Using Notate with MobileIron

February 29, 2016
Proprietary and Confidential
Do Not Distribute

Overview

Notate is the Secure Evernote Alternative. All of your notes and tasks remain secured within your own network. No additional servers are required. Start by mobilizing your user's Outlook notes and [1]tasks. Users can access and edit their notes securely from mobile devices. Next expand beyond basic function-ality by using Notate to capture rich data while mobile including handwriting, meeting audio, photos, web clippings and more.

Application Bundle ID: com.shafersystems.notate.pro

App availability

If you are a first time customer, please sign up at:

http://notateapp.com/notate-pro.html

Once Notate is set up, you can download Notate for MobileIron from the Apple App Store:

https://itunes.apple.com/us/app/notate-for-mobileiron/id794060913?mt=8

Notate for desktop computers can be downloaded from:

http://notateapp.com/notate-for-desktops.html

Device compatibility

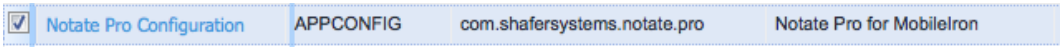
- iOS: Notate for MobileIron is compatible with iOS 7 and above.
- Windows: Notate is compatible with Windows 7 and above.
- Mac: Notate is compatible with Mac OS X version 10.8 and above.

Notate License Key

The first step in set-up is to add the Notate license key in the App-specific configurations. This key is emailed to the Admin assigned to the Notate account. The key should be copied and pasted into section "licensingKey" in the App-specific configuration. Notate synchronization and sharing will not operate without this key. If your key is lost of misplaced contact:

support@shafersystems.com

The App-specific configuration



NOTE: Boolean values should be set to 1 for True and 0 for False.

Key	Description	Default Value
licensingKey	Allows for synchronization and sharing and Notate policy controls from the MobileIron admin portal.	`FHA9bGiNQ1sdEC53PrUYs+jsCm6ksi`
autodiscoveryURLs	Note: This setting is NOT required if your autodiscovery URLs are in standard locations. Server URLs are separated with a semicolon and no space. URL example: http://autodiscover.domain.com/autodiscover/autodiscover.xml; https://domain.com/autodiscover/autodiscover.svc	
exchangeURL	Allows user to synchronize notes with Exchange server. Note:This setting is NOT required unless autodiscovery is not possible for your environment.	https://server.domain.com/EWS/Exchange.asmx

userEmail	If provided, the user won't be asked to provide their email address.	$EMAIL$
userName	If provided, the user won't be asked to provide their username.	$USERID$
userPassword	If provided, the user won't be asked to provide their password. To utilize, you need enable the "Save User Password" option under CORE>Settings>Preference page	$PASS-WORD$
disablePeerVerification	Enables the user of local/private certifi-cates on the Exchange Server	0
enableKerberos	Use Kerberos authentication instead of user credentials for Exchange access.	0
allowiOSEmail	A value of 0 disables use of sending notes with native iOS email. Open In with Email + is still supported.	1
allowAnnotations	Allows the use of handwriting and high-lighter tools.	1
annotationCompression	Handwriting and Annotations are com-pressed by default to save storage space. Values are: 2 = high compression, 3 = medium compression, 4 = no compres-sion	2
allowGeotag	User is permitted to automatically record location of notes.	1
allowHyperlinks	Allows hyperlinks to be active within notes. Safari browser is launched.	1
allowGallery	Allows the acces and use of the device photo/image gallery	1
allowVoiceRecordings	Permit the use of audio recordings	1
allowCamera	Allows the user to insert photos from the device camera into notes	1

allowWebClippings	Allow users to insert web clippings into notes.	1
allowSharing	Allow users to share notebooks with other users.	1
allowAttachments	Allow users to insert documents into notes.	1
allowCrashReports	Enable generic crash reports without user data to be sent to the developer.	1
allowTasks	Allow users to manage tasks in Notate.	1

AppTunnel support

Notate interacts with your organization's Exchange server using EWS over the secure AppTunnel.

A typical EWS connection will use a URL similar to:

https://exchange_server.yourdomain.com/EWS/Exchange.asmx

The address of your exchange server's EWS connection should be provided in the application configuration as described above.

Data loss prevention policy support (iOS SDK apps only)

Notate supports the following DLP policies:

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

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

Notate utilizes native iOS encryption for file I/O.

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

Notate for MobileIron is designed to work only in AppConnect mode.

User features

Save Everything

Collect everything that matters, knowing that you will always be able to find it.

- Handwritten meeting notes
- Audio recordings
- Annotated web clippings
- Business cards and receipts
- Photos and more

Plan to be Productive

Organize tasks to help manage your week. Share tasks with other team members.

- Tasks
- Reminders
- Projects

Get Things Done Faster

Let the team share the workload or assign tasks to individuals. Harness team knowledge with shared notebooks.

- Team Projects
- Team Notebooks

Better for Business

From meeting notes to research papers, Notate keeps *your* ideas on *your* network. Always available, always secure.

For more information

- Request a Trial: http://notateapp.com/notate-pro.html
- Contact Sales: sales@shafersystems.com
- Notate Homepage: http://notateapp.com
- Support: support@shafersystems.com

Configuration tasks

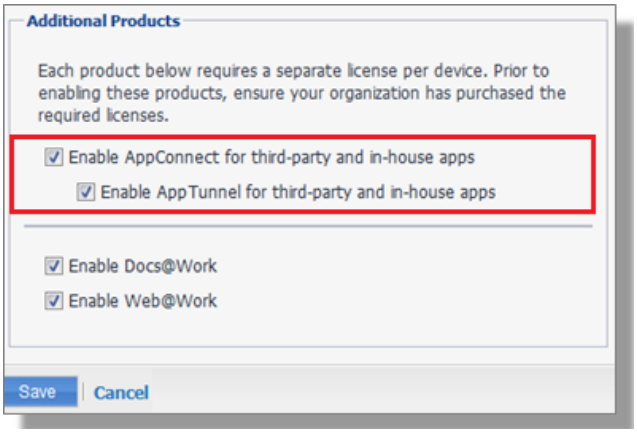
Use the following high-level steps to configure AppConnect for the app.

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.