Ping One Authentication Integration Module Installation Instructions [v1.0 Date: 9/29/2021]

Revisions: v1.0 Date: 9/29/2021

Introduction

Ping Identity's Ping One offering provides a Customer Identity Access Management platform (CIAM) as a service.

Key Features

- Customer authentication authority: centralized authentication services allow you to connect a user in any directory, accessing any app, hosted in any cloud, in any situation
- SSO and adaptive authentication across all apps
- Embed customer-friendly multi-factor authentication (MFA) in custom apps, or use SMS or email OTPs
- Self-service SSO integrations and delegated administration for application teams
- A single view of your customers across all applications

https://www.pingidentity.com/en/solutions/customer-identity/pingone.html

This document details how to install and configure a Ping One managed authentication to a Mendix web application. Further configuration and customization is required to take your application from test to practical usage. This module is not maintained by Mendix R&D.

Mendix Version 8.17+

Main steps:

1. **Install & Configure Pre-Requisite Marketplace Modules**
2. **Ping One Console – Provider Configuration**
3. **Ping One Integration Module – Module Configuration**

1. Install Pre-Requisite Marketplace Modules

In your Mendix application in install OIDC and related modules to support the Ping One Authentication Integration module.

1.2 OIDC Module Installation & Configuration

Add the OIDC Mendix store application and follow the _Documentation instructions within the module until you reach the step "OIDC Provider Configuration:" before continuing to the steps below.

As instructed, install the pre-requisite module and widget items called for by the OIDC module _Documentation instructions.

1.3 OIDC Module Modifications

1. Oauth2 script – Change OIDC module OIDC.Oauth2 script to target microflow PingOne_Integration.WebCallBack & save the form. Delete the state and code parameters and then re-add these followed by a second save form action

2. Delete the OIDC.Token_User association and place a new 1:1 association from OIDC.Token entity to Administration.Account. Set Access for Administrator of full rights to create, delete and read, write on all members. Allow the user context delete and read members objects.

3. Exclude the following components from project
    a. 1 - Provisioning \ User Provisioning Examples
        i. "Snip_Configuration"
    b. 2 - Login Flow \ b. Mobile
        i. "Login_Mobile_Automatic"
        ii. "Login_Mobile_Button"
    c. 4 - Logout
        i. "ACT_Logout"
    d. Implementation \ 0. Configuration \ Client Config
        i. "DS_ClientConfigHelper_Edit"
        ii. "DS_ClientConfigHelper_New"
        iii. "OIDC_Client_NewEdit"
        iv. "Token_NewEdit"
    e. Implementation \ 1. Start Login \ In App Browser
        i. "OL_RegisterAndStartLogin"
    f. Implementation \ 1. Start Login \ Web View
        i. "ACT_OpenLoginInWebVew"
    g. Implementation \ 1. Start Login
        i. "OL_RegisterDeepLink"
        ii. "SUB_RegisterMobileDeeplink"
    h. Implementation \ 2. Callback \ a. Web
        i. "webCallback"
    i. Implementation \ 2. Callback \ b. Mobile \ Helpers
        i. "HandleDeeplink"
        ii. "MobileCallback"
        iii. "SUB_HandleLoginDeeplink"
    j. Implementation \ 2. Callback \ Shared
        i. "handleAuthorizationCode"
    k. Implementation \ 5. Logout
        i. "SUB_GetLogoutURL"
    l. Implementation \ 6. Utililties
        i. "GetOrCreateToken"
        ii. "GetToken"

