MindLink with MobileIron

Overview

MindLink for MobileIron on iOS is a secure Chat & Messaging platform for global enterprises, integrated with AppConnect to offer state-of-the-art data security to corporate users.

MindLink offers Instant Messaging, Presence, Group Chat, file sharing & archiving, voice (coming soon) combined with data security, compliance archiving and business integrations with internal and external systems via chatbots/connectors.

MindLink also fully integrates with Unified Communication platforms such as Microsoft Lync™ and Skype for Business to extend its messaging capabilities.

The app's bundle ID is com.mindlinksoft.mindlinkmobile.mobileiron

Platform Support:

- Windows, Mac, Linux
- Android, iOS, BlackBerry

Security Features:

- Complete Encryption
- Multi-factor Authentication
- OnPremise/Private Cloud Deployment
- User & Access Management
- MDM/EMM support

Compliance Capabilities:

- Instant Messaging, Group Chat, File Attachments for Lync/Sfb
- Yammer, ICE CHAT

Integrations:

- RestFul API to connect internal/external systems
- SharePoint
- Social Media (Twitter, RSS)
- Email

App availability

Available from the Apple App

Device compatibility

iOS 8.0 or above

App-specific configuration

Key	Description	Default if the key-value pair is not configured
mlmServerUrl	The URL of the MindLink Server	A typical value would be https://mindlink.my-company.com. If this is not supplied, then the user is required to enter a server URL when the app is launched.
mlmLogOnName	The account name with which to pre-populate the log on form. This should map to the backend account used to authenticate to Skype for Business.	A typical value would be a variable like $USER_CUSTOM1$, which can be defined in the LDAP settings. If this is not supplied, then the user must enter their log on name on the password screen.

AppTunnel support

The app requires a backend server to operate. This server is typically deployed inside the on-premise network.

The server's role is to broker between the app and the Skype for Business components on behalf of the user, and maintain the user's Skype for Business endpoint whilst the app is not in use.

This communication occurs over HTTPS communication, the port used for this is configurable.

App-specific configuration can be used to push the server URL

Data loss prevention policy support (iOS SDK apps only)

- the pasteboard DLP policy: YES
- the print DLP policy: N/A
- the Open In DLP policy: YES

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

All at-rest data is stored in the MobileIron secure storage.

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

No, the app is required to operate in AppConnect mode.

Other Requirements

The app requires an on-premise Skype for Business or Lync Server deployment. In addition, the MindLink Server must be deployed as a trusted application server within the Skype for Business topology.

The MindLink Server is a .NET Windows Service that runs on a Windows Server machine.

MindLink Server Hardware Requirements

- Dual or Quad core, 64-bit CPU (minimum 2.4 GHz)
- Gigabit Ethernet connection
- 4GB RAM
- Minimum 1Gb disk space

MindLink Server Operating System Requirements

- Windows Server 2008 R2, 2012, 2012 R2 or 2016
- Domain Joined
- Microsoft .Net Framework 4.6.2
- C++ 2012 redistributable installation binary (for Lync 2013 only)
- C++ 2013 redistributable installation binary (for Skype for Business only)
- Domain Member Service Account

MindLink Server Network Connectivity Requirements

- Communication on Port 2195 for APNS Push Notifications (MindLink Mobile for iPhone/iPad)
- If you enable Server Pooling functionality (available to MindLink Mobile only), you may use a High Availability / Resiliency strategy supported by Microsoft SQL Server 2012, 2014 or 2016 such as 'Mirroring' or 'Always on'

Lync/Skype For Business Requirements

- OCS 2007 R2, Lync 2010, Lync 2013, Skype for Business 2015 - On-Premise
- Persistent Chat enabled

User features

MindLink for MobileIron has an intuitive chat interface with a wealth of content management features, including:

- Customizable Interface
- WhatsApp-style message feed & single conversations view
- Custom Alerts & Notifications
- #Tag for threaded conversations
- @Mentions to notify or assign tasks
- InLine Images
- Dynamic Search
- Secure Guest Access

For more information visit the MindLink Product Page

For more information

For release notes, installation, deployment and/or administration guides, please visit the MindLink Wiki.

Configuration tasks

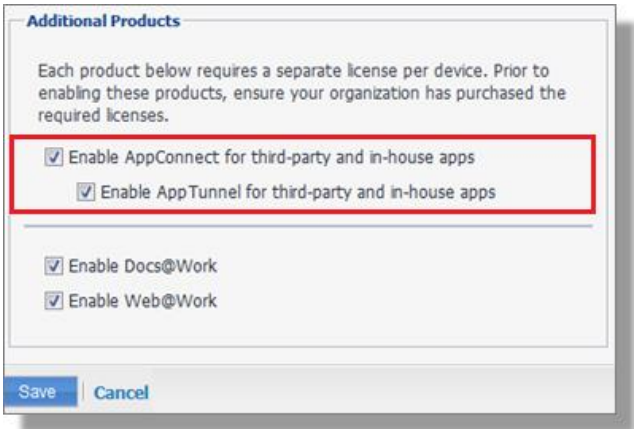
Use the following high-level steps to configure AppConnect for the app.

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 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 for details about each field.

Also, for more on AppTunnel configuration, see "Adding AppTunnel Support" in the AppConnect and AppTunnel Guide.

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.

3. 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.

4. 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.

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.

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