Edit and Save As**, when you back out of edit view, you are presented with options for saving or downloading the file.
3. Select one of the options to save the changes.

Option	Description
Save file to current location	Select, then tap **OK** to save the edited file to the same location.
Save file to a different location	Select, then tap **OK** to specify a different location to save the edited file. The file in the original location is not changed.
Download to My Files	Select, then tap **OK** to download the edited file to **My Files**. The file in the original location is not changed.

Extracting files from .zip files

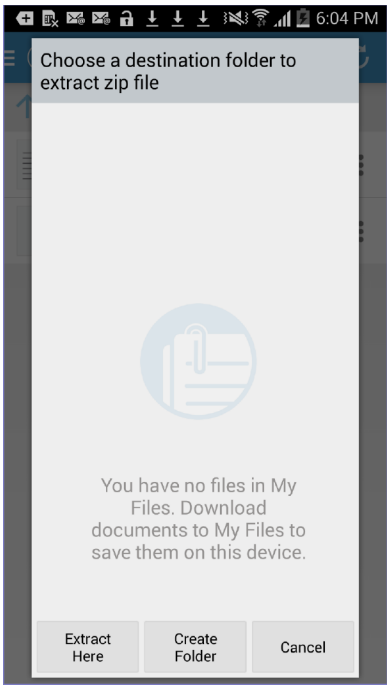
Only .zip compressed files and password protected .zip files are supported. Other types of compressed files, such as gzip, .tar files, are not supported.

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

Procedure

1. Tap on the .zip file.

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.



2. Tap **Extract Here**.
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** 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

Device users can add a new folder, document, note, presentation, spreadsheet, and media. You can also move, share, upload files to a site, rename, and delete folders in **My Files**. Folder creation in **My Files** has been available in previous versions of Docs@Work for Android.

NOTE: If **Allow Documents to be edited** is disabled in a Site Policy in Content Security Service, then file and folder creation will be disabled in Docs@Work. Devices users cannot upload or create files or folders in Published sites.

Creating files and folders in My Files

To create files and folders in **My Files**.

Procedure

1. In Docs@Work, tap **My Files**.
2. Tap on the (+) icon.
3. Tap **Folder** to create a new folder or tap one of the document types to create a new file. Tap **Media** to import image and media files.

Renaming files and folders in My Files

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

Procedure

1. In Docs@Work, tap **My Files**.
2. Tap the three vertical dots next to the file or folder.
3. Tap **Rename File** to rename the file.
   For a folder, tap **Rename Folder** from the folder options.
4. Enter a new name for the file or folder and tap **Rename**.

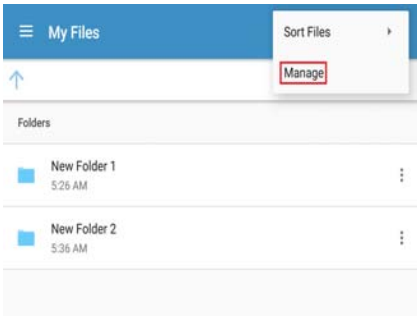
Moving files and folders in My Files

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

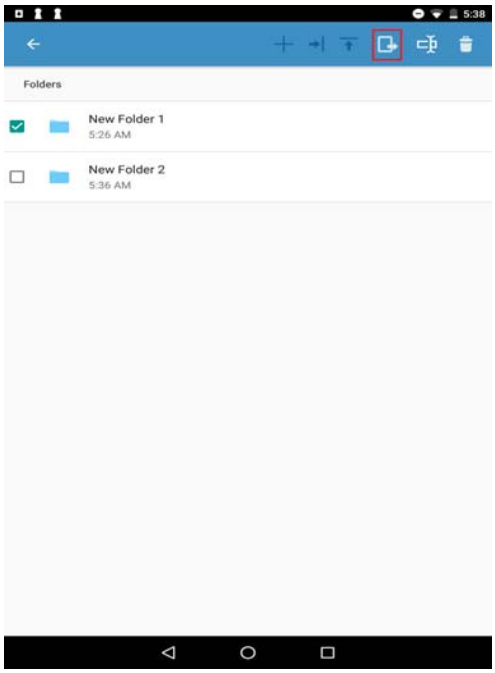
Procedure

1. In Docs@Work, tap **My Files**.
2. Tap the three vertical dots at the top of the screen, then tap **Manage**.

NOTE: Device users can also tap the three vertical dots next to a file to move that file.



3. Select the files and folder to move, then tap the move icon  . Device users can select multiple files or folders to move.



4. Tap a folder, or tap **Create Folder**, or tap **Move Here** to move the selected files and folders to a different location.

