Using WorkSite with MobileIron

November 3, 2014
Proprietary and Confidential
Do Not Distribute

Overview

The WorkSite 2 Mobility for ME app for iOS allows you to access your WorkSite documents and emails from anywhere, enabling mobile professionals to be productive in and out of the office. Designed especially to take advantage of iOS's unique interface and portability, WorkSite 2 Mobility for ME allows users to browse, search, view, edit, and upload content within WorkSite

Bundle identifier: com.autonomy.worksite2mobileiron

App availability

The application is available from within the App Store, and is named "WorkSite 2 Mobility for ME."

Device compatibility

The version in the App Store is compatible with iOS 8.

App-specific configuration

Key	Description	Default if the key-value pair is not configured
AllowEmailForwarding	If set NO, disables sending documents via. email	YES

AppTunnel support

WorkSite 2 Mobility for ME has no special setup for AppTunnel.

Data loss prevention policy support (iOS SDK apps only)

WorkSite 2 Mobility for ME supports

- the pasteboard DLP policy
- the print DLP policy
- the Open In DLP policy>

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

WorkSite 2 Mobility for ME uses the Secure File I/O system for all file data contained by the application. It does not encrypt the database. Filenames do not contain sensitive data except for extensions.

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

This application requires AppConnect to be configured. Other versions of the application do not.

Additional sections

Requirements:

To use WorkSite 2.n for Mobility ME, the following are required: n

- Apple iPhone 4, 4S or 5 is required for the WorkSite 2.n for Mobility ME client.
- iOS 7.1 or later is required for the WorkSite 2.n or later client.
- WorkSite Mobility Server for iOS 8.5 SP1 Update 6 or later or 9.0 Update 6 or later is required.

For more information on installing the iOS for server releases, please see the *WorkSite Mobility Server for iOS 9.0 or 8.5 SP1 Installation and Administration Guide, Revision 9*.

User features

<u>Audit History</u>

WorkSite 2 maintains an audit history in the DMS for all actions listed in Table 1.

Table 1 Actions included in Audit History

Object	Actions	Audit Status	Application
Documents and Email	View	Export, View	Mobility2Service
	Print (added to audit history only if item prints successfully)	Print	Mobility2Service
	Open in 3rd Party application	Open	Mobility2Service
Documents	Email document	Mail	Mobility2Service
	Email Link to latest version	Mail	Mobility2Service
	Email Link to current version	Mail	Mobility2Service
Email	Send Email	Mail	Mobility2Service
	Reply, Reply All, Forward	Export	Mobility2Service
	Email Link to latest version	Mail	Mobility2Service
	Email Link to current version	Mail	Mobility2Service
Document Uploading	Create New Document	Create	iOS
	Create New Version	Create version	iOS
	Replace Original	Checkout, Checkin	iOS

Authentication Options

SSL (Secure Sockets Layer) for Secure Communication

WorkSite 2.n for Mobility ME supports the following security and authentication options: SSL is an industry-standard form of secure web communications. It is widely used for securing Internet traffic—every bank and shopping website uses SSL. In the WorkSite 2.n for Mobility ME client, SSL is now a configurable option for Explicit and Trusted authentication. With SSL enabled, all data, including passwords, is encrypted when it is sent to the WorkSite Server and returned to the user's device.

HP Autonomy strongly recommends that SSL always be enabled. Self-signed SSL certificates are not accepted when users connect to WorkSite at https:// sites. Properly-signed SSL certificates have the following requirements:

- The DNS name of the WorkSite Mobility Server must exactly match the name on the SSL certificate.
- The certificate must not be expired.

- The Certificate Authority (CA) for the certificate must be valid and well-known. Self-signed or otherwise invalid SSL certificates will be rejected, and the WorkSite 2.n for Mobility ME client application will refuse connection.

Please see the *WorkSite Mobility Server for iOS 8.5 SP1* or *9.0 Administration Guide, Revision 9* for more details.

