*Using NetSfere for Android with MobileIron*

July 19, 2016
Proprietary and Confidential
Do Not Distribute

## **Overview**

NetSfere is a cloud-based, enterprise messaging service that offers a secure platform for internal communication and collaboration, giving IT total control over employee messaging across multiple devices.

Designed to meet the industry-specific challenges your organization is up against, NetSfere's next-generation approach allows employees to safely communicate business information in real-time via a user-friendly Web interface or mobile messaging app

Package name for Android: **NetSfere\_MobileIron\_Android.apk**

## **App availability**

MobileIron customers can download NetSfere for Android from the following URL: <http://downloads.netsfere.com/NetSfere_MobileIron_Android.apk>

For more information on NetSfere for MobileIron: Sales@NetSfere.com

## **Device compatibility**

Requires Android 4.1 and up

## **App-specific configuration**

Not applicable to NetSfere

## **AppTunnel support**

## There is no interaction with internal servers required for NetSfere

## **Data Loss Prevention Policy**



## **User features**

* 256-bit device-to-device encryption with elliptical curve key exchange provides the strongest security currently available
* Robust multimedia capabilities allow users to send text, documents, photos and videos up to 100 MB as attachments
* Centralized control features offer remote wipe, account management and message retention policies
* Real-time statistics track key performance indicators like number of accounts, actives sessions and messages sent
* Cloud-based storage provides instant message availability across multiple devices and enables zero-effort device upgrades

## **For more information**

NetSfere is a truly global messaging solution. Cloud-based architecture supports international service availability, creating a secure enterprise messaging platform for multinational businesses and geographically diverse users.

[NetSfere web site](http://www.netsfere.com/)

[NetSfere Secure Enterprise Messaging Support](https://www.netsfere.com/About-Us/Secure-Enterprise-Messaging-Support-Services)

## **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 Core, 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 Core, navigate to the Settings page on the Core 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 Core 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 and AppTunnel Guide](https://community.mobileiron.com/docs/DOC-3646) 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 and AppTunnel Guide](https://community.mobileiron.com/docs/DOC-3646) for details about each field.

Also, for more on AppTunnel configuration, see “Adding AppTunnel Support” in the [AppConnect and AppTunnel Guide](https://community.mobileiron.com/docs/DOC-3646).

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

1. On the Core Admin Portal, go to Policies & Configs > Configurations > Add New > AppConnect > App 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 Catalog, and clicking the hyperlink to edit the app. The bundle ID resides in the Inventory field in parenthesis.

1. AppTunnel: Click on the “Add+” button and enter the AppTunnel details. The AppTunnel service for this app must be pre-configured in order to use it here.
2. App Specific Configuration: Click on the “Add+” 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 and AppTunnel Guide](https://community.mobileiron.com/docs/DOC-3646).

To configure an AppConnect container policy:

1. On the Core 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 Catalog, and clicking the hyperlink to edit the app. The bundle ID resides in the Inventory field in parenthesis.

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