



Mobile Iron Core - Setup Guide

Mobile Iron Core - Setup Guide	1
Prerequisites	2
App Availability	2
Device Compatibility	2
Reachable KDC	2
Add Hypergate to Mobile Iron Apps	3
Enable Android Enterprise Support	4
Managed Configuration of Hypergate	5
Managed Configuration in Detail	7

This document aims to help you setup Hypergate with your Mobile Iron Core Instance, in order to deploy and integrate Hypergate within your organization. It is a step-by-step guide, leading you through the complete process that allows to successfully deploy and test Hypergate.

Prerequisites

MobileIron Core/Cloud must be enabled for Android Enterprise to use Android Enterprise work profile apps. To enable MobileIron Core/Cloud to provide Android Enterprise features, you must perform setup steps with Google, MobileIron Support, and MobileIron Core/Cloud Admin Console. Please ensure these steps are completed first.

- Core Admin Guide: <https://community.mobileiron.com/docs/DOC-3664>
- Cloud Admin Guide: <https://community.mobileiron.com/docs/DOC-2999>

App Availability

Hypergate is available through the Google Play Store, and Updates are released through this channel as well. You can find Hypergate through your Mobile Iron Core Interface if your organization has been added to the Hypergate Google Play Publishing Tool, a change that is done by the Hypergate Team.

Device Compatibility

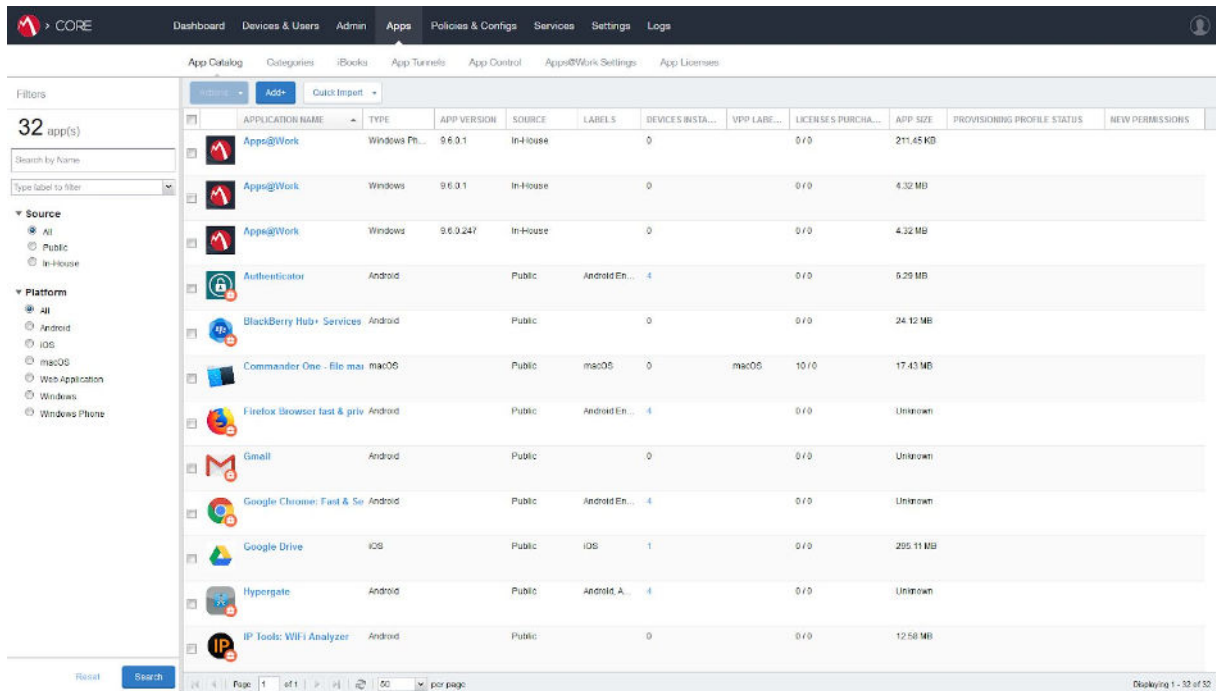
The Hypergate Android Application requires a minimum of Android 7.0.

