MobileIron FilePass 1.5.0 for iOS Guide

for MobileIron Core and MobileIron Cloud

February 18, 2021

For FilePass product documentation:
MobileIron FilePass for iOS Product

Contents

New feature summary

This release introduces the following new features and enhancements:

- FilePass app new features and enhancements
- FilePass administrator features and enhancements

FilePass app new features and enhancements

This release introduces the following new feature and enhancement.

- **FilePass supports-certificate based authorization**: FilePass now supports certificate-based authentication (CBA) using ADFS along with username and password authorization to ADFS.
- **Support for Swedish language enabled**: FilePass now supports Swedish language. See the *Language support* section under the *MobileIron FilePass 1.5.0 for iOS Release Notes*.

FilePass administrator features and enhancements

This release introduces the following new administrator features and enhancements.

- **New key value pair added**: New KVP **IdCertificate_1** and **IdCertificate_1_host** added to enable certificate-based authentiation (CBA). For more information on certificate-based authentication, see Configuring certificate-based authentication for FilePass.

FilePass for iOS Overview

FilePass enables users to share documents securely between MobileIron apps (Docs@Work and Email+) and Microsoft Intune MAM-protected Office 365 apps, while retaining identity coherency. The FilePass app honors Intune App Protection policies just like any app with Intune MAM.

When FilePass is enabled in Docs@Work and Email+ configuration, you can share docs between MobileIron apps and Intune-enabled Microsoft Office 365 managed apps such as Microsoft Word, Microsoft OneDrive, Microsoft OneNote, and so on.

FilePass is an AppConnect and Intune-enabled app, which means that it is containerized to protect the content on iOS devices. As an AppConnect app, all FilePass content is secure.

FilePass translates documents from MobileIron AppConnect container to Microsoft Intune container and vice-versa.

Where to find FilePass

You can download FilePass for iOS from the Apple App Store. You can also distribute FilePass for iOS as a recommended app through Apps@Work.

About FilePass for iOS configuration

- If you are using the Default AppConnect Global Policy, you may not need to create a new policy. If ApConnect Global policy is not used, see the *FilePass for iOS Overview* section for details.
- Configuring an AppConnect container policy is required only if you did not select Authorize for Apps without an AppConnect container policy in the AppConnect Global policy.

NOTE: The Core client (Mobile@Work) or the Cloud client (MobileIron Go) must be available on the device and registered with the server before installing the FilePass app.

Required components for FilePass for iOS deployment

- MobileIron Enterprise Mobility Management (EMM) platform: MobileIron Core or MobileIron Cloud.
- An iOS device that is registered with a MobileIron EMM.
- MobileIron client: Mobile@Work for MobileIron Core deployments; MobileIron Go for MobileIron Cloud deployments.

- MobileIron Docs@Work or Email+ apps.
- Microsoft Intune apps such as Microsoft OneDrive, Microsoft OneNote, and so on.

NOTE: FilePass is supported on Docs@Work from version 2.10.0 and higher and Email from version 3.9.0 and higher.

NOTE: FilePass tries to access the following URLs during Microsoft Intune enrollment:
- login.windows.net
- login.microsoftonline.com
- vortex.data.microsoft.com

Main steps for configuring FilePass for iOS (Core)

Configuration for FilePass is done in MobileIron Core. The following sections detail the process.

- Configuring FilePass app configuration policy
- Configuring an AppConnect container policy
- Configuring FilePass on Docs@Work or Email+ on MobileIron Core

Configuring FilePass app configuration policy

The following describe the steps to configure FilePass on MobileIron Core.

Procedure

1. In MobileIron Core Admin Portal, go to **Policy & Configs > Configurations**.
2. Click **Add New > AppConnect > App Configuration**.
3. Enter name for the configuration.
4. Enter description for the configuration.
5. Enter Application to **com.mobileiron.ios.filepass**.
6. Scroll down to **App-specific Configurations** section.
7. Click Add+ to enter the following key-value pairs:

Key	Description
filepass_key_identifier	The value for this is a string used to derive Cipher keys which is used to encrypt and decrypt files (using AC SDK) through FilePass app. **Value:** Enter a unique and complex alphanumeric string in the value field. The value for this key-value pair needs to be same for the all the supported MobileIron Apps (Docs@Work, Email+, and FilePass) participating in file sharing. NOTE: If Filepass_key_identifier does not have same values across FilePass app and Docs@Work then: - Importing files from Office apps to Docs@Work will fail. - Sharing files from Docs@Work to Microsoft Office apps using FilePass will fail.
username	The value for this key-value pair is used to login and enroll to Microsoft Azure portal. **Value:** $EMAIL$ is recommended for MobileIron Core Enter a user identifying user name variable for enrolling to Microsoft Azure Portal.

