



Notate for Android Enterprise Administrator's Guide

January 2024

Overview

This guide will help you configure Notate for your Android Enterprise environment. The configuration process consists of three steps:

1. Enable Notate to access back-end servers
2. Configure Notate policies
3. End users configure Notate on their mobile devices

Prerequisite:

Your MDM must be enabled for Android Enterprise in order to use Notate for Android Enterprise. Follow your MDM instructions for configuring Android Enterprise.

Step 1: Granting Application Access to Servers

Notate can access the Office 365 or on-prem Exchange servers via your MDM provided secure tunnel or MDM. Permissions for each application to access back-end servers must be granted.

Notate also requires access to api.notatepro.com on port 443 in order to send notification IDs to share recipients. Notebook sharing is required in order to use the calendar meetings functionality. No user data is ever sent or stored in the cloud. More details about how sharing notifications are processed can be found here: <http://support.shafersystems.com/customer/en/portal/articles/2303757-notate-sharing-infrastructure>

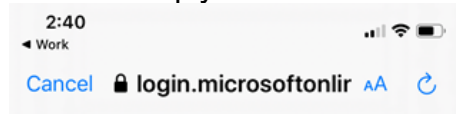
Application	Server Needed	Port
Notate	Exchange	443
Notate	api.notatepro.com	443

Ensure that Notate has access to the notification server by configuring your firewall to allow port 443 access to api.notatepro.com.

Ensure that Notate has access to the Exchange server by configuring your MDMs secure tunnel or VPN to allow Notate to access Exchange. Follow your MDMs instructions for this configuration.

Office 365 and Modern Auth

If you are connecting to Office 365 instead of an on-prem Exchange server, there are a few things that you need to do. First, as outlined in the application policies section below, make sure that you enable “Use Office 365 Settings”. Next be aware, that before end users can connect to Office 365 using Modern Auth, an Azure administrator must first grant Notate permissions to the enterprise. The admin can do this simply by launching Notate on a device and signing into his account and choosing to grant Notate permissions. If an end user without admin access first tries to launch Notate they will see a screen similar to the error below. Simply have an admin log in first to avoid this:



Need admin approval



Notate needs permission to access resources in your organization that only an admin can grant. Please ask an admin to grant permission to this app before you can use it.

[Have an admin account? Sign in with that account](#)

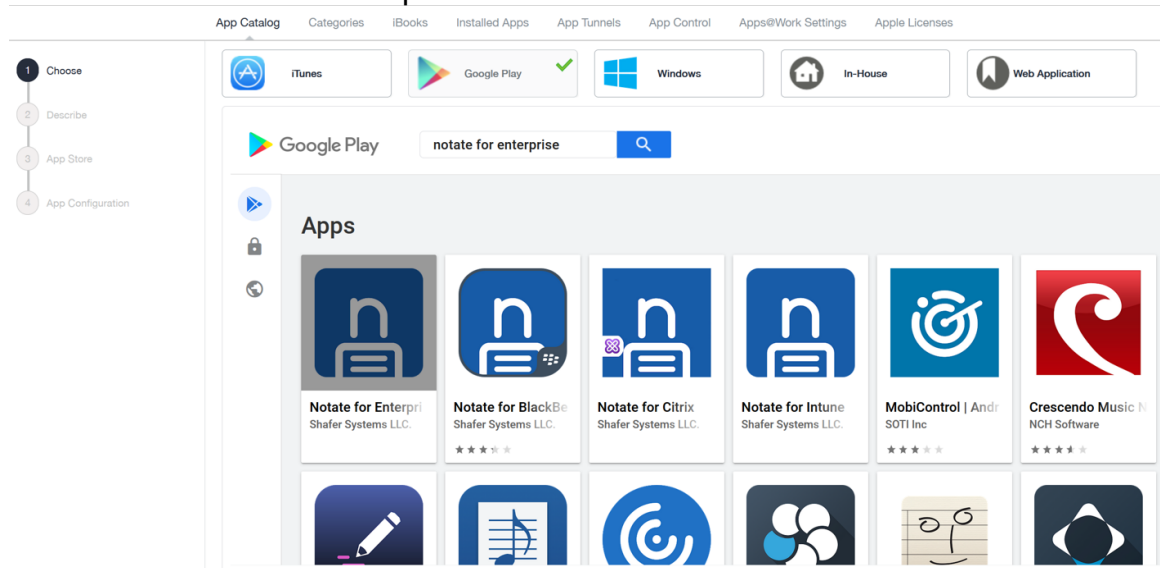
[Return to the application without granting consent](#)

