



# Microsoft Azure Active Directory: EmployeeConnect Mobile App Setup

# CREATE AN APP REGISTRATION



1. Login to Azure portal using your administrator account.
2. Navigate to **Azure Active Directory** and select **App Registration**
3. Click **New registration**

+ New registration | Endpoints | Troubleshooting | Download | Preview features | Got feedback?

Try out the new App registrations search preview! Click to enable the preview. →

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to support (MSAL) and Microsoft Graph. [Learn more](#)

All applications | Owned applications | Deleted applications (Preview) | Applications from personal account

Start typing a name or Application ID to filter these results

4. Let's name it "**EmployeeConnectMobileAuth**" and select "**Accounts in any organizational directory (Any Azure AD directory - Multitenant)**"
5. Leave the Redirect URI as blank. We will configure this afterwards, hit Register to continue
6. After Registration you will be redirected to **EmployeeConnectMobileAuth** App Registration **Overview** page. (If not, navigate to EmployeeConnectMobileAuth, under App Registration, under side menu select **Overview**) Take note of the client ID and tenant ID, you will need to send these IDs to Employee Connect via email after the setup.

# EmployeeConnectMobileAuth

Search (Ctrl+/) << Delete Endpoints Preview features

Overview

- Quickstart
- Integration assistant

Manage

Essentials

Display name : EmployeeConnectMobileAuth

Application (client) ID : [redacted]-651845c1c8ec

Directory (tenant) ID : [redacted]-7dde140ad6c8

Object ID : [redacted]-3c53ca6e9641

+ New registration Endpoints Troubleshooting Download

Try out the new App registrations search preview! Click to enable the preview. →

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory security updates but we will no longer provide feature updates. Applications will need to be updated to continue to work.

All applications Owned applications Deleted applications (Preview)

EmployeeConnect Mobile

Display name

EM EmployeeConnect Mobile Auth

7. Under the side menu, select **Authentication**

8. To add iOS platform, Click **Add a platform**

# EmployeeConnectMobileAuth | Authentication

Search (Ctrl+/) << Save Discard Got feedback?

Overview

- Quickstart
- Integration assistant

Manage

- Branding
- Authentication

Platform configurations

Depending on the platform or device this application is to redirect URIs, specific authentication settings, or fields specific

+ Add a platform

Supported account types


9. Select **iOs / macOS**

# Configure platforms




## Web applications


 **Web**  
Build, host, and deploy a web server application. .NET, Java, Python

 **Single-page application**  
Configure browser client applications and progressive web applications. Javascript.

## Mobile and desktop applications

 **iOS / macOS**  
Objective-C, Swift, Xamarin

 **Android**  
Java, Kotlin, Xamarin

 **Mobile and desktop applications**  
Windows, UWP, Console, IoT & Limited-entry Devices, Classic iOS + Android

10. Set value of **Bundle ID** to "**com.microinfosoft.employeeconnect**" and hit **Configure** button to continue.

# Configure your iOS or macOS app



[← All platforms](#)

[Quickstart](#) [Docs](#)

Configuring your iOS or macOS app enables your users to get SSO and seamlessly access your application.

You will be able to change this later.

## Bundle ID

Your app's Bundle ID can be found in XCode in the Info.plist or 'Build Settings'.


11. To add Android platform, under Authentication, Click **Add a platform**
12. Select **Android**

# Configure platforms




## Web applications


 **Web**  
Build, host, and deploy a web server application. .NET, Java, Python

 **Single-page application**  
Configure browser client applications and progressive web applications. Javascript.

## Mobile and desktop applications

 **iOS / macOS**  
Objective-C, Swift, Xamarin

 **Android**  
Java, Kotlin, Xamarin

 **Mobile and desktop applications**  
Windows, UWP, Console, IoT & Limited-entry Devices, Classic iOS + Android

13. Set value of **Package Name** to "**com.microinfosoft.employeeconnect**", Set Signature hash to "**mt1H8n65fM2UZzeTYRsp6gDfHMg=**" and hit **Configure** button to continue.

