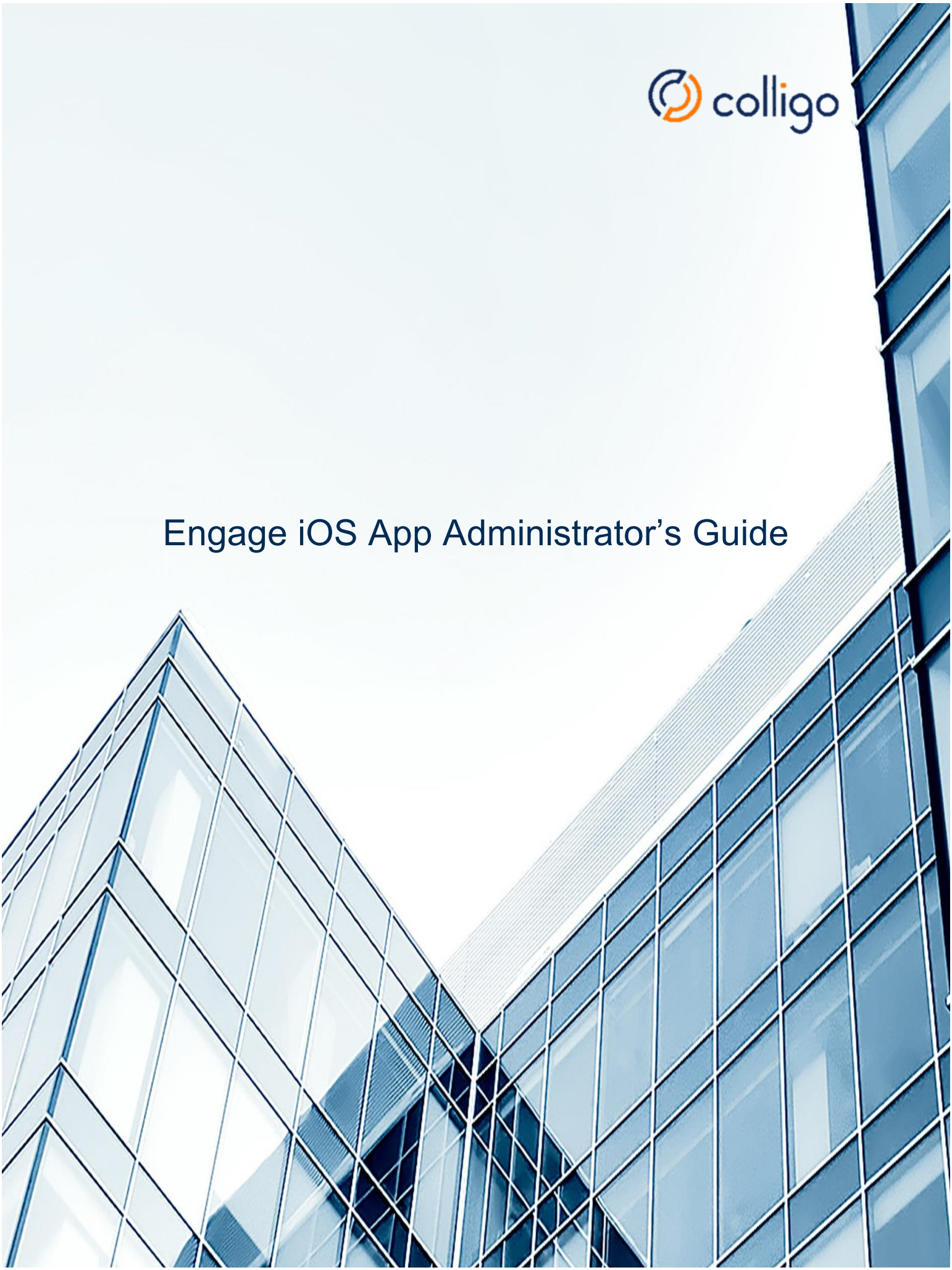
Engage iOS App Administrator’s Guide



Contents

Introduction

This document provides guidance for your deployment of Colligo Engage iOS App. User documentation is available on the Colligo support website at http://www.colligo.com/support/

For any further technical details please contact Colligo Technical Support at http://colligo.com/request.

For sales related question please contact Colligo Sales at sales@colligo.com.