Step 2: Add Notate as an Android Enterprise Application

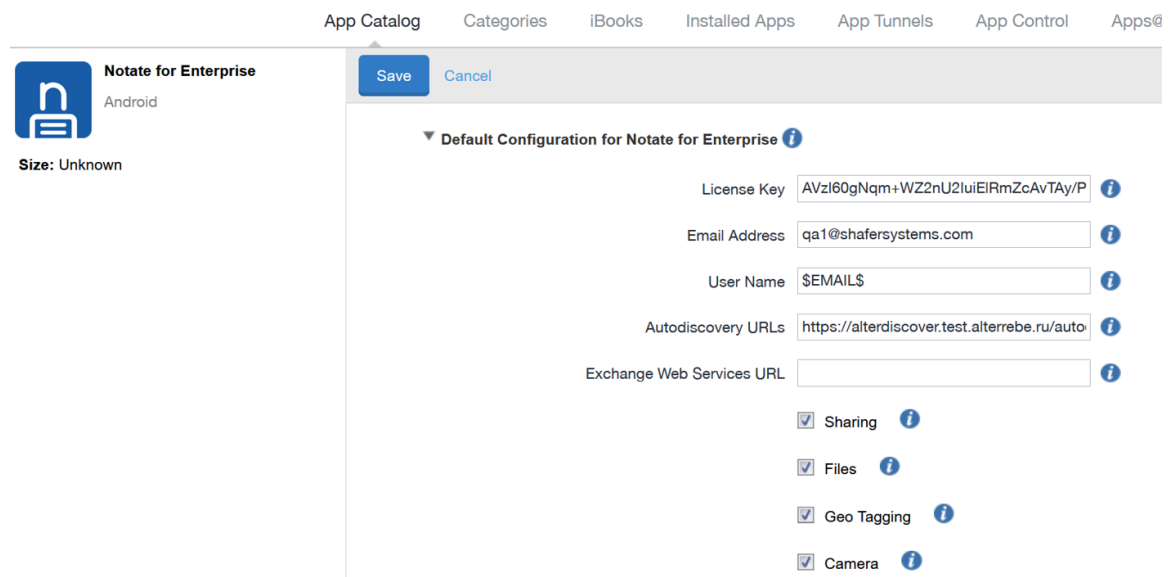
Each MDM has its own set of steps for adding an Android Enterprise application. This guide will show how to install Notate for Android Enterprise on a MobileIron server. Your MDM may look different. Refer to your MDM documentation for precise details.

For MobileIron use the following steps:

1. Go to the App Catalog and select “Add+”
2. Choose the “Google Play” as the apps source
3. Search for “Notate for Enterprise”:



4. Approve Notate and configure some initial values (like label, name, etc)
5. Now the Notate should be in the app list
6. Configure Notate policies from the “Edit” menu (in the app list)
7. Edit the values under “Default configuration for Notate for Enterprise”



Step 3: Configure Application Policies

The next step is to configure Notate application policies. This guide will walk you through this configuration.

Select the application Notate for Enterprise that you configured from the previous step. Specific policies to configure are:

Managed Configurations

This policy lets you control a variety of app configuration options and app restrictions. The options available for an app and the tooltips are defined by the app developer. If a tooltip mentions using a "templated value", use the corresponding Endpoint Management macro instead.