Locating files or folders

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

The **Locate** function does not display if the device user is in the same folder or location on Docs@Work 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.

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

Procedure

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

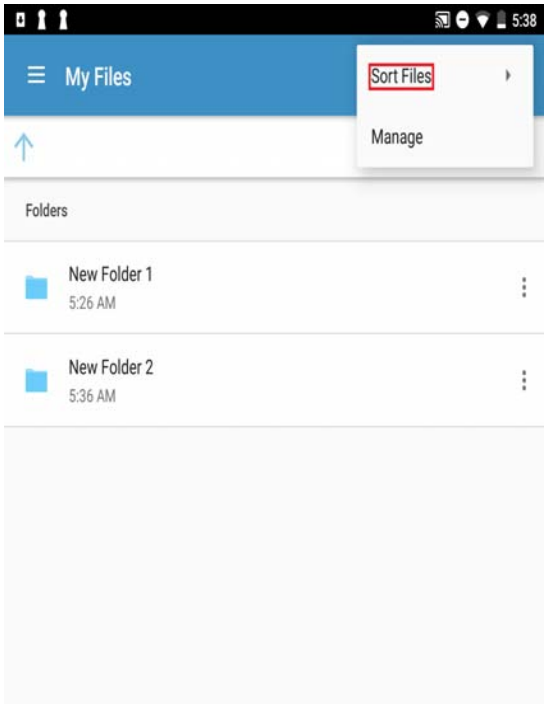
Device users can sort files and folders by the following methods:

- Name
- Date Created
- Last modified
- Last opened

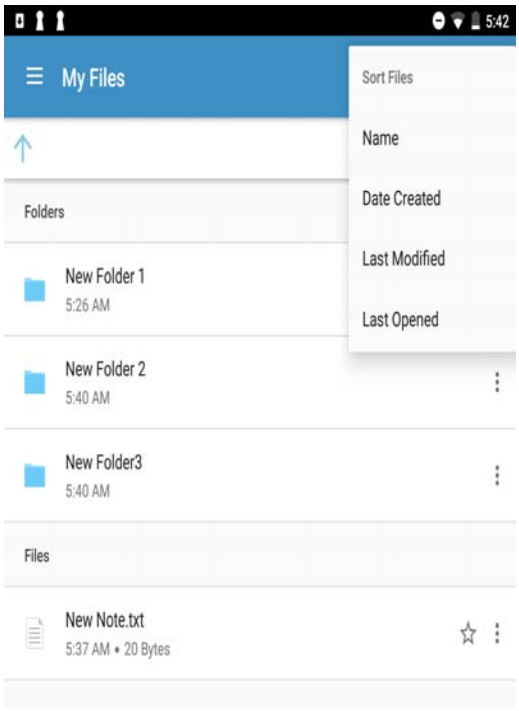
To sort files or folders in My Files.

Procedure

1. In Docs@Work, tap on the overflow menu.



2. Tap on Sort Files option.
3. Select the method to sort from the Sort Files menu.



Show title

Displays the title of files and folders in SharePoint.

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.

The watermark text is not supported for image files. The following message is displayed for image when watermark is enabled:

Image viewing is not supported when watermark is enabled.

Import images

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.

NOTE: Gallery must be set to Allow in the AppConnect policy to allows users to access the photo gallery.

To add images from the device to Docs@Work.

Procedure

Playing audio or video files

Docs@Work supports media playback. However, a media player is not embedded inside the Docs@Work application and has to be enabled separately as follows:

- In AppConnect-enabled Docs@Work, a media file can be played only if Media Player is allowed in the AppConnect Global Policy. This allows media files to be played outside the secure container using the system media player.
- In Android enterprise-enabled Docs@Work, the media file is rendered using a third-party media player application. Therefore, a media player application must be included in App Catalog. Android enterprise-enabled Docs@Work has been tested with the 'VLC for Android' media player application.

To play audio or video files

1. In Docs@Work, navigate to the content site where the file resides.
2. Tap on the file to view the video or listen to the audio file.

Digital signature for PDF files

Docs@Work supports digital signatures for PDF files. Once a digital signature is added to a PDF form, it cannot be deleted.

Opening non-media file extensions

Docs@Work allows files to be opened using third-party apps in Android enterprise mode. To open a non-media file, add wildcard character (*) or file extensions with comma separated values (for example: dwg, svg) to **Allow non-media files** configuration.

Other features

Devices users can also do the following:

- Track changes in .doc and .docx files.
- Add, edit, and delete bookmarks to a PDF.
- Search within a PDF.
- Choose between scrolling continuously or scrolling page by page. Device users can make the selection in Docs@Work settings.