# Configure your Android app



[← All platforms](#)

[Quickstart](#)

[Docs](#)

Configuring your Android app enables your users to get device-wide SSO through the Microsoft Authenticator and seamlessly access your application.

You will be able to change this later.

## Package name

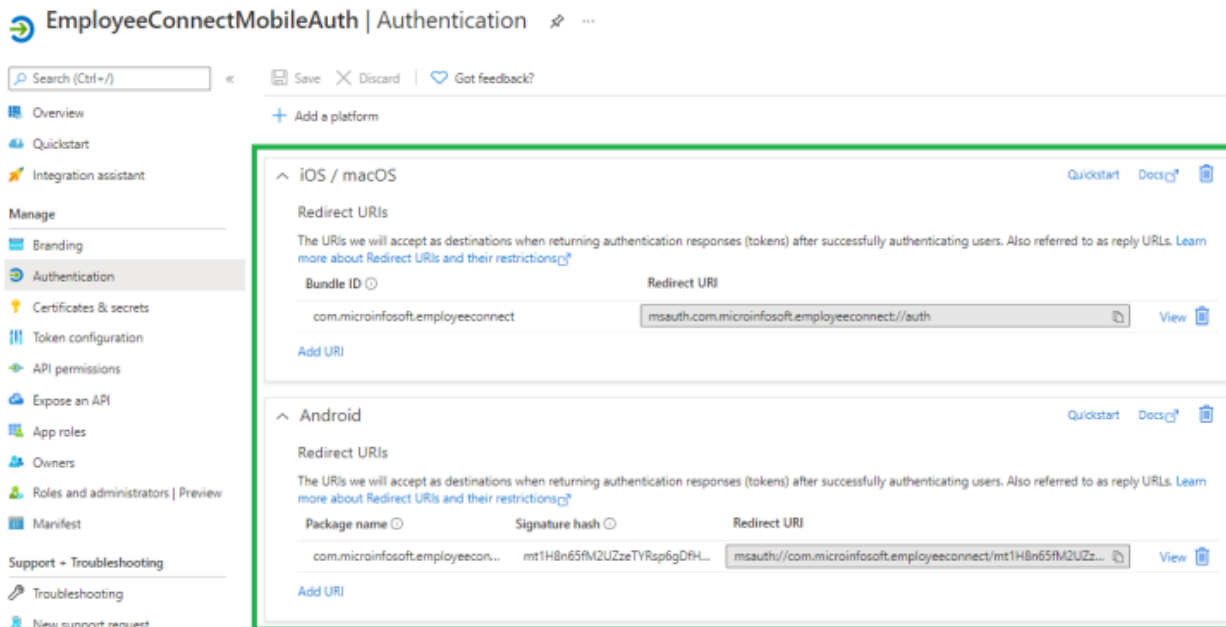
Your app's Package Name can be found in the Android Manifest.

## Signature hash

The Signature Hash can be generated via command line.

The signature hash must be unique within the package.

14. After configuring **Authentication** both for **iOs** and **Android** make sure all changes were saved, you should have something like the screenshot below.



## SEND AZURE ACTIVE DIRECTORY DETAILS VIA EMAIL

Please send an email to elisha.sagcal@employeeconnect.com cc: [ari@employeeconnect.com](mailto:ari@employeeconnect.com) attached with the following details located on the **Overview** page of the App Registration we created:

1. Application (client) ID - xxxxxxxx-xxxx-xxxx-xxxx-651845c1c8ec
2. Directory (tenant) ID - xxxxxxxx-xxxx-xxxx-xxxx-7dde140ad6c8



# LOGGING INTO EMPLOYEE CONNECT APP

1. After being advised of a successful AAD SSO integration by Employee Connect, download **Employee Connect App** on App Store (iOS) or Play Store (Android)
2. Open **Employee Connect App**
3. Input the **Username** of the employee that uses AAD (Note: make sure that the Employee Connect user's Login is configured as "AAD SSO").
4. Tap on "**Log in via Azure AD**"
5. You will then be redirected to a page where you can input your AAD password.