Target Audience

- IT Administrators
- Technical Evaluators
- Deployment Managers

Devices Supported

NOTE: All devices require iOS 7.0 or later

- iPad (2nd generation and above) and iPad mini
- iPhone (4 and above)
- iPod Touch (4th generation)

SharePoint Platforms Supported

- SharePoint 2010
- SharePoint 2013
- SharePoint Online (Office 365)

SharePoint Security & Privileges

By using SharePoint's web services to access SharePoint data, Colligo Engage apps respect all privileges defined on the site. Colligo Engage supports most standard sign-on processes supported by SharePoint, including support for default credentials and other specified credentials. Passwords are stored in the keychain.

The Colligo Engage iOS app supports Claims-based and Forms-based authentication, as well as ADFS. SharePoint by default does not provide web service permissions to anonymous users, so this permission level cannot be used for uploading documents to SharePoint.

Deploying the Colligo Engage iOS App

There are three possible methods of deployment:
1. Via the app store, using the Colligo Engage Console for user management
2. Enterprise Deployment
3. Business to Business (B2B) with Volume Purchase Program (VPP) via the Apple store

The processes are similar but each of the following sections provides details on the differences between the two.

NOTE: The VPP option is only available for specific countries. To see if VPP is available for your country, check here: http://www.apple.com/business/vpp/

App Store Deployment

If you are using the Colligo Engage Console you can use the Colligo Engage iOS App available in the public iTunes App Store. Each user will need an account setup in the Engage Console and will need to sign in to the app using their Engage Console credentials after installation. For more information on the Colligo Engage Console please refer to the Colligo Engage Console Administrator Guide or contact Colligo support.

Enterprise Deployment

An Enterprise Deployment requires an Enterprise Development account.

This account allows Apple to identify apps as being owned by a company for internal use. Any applications signed by this account are identified with the company. There is an annual cost of $300 for the account, payable by the company to Apple directly.

To get an enterprise development account:
1. If your company does not already have a D-U-N-S Number, register for a D-U-N-S Number for your business through Dun & Bradstreet (http://www.dnb.com/)
2. Sign up for the Enterprise Developer Account through Apple. Allow approximately a week for processing by Apple.
3. Assign a Colligo representative as an Admin developer for your enterprise account.

For more information, see: http://developer.apple.com/programs/enterprise/

To build and deploy the app, complete the following steps:
1. Create an App ID with the following naming convention: **"com.[your company].engage**"
2. Set up a Distribution Certificate for the account, followed by a Distribution Provisioning file.
3. Install the certificate file on the computer that sent the request for the certificate.
4. Export the certificate identity so it can be installed on other machines.
5. Provide the two files (certificate and identity as a p12 file, and the provisioning file as a .mobileprovisioning) to Colligo for signing the application.

For more information about these steps see **Obtaining your Distribution Certificate**.

B2B with VPP (only available for specific countries)

B2B with VPP is only available if this option was selected prior to placing an order with Colligo, as it requires the product purchase to be placed through the Apple App Store.

To do a B2B with VPP deployment, you need to set up a VPP account with Apple. There is no cost for this. The company information is verified by Apple and can take one week to process. For more information, see: https://enroll.vpp.itunes.apple.com/

Provide Colligo with the VPP account email address / login name. This allows Colligo to make the app available to the VPP account after customization.

MDM (Optional)

Another option for deployment is Mobile Device Management (MDM). MDM systems allow enterprise organizations to track and provide support for any mobile device accessing their system. Using MDM is optional for either app store, enterprise, or B2B. It is a system designed to monitor and deploy applications within an enterprise environment. This can simplify the deployment process.

Colligo Engage iOS App works with all major MDM systems. If you require help with selecting an MDM system for your company, contact Colligo.

Branding

To include specific branding in the application, such as company specific graphics or text, Colligo can provide you with some template images that you can change. Alternatively, Colligo can make the changes for you. Note that this requires the purchase of a Branding option when purchasing Colligo Engage.

App Delivery

Once the changes to the App are finalized, an IPA (iOS application) file is created for delivery.

Enterprise Deployment

After the IPA file is created, Colligo will send it to you. The file needs to be added to the MDM system for deployment. Individual users can then install the app on their devices.

If you are not using an MDM system, Colligo can host the application on our website and integrate the Activation Key mechanism. This option would also mean that the app cannot check for updates or notify users if there is a new version that can be downloaded.

