Using AeroFS with MobileIron

Oct 20, 2014
Proprietary and Confidential
Do Not Distribute

Overview

"*Compared to previous solutions, there is no contest. AeroFS is much easier to use and share with.*"
-- Stephanie So, Operations Manager at Centre for Global eHealth Innovation

AeroFS empowers employees to sync and share files without the use of public cloud servers. Files are shared directly between users and the file transfer is blazing fast. AeroFS uses a familiar user experience that is currently available in consumer-based file sharing products, and as a result no training is required. And unlike most file-syncing cloud software, files are not stored on 3rd party servers. Sensitive corporate files remain safely stored and secured by existing IT security protocols. Employees can share confidential or sensitive data without compromising security.

App's bundle ID: com.aerofs.ios.mobileiron

Android package name: forgepond.com.aerofs.android.mobileiron

Files are never stored on AeroFS servers

Your files are never stored on AeroFS servers. AeroFS enables you to share and collaborate while keeping full control over your data, even when sharing with your customers, vendors, and partners.

Fast Syncing

With AeroFS's Smart Routing technology you can sync data at 80-90mb/s inside your LAN. AeroFS shares files using the fastest possible transport available. Other file sharing tools require files to be transmitted through either public cloud servers or file servers, which creates a single point of failure and hampers scalability. Why send files to a corporate server when users are sitting next to each other?

Familiar User Experience

Private file sharing tools are difficult to use. AeroFS provides the same convenience as the most popular public cloud sharing tools. Employees

can sync and share files directly from their desktops and their mobile devices. Files changes are automatically detected and synced with other devices and users.

App availability

If you are first time customer, please signup at https://privatecloud.aerofs.com/request_signup

Once AeroFS is set up, you can download AeroFS for MobileIron in 2 ways:

- Administrators can download the app through their admin web interface at https://privatecloud.aerofs.com on the Dashboard page.

- Employees can download AeroFS for MobileIron directly on Apple App Store and Google Play Store.

Device compatibility

- iOS: AeroFS for MobileIron is compatible with iOS 7 and onwards.

- Android: AeroFS for MobileIron is compatible with Android 4.2 and onwards.

AppTunnel support

In order for you to configure AeroFS for MobileIron, you need to have an AeroFS appliance running first. At set up, this appliance is configured with a customer specific URL such as share.example.com.

AeroFS for MobileIron needs to communicate with the following servers:

- share.example.com:4433

Data loss prevention policy support (iOS SDK apps only)

We support the open in, pasteboard, and print policies; however the app does not display system actions like copy and print on iOS 8+ because of an issue in iOS. Therefore, the pasteboard and print policy will have no effect on devices running iOS 8+, they will always act as if it were disabled.

Secure file I/O support (iOS SDK apps only)

Our iOS SDK app uses secure file I/O when storing its sensitive data on the device.

AppConnect and non-AppConnect mode support (iOS SDK apps only)

Though the iOS App supports AppConnect and non-AppConnect mode, we recommend any customers that are not using AppConnect mode to use "AeroFS" from the app store instead of the MobileIron version.

Additional sections

Running AeroFS requires the installation of the AeroFS appliance. To request the appliance, please sign up at
https://privatecloud.aerofs.com/request_signup

User features

For employees, AeroFS provides:

- File Syncing: sync files fast and seamlessly on desktop and mobile.
- File Sharing: share files with co-workers by adding their email address.
- Link Sharing: share a file or folder by creating a link.
- Version History: look at previous versions and recover files.

More information at https://www.aerofs.com/product/simple-experience/

For Administrators, AeroFS provides:

- Central Administration: manage your employees, sharing permissions and devices.
- Auditing: audit account, file, device and sharing events.
- Data Loss Protection: manage and remote wipe lost/stolen devices.
- LDAP/AD Integration

For more information

- Request a trial: https://privatecloud.aerofs.com/request_signup
- Contact Sales: 1-800-656-2376
- AeroFS homepage: https://www.aerofs.com/