Reachable KDC

Your Kerberos KDC has to be reachable from the Device, either through a public URL or by using a VPN Application like Mobile Iron "Tunnel".

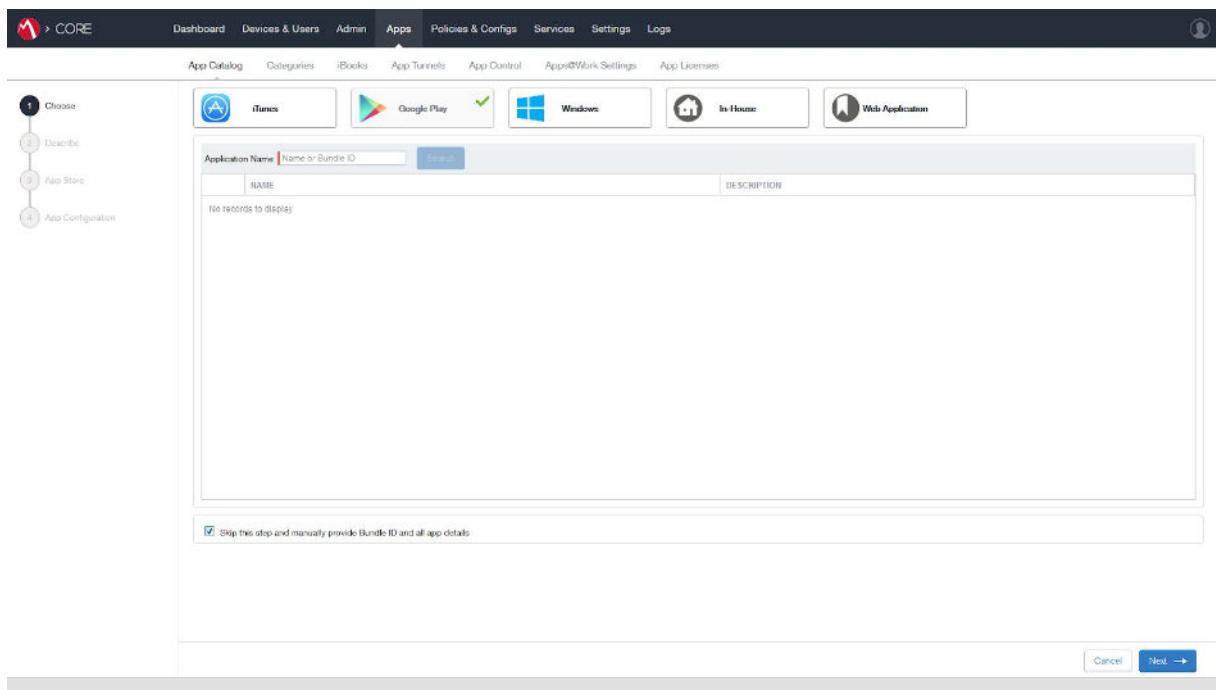


Add Hypergate to Mobile Iron Apps



APPLICATION NAME	TYPE	APP VERSION	SOURCE	LABELS	DEVICE INSTA...	VPP LAR...	LICENSE'S PURCHA...	APP SIZE	PROVISIONING PROFILE STATUS	NEW PERMISSIONS
Apps@Work	Windows Ph...	9.6.0.1	In-House		0		0/0	211.45 KB		
Apps@Work	Windows	9.6.0.1	In-House		0		0/0	4.32 MB		
Apps@Work	Windows	9.6.0.247	In-House		0		0/0	4.32 MB		
Authenticator	Android		Public	Android En...	4		0/0	6.29 MB		
BlackBerry Hub Services	Android		Public		0		0/0	24.12 MB		
Commander One - File ma	macOS		Public	macOS	0	macOS	10/0	17.43 MB		
Firefox Browser fast & priv	Android		Public	Android En...	4		0/0	Unknown		
Gmail	Android		Public		0		0/0	Unknown		
Google Chrome: Fast & Se	Android		Public	Android En...	4		0/0	Unknown		
Google Drive	iOS		Public	iOS	1		0/0	295.11 MB		
Hypergate	Android		Public	Android, A...	4		0/0	Unknown		
IP Tools: WiFi Analyzer	Android		Public		0		0/0	12.58 MB		

Switch to the “Apps” view and click on “Add”.