8. Click **Save**.
9. Select the **FilePass** configuration.
10. Click **Actions > Apply to Label**.
11. Select the appropriate labels to which you want to apply the configuration.
12. Click **Apply**.

Next steps

Configuring an AppConnect container policy

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.

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.

NOTE: Ensure that only one FilePass 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 FilePass container policy for iOS.
4. Enter a description for the policy.

5. Enter **Application** field to **com.mobileiron.ios.filepass**.
6. Select **Save**.
7. Select the **FilePass** container policy.
8. Click **More Actions > Apply To Label**.
9. Select the appropriate labels to which you want to apply this policy.
10. Click **Apply**.

Next steps

Configuring FilePass on Docs@Work or Email+ on MobileIron Core

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 FilePass on Docs@Work or Email+ on MobileIron Core

The following describe the steps to configure FilePass on Docs@Work and Email+ on MobileIron Core.

Procedure

1. In MobileIron Core Admin Portal, go to **Policy & Configs > Configurations**.
2. Select the Docs@Work or Email+ configuration, click **Edit**.
3. Scroll down to **Custom Configurations** section.
4. Click **Add+** to enter **filepass_key_identifier** key-value pair and its value.
5. Click **Save**.

For more information on configuring KVPs, see Configuring FilePass app configuration policysection.

Main steps for configuring FilePass for iOS (Cloud)

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

- Configuring FilePass for iOS on MobileIron Cloud
- Configuring FilePass for Docs@Work or Email+ for iOS on MobileIron Cloud

Configuring FilePass for iOS on MobileIron Cloud

The following describe the steps to configure FilePass on MobileIron Cloud:

Procedure

1. In MobileIron Cloud, go to **Apps > App Catalog > +Add >** search for FilePass in App Store.
2. Make any updates as necessary and click Next. You can change the category and add a description.
3. Choose a **App Delegation** option and click **Next**.
4. Choose a **Distribution** option for the app and click **Next**.
5. Update the default install settings or add install settings as necessary.
6. Scroll down to **AppConnect Custom Configuration**, click **+**.
7. Perform the following steps:
   a. Enter a **name** for the configuration.
   b. Click **Add+** to enter the following keys for AppConnect Custom Configuration:

Key	Description
filepass_ key_ identifier	The value for this is a string used to derive Cipher keys which is used to encrypt and decrypt files (using AC SDK) through FilePass app. **Value:** Enter a unique and complex alphanumeric string in the value field. The value for this key-value pair needs to be same for the all the supported MobileIron Apps (Docs@Work, Email+, and FilePass) participating in file sharing. NOTE: If Filepass_key_identifier does not have same values across FilePass app and Docs@Work then: - Importing files from Office apps to Docs@Work will fail. - Sharing files from Docs@Work to Microsoft Office apps using FilePass will fail.
username	The value for this key-value pair is used to login and enroll to Microsoft Azure portal. **Value:** **${userEmailAddress}** is recommended for MobileIron Cloud. Enter a user identifying user name variable for enrolling to Microsoft Azure Portal.

   c. Select a **Distribution** option for the configuration.
8. Click **Done**

The configuration is distributed to the subset of the devices to which the app is distributed.

Next steps

Configuring FilePass for Docs@Work or Email+ for iOS on MobileIron Cloud

Configuring FilePass for Docs@Work or Email+ for iOS on MobileIron Cloud

The following describe the steps to configure FilePass for Docs@Work and Email+:

Procedure

1. In the MobileIron Cloud Admin portal, **Apps >App catalog > Docs@Work configuration**.
2. Edit the Docs@Work or Email+ configuration.
3. Select **App Configuration > AppConnect Custom Configuration**.
4. Click **+Add**, enter FilePass key and value.
5. Click **Save**.