B2B with VPP

After the IPA file is created, it is uploaded to the Apple App Store. Apple validates the build, which is typically a one-week process. Once approved, you will be notified that you can purchase the app through the VPP account. You can then purchase a number of licenses and distribute the app through an MDM solution. Individual users are then able to install the app on their iPads, iPhones or iPod Touches.

NOTE: After you have created your site, you can provide Colligo with the URL and have it included in your customized Enterprise build so it is automatically enabled on startup for your users.

Licensing

App Store Deployment

Licensing of the Colligo Engage iOS App when using the app store deployment is based on active user management within the Colligo Engage Console.

Enterprise Deployment

When an IPA file is distributed to a client, some analytical data will be integrated into the account to track the number of devices using the app to maintain licensing and billing. To discuss the possibility of purchasing an unlimited license, contact Colligo Sales.

B2B with VPP

Customers can install the App based on the volume purchase through the App store.

Updates

New versions of Colligo Engage will be periodically released and be available for redeployment. Colligo will contact your company directly when a new version is available.

App Store Deployment

The Colligo Engage iOS App available via the public iTunes App Store will be regularly updated to the latest version and the app store will handle notifying users of updates.

Enterprise Deployment

To upgrade to the latest version of Colligo Engage, you will receive a newly generated IPA file to integrate into your MDM.

B2B with VPP

To upgrade to the latest version of Colligo Engage, a new IPA is uploaded to the Apple App Store. Users are notified of the update through the Apple App Store on their device, which can be installed directly.

Distribution Certificates

Certificate Expiry

Certificate expiry applies only to Enterprise Deployments. Distribution Certificates last for one year, at which time they need to be re-generated. Once the certificate has expired, no new installations or updates of the app can take place.

If a certificate is revoked earlier that the first year and replaced with a new one, the app will continue to function until the original certificate expires. However if the certificate expires, that installation will no longer function. If a provisioning file expires, the app will stop working until a new provisioning file is added to the device that uses the same unexpired certificate.

The updated certificate, identity, and provisioning must be provided to Colligo to create a new version of the App that can be distributed to you.

Obtaining your Distribution Certificate

To distribute your OS application with Enterprise Deployment, Apple requires your Team Agent to create a Distribution Certificate. Only your Team Agent can create it, and only that certificate enables application submission.

Generating a Certificate Signing Request

To request a Distribution Certificate, you first need to generate a Certificate Signing Request (CSR) utilizing the Keychain Access application in Mac OS X. The creation of a CSR prompts Keychain Access to simultaneously generate your public and private key pair, establishing your Distribution identity. Your private key is stored in the login Keychain by default and can be viewed in the Keychain Access application under **Keys**.

To generate a CSR:

1. In your **Applications** folder, open the **Utilities** folder and launch **Keychain Access**.
2. Choose **Keychain Access > Certificate Assistant > Request a Certificate from a Certificate Authority**.
   NOTE: If you have a private key highlighted (**Request a Certificate From a Certificate Authority with <Private Key>**) in the Keychain during this process, the resulting Certificate Request will not be accepted by the Provisioning Portal.
3. In the **User Email Address** field, enter your Enterprise Development account. Ensure that the email address entered matches the information that was submitted when you registered as a Developer.
4. In the **Common Name** field, enter Company_name.
5. Leave the CA Email Address blank. No CA Email Address is required.
6. Select the **Saved to Disk** radio button.
7. Click **Continue**.
8. Specify a file name and click **Save**.
9. Click **Continue**. The Certificate Assistant creates a CSR file on your desktop.

Submitting a Certificate Signing Request for Approval

Complete this procedure after generating a CSR.

1. Log in to the Provisioning Portal and navigate to **Certificates > Distribution.**
2. Click the **Add Certificate** button.
3. Click **Upload File** and browse to the CSR file.
4. Click **Submit**.
5. Approve your Distribution Certificate.

Downloading and Installing Distribution Certificates

1. In the **Certificates > Distribution** section of the Portal, control-click the **WWDR Intermediate Certificate** link and select **Saved Linked File to Downloads** to initiate download of the certificate.
2. After downloading, double-click the certificate to launch Keychain Access and install.
3. In the same area of the Provisioning Portal, click on the name of the Distribution Certificate to download.
4. On your local machine, double-click the downloaded .cer file to launch Keychain Access and install your certificate.