IIS (Internet Information Services) Active Directory Service Authentication

IIS, also used by the WorkSite Web application, is a configurable option in WorkSite 2.n for Mobility ME. When the WorkSite Mobility Server is configured for IIS Basic Authentication, it is the IIS server that authenticates users. In this case the WorkSite 2.n for Mobility ME application should be configured as **Trusted** with **IIS** selected. When the WorkSite Mobility Server is configured for WorkSite Authentication (Explicit or Trusted) the user is authenticated in the WorkSite Mobility Server. In this case the application should be configured either for **Trusted** with **IIS** turned off or for **Explicit** login.

- **IIS Basic Authentication Off.** The web service is secured with Active Directory authentication. Basic Authentication is not used.
- **IIS Basic Authentication On.** The web service is secured with Active Directory authentication. Basic authentication is also used (challenge/ response).

Options **IIS On** and **IIS Off** both provide security. Please note that when SSL is turned off, passwords are not encrypted. Using SSL is always recommended when possible.

RSA Single Sign-on

RSA Single Sign-on is a configurable option in WorkSite 2.n for Mobility ME. When RSA authentication is set on the WorkSite Mobility Server, RSA users can log on using the real-time passcode on their RSA SecurID token.

Client Security Features Set Globally on the WorkSite Mobility Server

Several security options set on the WorkSite Mobility Server for iOS can be enforced globally on the WorkSite client. Please refer to the *WorkSite Mobility Server for IOS 9.0 and 8.5 SP1 Installation and Administration Guide* for more details on applying these policies on your WorkSite Mobility Server. Several of these policies cannot be enforced on WorkSite 2.n for Mobility ME because MobileIron provides a more restrictive policy. For example, because MobileIron automatically authenticates the user on WorkSite 2.n for Mobility ME using Mobile@Work credentials, all WorkSite policies related to PIN or Passphrase requirements are not enforced.

- **Prevent Data Leakage.** This policy enables WorkSite Mobility Server administrators to enforce restrictions on users of WorkSite client to prevent them from exposing content. When set, users will not be able to copy, cut or paste data from

an open file to the clipboard, and Print, Email and Export Document actions are disabled. NRLs may still be emailed.

- **Enable Uploads.** This WorkSite Mobility Server policy is set to True by default for full functionality in the WorkSite client. When set to False, any user running WorkSite 2.n for Mobility ME is not allowed to see the Upload dialog and, consequently, is not allowed to upload documents to the WorkSite DMS. If a user attempts to open a document in the Uploads list, a message notifies the user that uploading is disabled. The document remains visible in the Uploads folder, but it will not be uploaded to the WorkSite Server. For more information on the security of the iOS Server, please see the *WorkSite Mobility Server for iOS Installation and Administration Guide*.

For more information

For your information, please refer to the various documents discussed above, available to WorkSite customers via the customer support site.

Configuration tasks

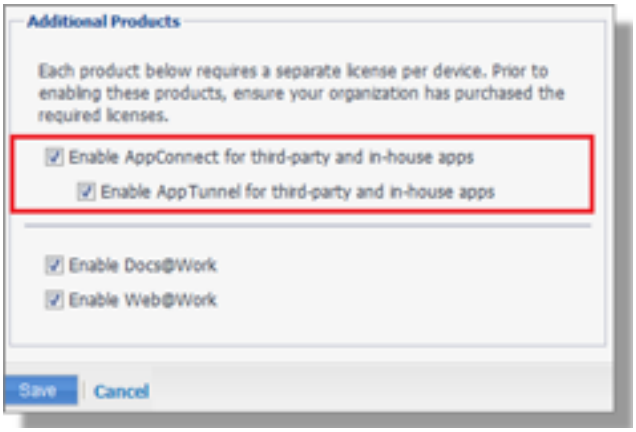
Use the following high-level steps to configure AppConnect for the app.

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 de-fault
- 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.