Application Name Name or Bundle ID

NAME DESCRIPTION

No records to display

Skip this step and manually provide Bundle ID and all app details

Cancel Next →

You will be redirected to the page shown above. To add Hypergate:

1. Select “Google Play” in the top row of store selections
2. Check “Skip this step and provide Bundle ID and all app details” towards the bottom of the page



Now, click “Next”.

The screenshot shows the 'New App' configuration interface. The top navigation bar includes 'Dashboard', 'Devices & Users', 'Admin', 'Apps', 'Policies & Configs', 'Services', 'Settings', and 'Logs'. Below this, a secondary navigation bar lists 'App Catalog', 'Categories', 'iBooks', 'App Tunnels', 'App Control', 'Apps@Work Settings', and 'App Licenses'. On the left, a vertical progress bar indicates the current step is 'Describe' (2). The main form area is titled 'New App' and contains the following fields:

- Package Name:
- Application Name:
- Min. OS Version:
- Description:
- Category:

At the bottom right of the form, there are 'Cancel' and 'Next ->' buttons.

Enter the following details:

- Package Name: “ch.papers.hypergate”
- Application Name: “Hypergate”
- Min. OS Version: “7.0”
- Description: “Android Kerberos SSO Authenticator”

Now, click “Next”.

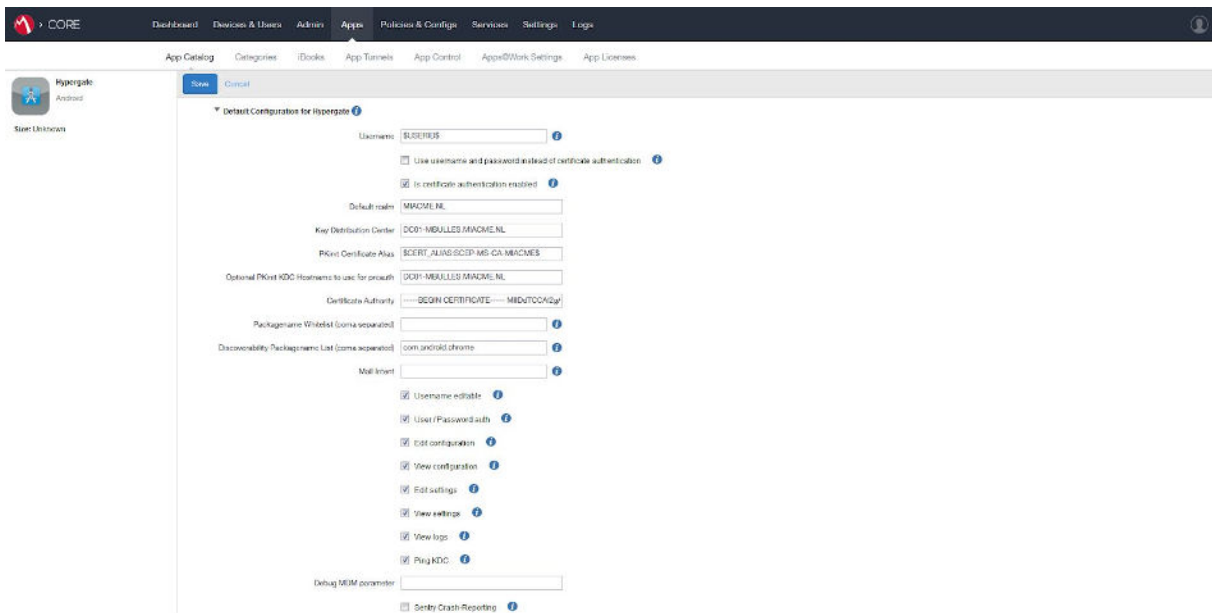
Enable Android Enterprise Support

After the successful import, “Edit” the Hypergate Application again and enable “Install this App for Android Enterprise” in the Android Enterprise Section.



