Using TigerText with MobileIron

April 28, 2015
Proprietary and Confidential
Do Not Distribute

Overview

Built for the enterprise, TigerText℠ is the #1 App for sending secure, encrypted text messages and files that permanently disappear from phone company servers and devices so company information remains safe.

TigerText not only keeps your communications secure, it helps transform your workflows for maximum productivity, all while remaining compliant with industry regulations such as HIPAA and Sarbanes-Oxley (SOX).

TigerText also offers a secure platform with API integration for connecting to 3rd-party applications. With the TigerConnect SDK, customers can implement a secure communication channel with custom triggers that automatically send critical information and alerts directly to the user's smartphone, tablet and web browser. These integrations allow companies to unlock the full potential of stored data, making it instantly accessible and actionable.

App iOS Bundle ID: com.tigertext.tigertext

Key Features

SECURE MESSAGING: Keep messages private with fully encrypted, end-to-end, secure texting solution.
DELIVERY CONFIRMATION: Know instantly when messages have been sent, delivered, and read.
MESSAGE LIFESPAN: Set message lifespan to dictate when messages will be automatically deleted.
MESSAGE RECALL: Recall a message and attachments before or after it has been read.
UNIVERSAL MESSAGING: Securely converse with colleagues who do not have TigerText.
VOICE NOTES: Record, attach, and send voice files for more detailed messages.
DO NOT DISTURB: Let colleagues know when you're not available. Create custom auto-replies.
GROUP MESSAGING: Create groups on the fly to improve collaboration and coordination.
MESSAGE FORWARDING: Easily add colleagues and experts to ongoing text conversations.
DELIVERY ESCALATION: Notifications not delivered within 5 minutes are re-sent via SMS.

MULTIPLE INBOXES: Quickly switch between inboxes when using multiple TigerText accounts.
MULTI-PLATFORM SUPPORT: Access secure messages on any smartphone, tablet, or desktop.
INTEGRATED CORPORATE DIRECTORIES: Active Directory, LDAP, and eDirectory integration.
SECURE ATTACHMENTS: Securely attach files, photos and voice notes. From desktop attach PDFs and files from Box and Google Drive.
PIN LOCK: Admins or users can configure 4-digit numeric PIN settings in the app for added security.
MESSAGE ARCHIVING (OPTIONAL): Compliance-based industries may add hosted archiving to capture transactional data.

Additional Information

TigerText is currently certified to work in the U.S. and Canada. While users in other countries may download and use the app for free, TigerText access may be inconsistent outside the U.S. and Canada.

App availability

TigerText is available for download in both the Apple App Store and Google Play store. A web browser version is also available at home.tigertext.com. For more information, go to www.tigertext.com/download.

Device compatibility

TigerText currently supports devices that work with iOS7 and iOS8. For more information, go to www.tigertext.com/system-requirements.

App-specific configuration

TigerText currently does not require any MobileIron app-specific configurations. User access, message lifespan and other additional configurations can be controlled via the TigerText Admin Console.

AppTunnel support

TigerText currently does not require AppTunnel support.

Data loss prevention policy support (iOS SDK apps only)

TigerText does not support MobileIron data loss prevention policy. TigerText keeps your communications secure while remaining compliant with industry regulations such as HIPAA and Sarbanes-Oxley (SOX).

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

TigerText does not support MobileIron secure file I/O. However, TigerText keeps messages private with fully encrypted, end-to-end, secure texting capabilities.