Saving your Private Key and Transferring to Other Systems

It is critical that you save your private key somewhere safe in the event that you need to build your application on multiple Macs or decide to reinstall your system OS. Without your private key, you cannot sign binaries in Xcode and will be unable to upload your application to the App Store or install your application on any Apple device. When a CSR is generated, the Keychain Access application creates a private key on your login keychain. This private key is tied to your user account and cannot be reproduced if lost due to an OS reinstall. If you plan to do development and testing on multiple systems, you need to import your private key onto all of the systems you'll be doing work on.

To export your private key and certificate for safe keeping:

1. Open the **Keychain Access Application** and select the **Certificates** category.
2. Highlight the certificate associated with your Distribution Certificate. Tap the arrow beside it to show the private key associated with it. Highlight both using Shift and select **File > Export Items**. Save your key in the Personal Information Exchange (.p12) file format.
   A prompt displays to create a password that will be used when you attempt to import this key on another computer.
3. Enter the password.
4. You can now transfer this .p12 file between systems. Double-click on the .p12 to install on a system. You will be prompted for the password you first entered above.

Creating and Downloading your Distribution Provisioning Profile for Distribution

To successfully build your application with Xcode for distribution via the App Store, you first need to create and download an App Store Distribution Provisioning Profile. These are different than the Development Provisioning Profiles that were used earlier in that Apple will only accept applications if they are built with an App Store Distribution Provisioning Profile.

NOTE: App Store provisioning profiles do not allow for a distribution built application to be installed on an Apple device.

To install your distribution ready application on a device, create an Ad Hoc provisioning profile:

1. Navigate to the **Provisioning** section of the **Provisioning Portal** and select the **Distribution** tab.
2. Select the **In House** radio button.
3. Enter the name for your Distribution Provisioning Profile.
4. Confirm your Distribution Certificate has been created and is displayed.
5. Select your wild-card App ID to build all of your applications with your single Distribution Provisioning Profile and click **Submit**.
6. Click on the name of the Distribution Provisioning Profile to download the .**mobileprovision** file.
7. Drag the .mobileprovision file onto the Xcode or iTunes icon in the dock to install.

Connecting InfoPath Form Lists and Libraries

Colligo Engage supports the viewing, editing, and creating of InfoPath forms in both lists and libraries. This feature is only available when users are online; however, InfoPath list items can be viewed when offline, and new items can be added by filling out the fields in list form, and the item is then uploaded on the next sync.

InfoPath Constraints and Supported Settings

InfoPath form types supported:

- InfoPath forms created for SharePoint Lists and SharePoint Form Libraries
- Web browser compatible forms

InfoPath Filler Forms, or any filler-specific controls, are not supported.
InfoPath rules (for field and button verification) and data connections are supported.
Additionally, Digital Signatures are currently untested.

Ribbon Commands

The following ribbon commands are supported:

- Submit
  NOTE: All submission options are supported, though only submitting to a SharePoint document library has been tested
- Save
- Save As
- Close
- Update

The following ribbon commands are not supported:

- Views
- Print Preview
  NOTE: These commands are actively hidden by Engage because they are not applicable to the iPad, iPhone, or iPod Touch

InfoPath Control Support

The following controls are supported for InfoPath Form Lists:

- Text Box
- Rich Text Box
- Drop-down List
- Check Box
- Option Button
- Date Picker
- Date/Time Picker
- List Box
- Person/Group Picker
- Button
- Calculated Value
- All containers
- Web browser compatible custom controls are also supported

The following controls are not supported for InfoPath Form Lists:

- File or picture attachments.
- Users can manually attach files/pictures/sketches to InfoPath Form List items through the Colligo Engage iOS app.

The following controls are supported for InfoPath Form Libraries:

- Text Box
- Rich Text Box
- Drop-down List
- Combo Box
- Check Box
- Option Button
- Date Picker
- Date/Time Picker
- Multiple-Selection List Box
- List Box
- Bulleted List
- Numbered List
- Plain List
- Person/Group Picker
- Button
- Calculated Value
- All containers
- Hyperlink
- Picture
- Web browser compatible custom controls are also supported

The following controls are not supported for InfoPath Form Libraries:

- Picture Button
- Ink Pad/Signature
- File Attachment

Viewing InfoPath forms

All saved/submitted InfoPath forms (xml) are viewable as forms outside form libraries as long as the corresponding .xsn files are accessible to the Colligo Engage iOS App. For example: If a form in library A is filled out and submitted to library B, users who access the submitted .xml file in Library B should have no issues viewing that .xml file as an InfoPath form, as long as the .xsn associated with that form is accessible to the user.