Deploying SL2™ using MobileIron

CellTrust

SL2™—comprised of SecureVoice™ and SecureSMS™—empowers the workforce with seamless mobile communications that can be secured, traced and archived. The powerful app supports enterprise mobile communication, eDiscovery and compliance enforcement to give leading organizations a competitive advantage by balancing mobile productivity, risk and control.

MobileIron

Mobileiron (now acquired by Ivanti) is the industry's first Mobile-centric zero trust platform that secures digital workspace with its industry-leading unified endpoint management (UEM) capabilities and with additional zero trust-enabling technologies, including zero sign-on, multi-factor authentication (MFA), and mobile threat defense (MTD). Together, they enable a seamless, secure user experience by ensuring only authorized users, devices, apps, and services can access business resources.

MobileIron AppConnect

MobileIron AppConnect containerizes apps to protect app data at rest without touching personal data. Each app becomes a secure container whose data is encrypted, protected from unauthorized access, and removable.

Access to each containers app is authorized with a passcode / passphrase or biometric challenge gated by MobileIron client residing on the managed device and data sharing between other AppConnect and non-AppConnect apps is controlled via an AppConnect policy enforced by the UEM. The MobileIron AppConnect version of CellTrust SL2 apps are available for both IOS and Android OS.

TABLE OF CONTENTS

SL2 KEY BENEFITS

- Capture text and/or voice communications
- Integration with leading archivers
- Integration with CRM and personal email
- Option for multiple business numbers on same device
- Office landlines can be text enabled and integrated
- SMS prescheduling
- Out-of-office/auto-reply SMS

AppConnect Custom Configuration

iOS

Configuration Key	Value	Description
SL2_Policy_AllowDeviceStorageAccess	True	EMMs can use this field to block access to device contacts
SL2_Policy_AllowTakingPhotos	True	EMMs can use this field to block access to device photos.
SL2_Policy_AllowTakingVideos	True	EMMs can use this field to block access to videos.
SL2_Policy_AllowEmojis	True	EMMs can use this field to block emojis.

Android

Configuration Key	Value	Description
SL2_Policy_AllowEmojis	True	EMMs can use this field to block emojis.

iOS Managed App Configuration

App configuration enables you to customize the installation, promotion, and distribution of each app you deploy to your users' devices. The apps can be your own in-house apps, apps from a public store, or MobileIron apps. You have the flexibility to deploy the apps to many different users and groups with unique names and configurations specifically tailored to each recipient.

Following the AppConfig.Org standards, the CellTrust SL2 app configurations can be deployed on both iOS and Android managed devices. The AppConfig standards allow configuring app settings remotely from a centralized location (such as UEM console) in a secure manner in order to increase mobile adoption in business. Users benefit with instant mobile productivity and a seamless out-of-the box experience, and businesses benefit with secure work-ready apps with minimal setup required while leveraging existing investments in Device Management (UEM/MDM), VPN, and identity solutions.

Using iOS Managed App Configuration

Using the iOS Managed App Configuration, specific settings can be configured for the installed managed app. An application might have some configuration parameters implemented or restricted by the developer. For applications with such restrictions your configuration options might be limited.

To configure iOS managed apps:

1. Go to **Apps > App Catalog**.
2. Select **SL2 for MobileIron App**.
3. Click the **App Configurations** tab.

4. Click **iOS Managed App Configuration** or click the **+** button.

   In the iOS Managed App Configuration there are some default configuration settings in place.

5. Click **Add** to add another configuration, if needed. Optionally, click name of the configuration to edit the configuration.

6. Under **Configuration Source** select any of the **Source Type** options
   - **AppConfig Community** - This option is available only for those apps that have an app configuration specification available in the community repository. If this option is available, it is selected by default.
   - **Use .xml spec** - Select this option to upload the schema for the app to push a particular version of app configuration. Click **Choose File** to upload the .xml file. Ensure that the .xml file contains the bundle ID and the version. An error message will be displayed if the bundle ID in the file does not match with the bundle ID of the app.
   - **None** - Select this option if you do not want to apply any schema for the app. This option is selected by default if the **AppConfig Community** option is not available.

     The uploaded .xml file is displayed in the **Configuration Source** section. Click the Delete icon to delete the uploaded .xml file.

7. In the **iOS Managed App Settings**, you can set the configuration options to enter key value pairs.
   - **+ Add** - Click **+Add** to add the key value pairs to the managed app configuration to retrieve the registration name identity by MobileIron Go client during iReg or Apple Device Enrollment.

Key	Value	Type
hostname	APP2.CELLTRUST.COM	String
username	${userEmailAddress}	String

8. Click **Update** to save your entries.
9. Choose a distribution level for this configuration of the app:
   - **To everyone** - The app is added to all the user compatible devices.
   - **To no one** - The app is staged for distribution at a later date.
   - **Custom Distribution** - Select any of the following options:
     - **User/User Groups** - The app is distributed to only the users or user groups you choose.

       Click the **Users** tab to select the user(s).

       Click the **User Groups** tab to select the user group(s).
     - **Device/Device Groups** - The app is distributed to only the devices or device groups you choose

       Click the **Devices** tab to select the device(s).

Click the **Device Groups** tab to select the device group(s).

iOS Managed App Settings

SL2 for MobileIron App supports the following iOS Managed App Settings:

Configuration Key	Value Type	Value Example	Description
idpurl	String	https://account.activedirectory.windowsazure.com/applications/signin/c8830133-f83d-4efa-9632-3fb95c26a40f?tenantId=98325c7e-cff0-45bf-b052-d6e7448681ea	EMMs can use this field to configure the SL2 Mobile App to leverage the company's Single sign-on (SSO) to verify the identity of the end-user. **Example: https://account.activedirectory.windowsazure.com/applications/signin/c8830133-f83d-4efa-9632-3fb95c26a40f?tenantId=98325c7e-cff0-45bf-b052-d6e7448681ea** **Note:** Send email to cs@celltrust.com to configure your SL2 Domain to support modern authentication.
Hostname	String	APP2.CELLTRUST.NET	EMMs can use this field to populate the SL2 Mobile Domain Address on behalf of the end-user. **Example: app2.celltrust.net**
Username	String	${userEmailAddress}	EMMs can use this variable field to populate the end-users corporate email address on behalf of the end-user. **${userEmailAddress} = user@domainname.com**