License Key	tINLBh5qrCMK51OHkMCujViYep+4FUOgaEW	?
Email Address		?
User Name		?
Autodiscovery URLs		?
Exchange Web Services URL		?
Hashed Sharing	☒ ?	
Files	☒ ?	
Use Modern Authentication	☒ ?	
Geo Tagging	☒ ?	
Camera	☒ ?	
Photo Gallery	☒ ?	
Voice Recordings	☒ ?	
Attachments	☒ ?	
Tasks	☒ ?	
Contacts	☒ ?	
Allow Crash Reports	☒ ?	
Support Email	support@shafersystems.com	?
Trusted Certificates	D189F05FF6F63BD56DB64BAD4F8047BA4E	?

licensingKey

Allow users to work with Notate features, e.g. syncing, scanning, etc. Get your licensing key from sales@shafersystems.com

userEmail

Usually leave blank. Used to overrides field from SDK (if supported by specific target)

exchangeURL

Exchange Web Services URL. This setting is NOT required unless autodiscovery is not possible for your environment. For instance, <https://server.domain.com/EWS/Exchange.asmx>.

supportEmail

The email address where user feedback will be submitted and debug logs will be sent. Default is `support@shafersystems.com`.

allowCamera

Allow device camera to insert pictures in notes, allow scanning. Default value is `true`.

allowGallery

Allow users to paste images from photo gallery. Default value is `true`. REG_DWORD type.

allowTasks

Allow users to manage tasks in Notate. Default value is `true`. REG_DWORD type.

allowContacts

Allow users to scan business cards into Exchange and manage Contacts in Notate.

allowFiles

Allow users to manage files and PDF editing in Notate. If policy is off - Files tab shouldn't be shown to the user. If transfer file to Notate - it should be attached in the note as file attachment. PDF files are not opened in PSPDF Editor - "Permission denied. This functionality has been disabled by your IT administrator." is shown REG_DWORD type.

trustedCertificates

Allow an admin to setup one or a few server trusted certificates. Policy should contain SHA1 hashes which separated by , or ; characters. SHA1 should be present as HEX formatted string with or without spaces in any register.

For instance,

- 3C EA DA D1 89 F0 5F F6 F6 3B D5 6D B6 4B AD 4F 80 47 BA 4E
- 3ceadad189f05ff6f63bd56db64bad4f8047ba4e, 3caedad189f05ff6f63bd56db64bad4f8047ba4e

allowHashedSharing

Allow an admin to turn on/off Sharing.

allowMicrosoftAuthenticator

Having the policy off will allow the user to log in with modern authentication (Office 365) even if ms Authenticator is installed.

useModernAuth

Allow an admin to setup sign in to Exchange via modernAuth (MSAL for Android) if it's turned on. REG_DWORD type.

httpProxy

Workaround for Windows (JPMC case). Allows an admin to setup proxy server to be used for web requests. Should be in format <domain>:<port> (i.e. localhost:3128)

Step 3: Mobile Client for Configuration

The last step for configuring Notate is to configure the mobile clients. If the previous steps have been followed correctly then the client configuration is very easy and can be performed directly by end users.

Exchange Synchronization set-up

If KCD is available, then a user does not have to enter any credentials and no mobile client configuration is required.

Users will be requested on first launch to provide their Exchange email password. In most cases this will complete user set-up for synchronization. In some cases, the user may be prompted for their user name to complete authentication. User Name should be added as the pre AD domain account name in the following format "domain\username or as the AD account name in the format [user@domain.com](#). Note that this field may be pre-filled if you specified it's format in the application policy settings in step 2.

The Exchange Server EWS URL field should be pre-populated thru the policy settings. If not pre-populated Notate will use the Exchange auto-discovery mechanism to locate the proper server. If auto-discovery fails the User will be prompted to enter the Exchange EWS URL as a final step. The URL should be entered in the following format: exchange.domain.com/EWS/Exchange.asmx

Close Settings Syncing	
General Syncing	Logout
	CONNECT TO EXCHANGE SERVER Email Address mark@shafersystems.net User Name mark_shafersystems.n Password Exchange Server exchange.domain.com Connect

If notes do not automatically begin the sync process, confirm the Exchange EWS URL, use the pre AD domain account name for the user, and make sure that the application has been granted permission to access the Exchange server from your MDM.

For questions contact: support@shafersystems.com