Managed Configuration of Hypergate

To properly configure Hypergate for authentication with your Kerberos environment, Hypergate exposes a set of managed configuration properties that can be managed within Mobile Iron Core. Visit the Hypergate App entry and click on “Edit” at the top. Then scroll down until you can see “Default Configuration for Hypergate”, which you can show completely by clicking on the small arrow. This reveals the available configuration options for Hypergate.



The following properties are **required** for Hypergate to work properly:

Configuration Key	Description	Example
Username	Kerberos Username	\$USERID\$
Default Realm	Hostname of your Kerberos Realm	HYPERGATE.ME
Key Distribution Center	Hostname for your Kerberos KDC	KDC.HYPERGATE.ME
Discoverability Packagename List	Apps that are able to use Hypergate as default SPENGO Authenticator, given they use the Google Account API. Works with native Google Chrome.	com.android.chrome

Check either of “Use username and password” or “Is certificate authentication enabled”



Additionally, for **Certificate-based Authentication**, the following properties are **required as well**:

Configuration Key	Description	Example
PKInit Certificate Alias	Usually set using a variable to the certificate alias.	\$CERT_ALIAS_SCEP\$
Is certificate authentication enabled	Required for Cert-Based Authentication	<input checked="" type="checkbox"/>
Certificate Authority	Your public *.cert	-----BEGIN CERTIFICATE----- DYLDKSDA...

You can convert your *.cert file using our online tool (<https://converter.hypergate.me>). The certificate is not sent anywhere, but converted locally in your browser. The tool is also available for download, additionally we are also able to help you to convert your certificate manually.

You can choose to enable “Sentry Crash-Reporting” in order to help us gather more detailed information about potential problems, as crashes are sent to a service hosted within Papers that collects crash reports. This option might be helpful during the setup process, but is no requirement for a successful production deployment.

Managed Configuration in Detail

Hypergate supports additional configuration options, outlined below. These have sensible defaults and do not need to be configured in order for Hypergate to work.

*required configuration key

Configuration Key	Description	Default Value
Username*	Username for Kerberos	""
Use username and password instead of certificate authentication	If Hypergate should use the Password Authentication by Default	false
Is certificate authentication enabled	If Certificate-Based authentication is enabled	true
Default Realm*	Default Kerberos Realm	-
Key Distribution Center*	Default KDC Hostname	-
PKInit Certificate Alias*	pkInit Certificate Alias	-
Optional PKInit KDC Hostname	pkInit KDC Hostname	-
Certificate Authority*	Certificate Authority	-
Package Whitelist*	Packages/APKs that are allowed to call Hypergate for SSO using an explicit intent, accepts a single string or comma-separated list of strings	-
Discoverability Package List*	Packages/APKs that are allowed discover Hypergates Capability for SSO through an implicit Intent, accepts a single string or comma-separated list of strings	-
Mail Intent	Package of E-Mail application to use to send Intent. For Google Mail, such as "com.google.android.gm"	-
Username editable	If users are allowed to edit their username	true
Is certificate authentication enabled	If Hypergate should allow Password Authentication	false
Edit Configuration	If users are allowed to edit the kerberos configuration in general	true
View Configuration	If users are allowed to view the kerberos configuration	true
Edit Settings	If users are allowed to edit settings	true
View Settings	If users are allowed to view the settings	true
View Logs	If users are allowed to see the logs of the application	true
Ping KDC	If users are able to ping the KDC	true
Sentry Crash-Reporting	Reports Crashes to a internal service of Hypergate, in order to help with debugging and investigation of issues.	false

