Link to article: https://discover.claromentis.com/knowledgebase/articles/622/requesting-custom-native-mobile-app-for-ios-and-android

Requesting Custom Native Mobile App for iOS and Android

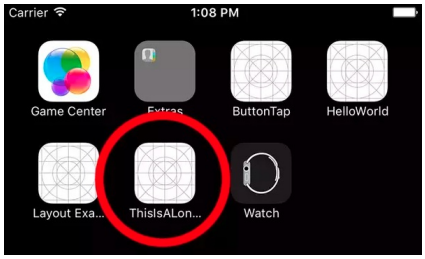
Why your company may need a Custom Native Mobile App?

Your company or organisation may need a dedicated app for the following reasons:

- White-label - a dedicated app that reflects a company's branding
- Your organisation wish to deploy the app for your staff through Mobile Device Management (MDM)
- The system is not available publicly and requires a custom way to connect such as VPN or by installing other apps.
- Your system may require additional security or restriction.
- You are using Single Sign On (SSO) based on ADFS that requires custom authentication.
- You require **push notification** to the devices.

Requirements for Native Mobile App

- **Final publicly accessible URL** to your intranet with SSL (https://). Please note that the URL is embedded within a compiled version of the app, and changing the URL requires rebuilding and releasing a new version of the app.
- **URLs for SSO (Single Sign On) Authentication.** If your system uses SSO to authenticate users, such as Microsoft Entra, Okta, Ping or Duo, please provide SSO Authentication URLs. For example https://auth.pingone.com, https://login.microsoftonline.com
- **Graphic for App Icon** (min resolution 1536x1536 pixels in PNG format. Keep things simple and avoid having text unless it is part of the logo.read more
- **App name** (keep it short, ideally less than 12 characters if possible - so that it fits without being truncated on mobile devices)
- **App description**
- **A dummy claromentis user account (and password,)** unless specified, we will create a dummy user account for App Review called 'mobileapp"
- **Link to your privacy policy - a**publicly accessible web page or PDF must include your app's name, or the legal entity, for example, developer or company.



How to request

Contact your Project Manager or

Submit Change Request

Publishing Mobile App

There are three ways you can publish and distribute your mobile apps to your users.

IMPORTANT CHANGE to Apple Enterprise Distribution Programme
Apple is changing their policy on Enterprise Distribution Programme and our membership is expiring on 24th May 2023.

1. Claromentis Unlisted App Distribution App Store

iOS

Claromentis by nature is an Internal app and Apple has recommended The unlisted app distribution allowing users to download the app directly from Public AppStore only by specific links.

The app won't be promoted in the AppStore to ensure only users with access to the link can download the app.

This is the default route if you don't have your own Developer Account or a specific way to distribute an enterprise app for your organisation through MDM (Mobile Device Management)

The link to download your app will be available from

```
https://apps.claromentis.net/[app_name]
```

Please note that Apple implements the same rigorous checks as regular apps in Public App Store and this process can take up to 4 weeks.

The benefit of this method is that there are no requirements to renew Enterprise Distribution Certificates every year and the user doesn't have to perform the extra step of Trusting Enterprise Developer.

If Automated is enabled the app will be updated automatically for the user just like the regular app and it also can be backed up in iCloud.

Android

Your app will be available in Google Play and it will be discoverable by searching. If you don't want your app to be published in Google Play please let us know and it will be available instead to download *.apk file.

2. Your Company Developer Account or Enterprise Mobile Distribution

If your company has its own Enterprise Mobile Distribution with Apple and Google Play you can add us to your development team so that we can submit the app on behalf of your company. Claromentis is acting only as **Mobile Developer.**

iOS: App Store Connect

Please add `claromentis@claromentis.com` to your mobile development team allowing us to publish the app under this account.

Google Play Store

Please add `michael.christian@claromentis.com` to your mobile development team in Google Play Console.

On-Prem Push Notification Firewall Requirements

HTTPS. All traffic to the REST API uses HTTPS on standard port 443.

Firewalls and proxies must allow outbound HTTPS traffic on port 443 to connect to OneSignal REST API.

IP Addresses: OneSignal's infrastructure dynamically assigns IP addresses for the REST API from a large range of Cloudflare IP addresses, and those IP addresses can change without advance notice.

We recommend whitelisting HTTPS traffic to any public IP address or allowing `api.onesignal.com`. Be sure your DNS cache respects OneSignal's TTL of 60 seconds to avoid making requests to stale IP addresses.

TLS 1.2 connection or higher

FAQs

Our users connect to our intranet via VPN, will it work with the app?

Your users need to be connected to the VPN using the equivalent VPN app on their mobile prior to using the app.

Created on 27 September 2019 by Michael Christian. Last modified on 28 August 2025
Tags: app, custom, mobile