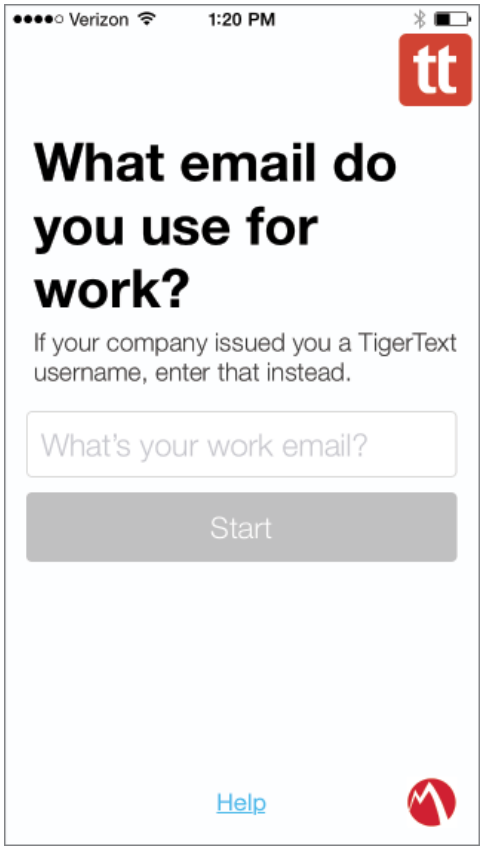
AppConnect and non-AppConnect mode support (iOS SDK apps only)

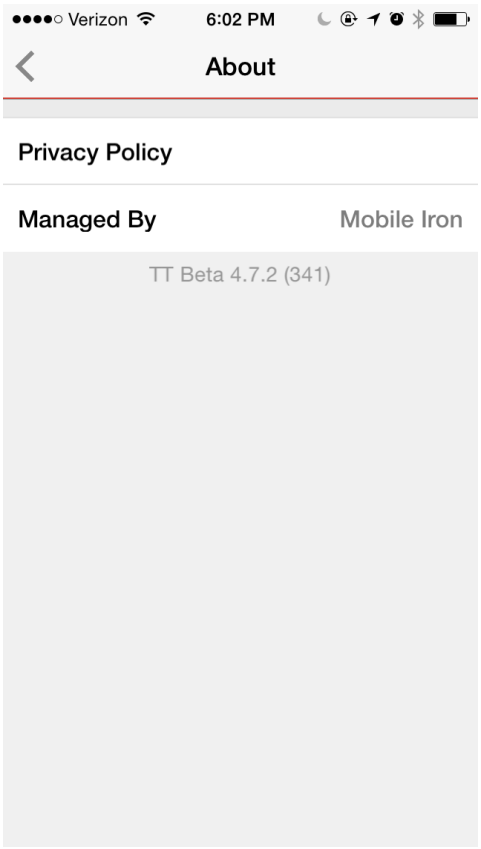
TigerText can behave as either an AppConnect-enabled app or a regular, secure texting app. If the device is MobileIron-enabled and has the MobileIron app installed, TigerText will behave as an AppConnect-enabled app. If not, TigerText will continue to behave as a secure texting app. To switch between the two modes, the user is required to uninstall and reinstall the app.

User features (iOS)

To quickly determine if TigerText is AppConnect-enabled, the user will be able to find visual UI cues in the login screen and within the app – as shown:

Login Screen (bottom right) *Settings => About (managed by)*





If TigerText becomes "Retired" by MobileIron, the user will be logged out of the app for security reasons and notified of the reason. Once notified, TigerText will prevent the user from logging in until the user's device is authorized. The user can continue to use TigerText in a non-AppConnect enabled fashion by uninstalling and re-installing the app.

Configuration tasks

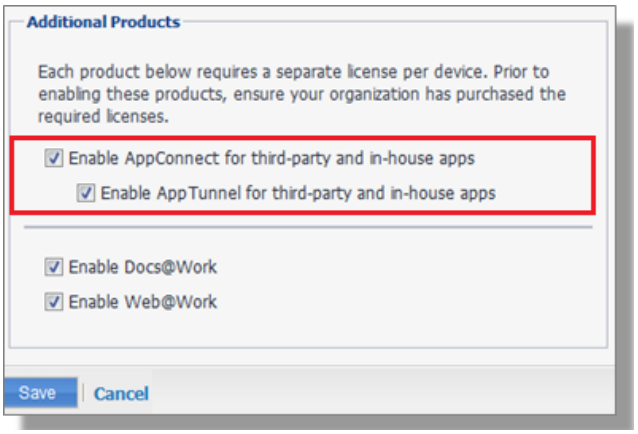
Use the following high-level steps to configure AppConnect for the app.

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.