Configuration tasks

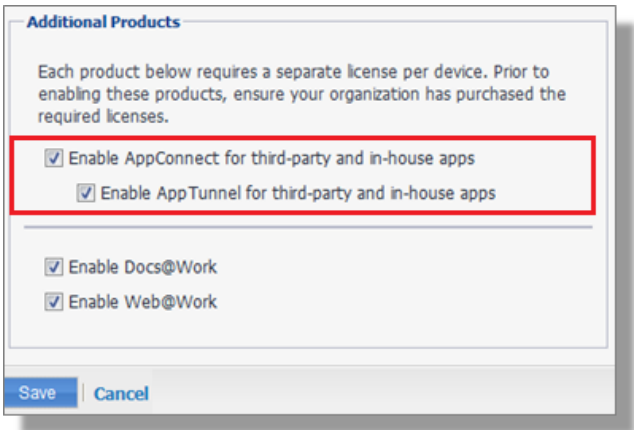
Use the following high-level steps to configure AppConnect for the app.

1. Enable AppConnect.
2. Configure an AppConnect global policy.
3. Configure a new AppConnect app configuration for the app.
4. Configure a new AppConnect container policy for the app.

Enable AppConnect

Before enabling AppConnect on your VSP, confirm that your organization has purchased the required AppConnect licenses. Contact your MobileIron representative if you require additional details on AppConnect license purchases.

To enable AppConnect and AppTunnel functionality on the VSP, navigate to the Settings page on the VSP Admin Portal and check the boxes as shown below.



1. Select the option for "Enable AppConnect for third-party and in-house apps".
2. Select the option of "Enable AppTunnel for third-party and in-house apps".

Configure an AppConnect global policy

An AppConnect global policy configures the security settings for all AppConnect apps, including:

- Whether AppConnect is enabled for the devices that the policy is applied to
- AppConnect passcode requirements.

Note: The AppConnect passcode is not the same as the device passcode.

- out-of-contact timeouts
- the app check-in interval

  Note: The app check-in interval is independent of the MDM check-in timer and controls, and apps cannot be forced to check-in before the interval expires. The recommended configuration for the app check-in interval is 60 minutes.

- the default end-user message for when an app is not authorized by default
- whether AppConnect apps with no AppConnect container policy are authorized by default
- data loss prevention settings

To modify an existing AppConnect global policy:

1. On the VSP Admin Portal, go to Policies & Configs > Policies.
2. Select an AppConnect global policy.
3. Click Edit.
4. Edit the AppConnect global policy based on your requirements.

   See the AppConnect chapter of the VSP Administration Guide for details about each field.

Configure a new AppConnect app configuration

The AppConnect app configuration defines the app-specific parameters that are automatically pushed down to the app, as well as configurations for establishing and authenticating an AppTunnel associated with the app. See the AppConnect chapter of the VSP Administration Guide for details about each field.

Also, for more on AppTunnel configuration, see "Adding AppTunnel Support" in the AppConnect chapter of the VSP Administration Guide.

Use the following steps to configure the app-specific configuration:

1. On the VSP Admin Portal, go to Apps > Configurations > Add New > AppConnect > Configuration.
2. Edit the AppConnect app configuration with the Name, Description, Application, AppTunnel configuration including the identity certificate, and App-specific key-value pair configurations required for the app.

Note: For the Application field, choose an application from the app distribution library, or for iOS apps, specify the iOS bundle ID. You can find the bundle ID by going to Apps > App Distribution Library, and clicking to edit the app. The field Inventory Apps displays the bundle ID in parenthesis.

3. AppTunnel: Click on the "+" button and enter the AppTunnel details. The AppTunnel service for this app must be pre-configured in order to use it here.

4. App Specific Configuration: Click on the "+" button to enter the key-value pair information.

Configure a new AppConnect container policy

An AppConnect container policy specifies data loss protection policies for the app. The AppConnect container policy is required for an app to be authorized unless the AppConnect global policy allows apps without a container policy to be authorized. Such apps get their data loss protection policies from the AppConnect global policy.

Details about each field are in the AppConnect chapter of the VSP Administration Guide.

To configure an AppConnect container policy:

1. On the VSP Admin Portal, go to Policies & Configs > Configurations > Add New > AppConnect > Container Policy.

2. Enter the Name, Description, and Application.

   Note: For the Application field, choose an application from the app distribution library, or for iOS apps, specify the iOS bundle ID. You can find the bundle ID by going to Apps > App Distribution Library, and clicking to edit the app. The field Inventory Apps displays the bundle ID in parenthesis.

3. Configure the data loss protection policies according to your requirements.