Configuring FilePass on Microsoft Intune

To enable sharing of documents between MobileIron apps and Microsoft Intune, enroll FilePass to Microsoft Intune and get App Protection policies. The following steps describe how to create **App protection policies** for FilePass on Microsoft Intune.

Procedure

1. Login as admin to https://portal.azure.com.
2. In the **Microsoft Azure** portal page, select **Home**.
3. Click on **See all (+100)** to list all the Azure services.
4. Scroll down to **Intune** section, or in the **All services** field search for **Intune**.
5. In the **Intune** section, select **Intune App Protection**.
6. In the **Client apps** page, go to **Manage > App protection policies > Create policy**.
7. In the **Create policy** section, update the following fields with the values mentioned in the table:

Field	Option	Values
Platform	Not applicable	iOS
Target to all app types	Not applicable	Yes
Apps	Select required apps > + More apps > Bundle ID	1. Enter the following bundle ID: **com.mobileiron.ios.filepass** 2. Click **Add** 3. Click **Select**
Settings	Data protection > Data Transfer	-

Field	Option	Values
Data Transfer	Send Org data to other apps	Select Policy managed apps from the drop-down list.
	Select apps to exempt	For this option two apps need to be added: 1. Click **Select**, enter the following: - For Docs@Work deployment, type in: Name: **Docs@Work** Value: **acextensionsupport** - For Email+ deployment, type in: Name: **Email+** Value: **email+launcher** **Note**: The values are case sensitive. 2. Click **OK**. 3. Repeat step 1, to add another Exempt app: Name: **ACSchema** Value: **appconnect** 4. Repeat step 1, to add another Exempt app: Name: **AppStationSchema** Value: **alt-appconnect** 5. Click **OK**.
	Receive data from other apps	Select All apps with incoming Org data from the drop-down list.

8. See the Microsoft documentation for details on how to create a new policy.

Configuring certificate-based authentication for FilePass

To enable certificate-based authentication (CBA) on FilePass, configure the following KVPs on MobileIron Core:

Key	Description
filepass_key_identifier	The value for this is a string used to derive Cipher keys which is used to encrypt and decrypt files (using AC SDK) through FilePass app. **Value:** Enter a unique and complex alphanumeric string in the value field. The value for this key-value pair needs to be same for the all the supported MobileIron Apps (Docs@Work, Email+, and FilePass) participating in file sharing. NOTE: If Filepass_key_identifier does not have same values across FilePass app and Docs@Work then: - Importing files from Office apps to Docs@Work will fail. - Sharing files from Docs@Work to Microsoft Office apps using FilePass will fail.
username	The value for this key-value pair is used to login and enroll to Microsoft Azure portal. **Value:** $EMAIL$ is recommended for MobileIron Core Enter a user identifying user name variable for enrolling to Microsoft Azure Portal.
IdCertificate_<number>	Name of the certificate enrollment that corresponds to the user certificate.
IdCertificate_<number>_host	URL for the ADFS to which the certificate will be presented. Example: myhost.mycompany.com

For more information on configuring KVPs, see Configuring certificate-based authentication for FilePass and Main steps for configuring FilePass for iOS (Cloud) sections.

For CBA, FilePass app on the device connects to FilePass Auth Azure application which requires admin approval. User is prompted to request approval for FilePass Auth Azure application, if not already granted by the admin. Admin can grant tenant-wide permission to FilePass Auth Azure application by one of the following ways:

- **Admin consent**: This allows the admins to securely grant access to the applications that need admin approval. Login to FilePass using admin account and provide consent by clicking Accept (recommended). For more information see, Enable admin consent workflow.

- **Approval request**: The users can request admin approval for an application that they are unauthorized to consent. The admin logs in Azure portal and approves the requests from the users. For more information on how to get admin consent through user request, see User request admin consent.
- **URL based approval**: The admin directly granting permission FilePass Auth Azure application using the URL. All users will be able to use the application without additional approvals.
  URL similar to the following is displayed:

```
https://login.microsoftonline.com/{tenant-id}/adminconsent?client_id=e8174e3d-c579-4575-bf20-afe069315bdf
```

  For more information on how to grant tenant-wide admin consent to an application, see Grant admin consent.