2. Ping One Console – Provider Configuration:

Console Steps Overview

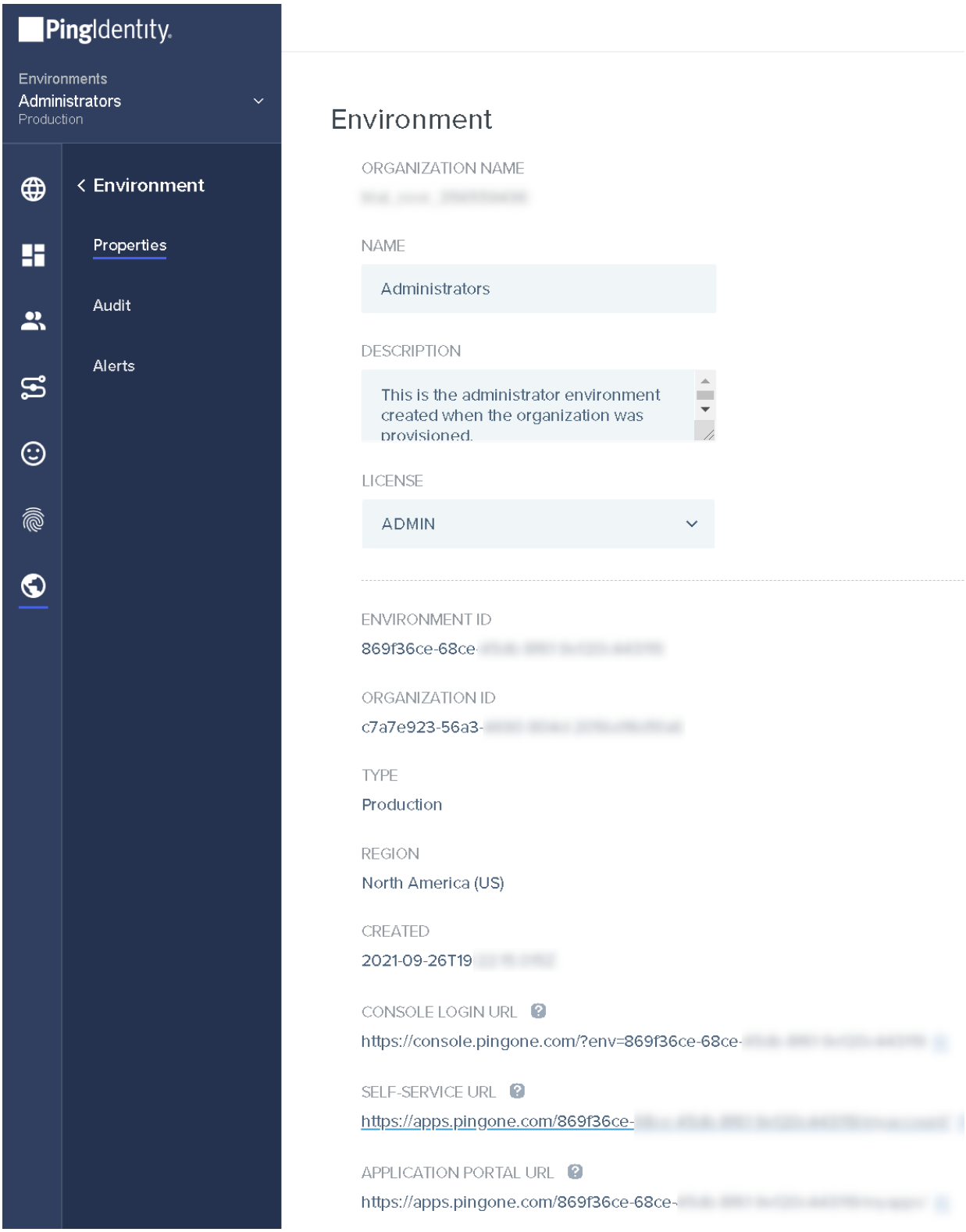
This integration module provides a pathway to modern authentication in your Mendix web app via Ping Identity's Ping One offering. historically were limited to the application & client domain are integrated and managed within an application are able to

Note: These steps may vary slightly for each use case. Settings required by this module are highlighted where applicable. If you need to deviate from such settings the module will need to be customized to accommodate.

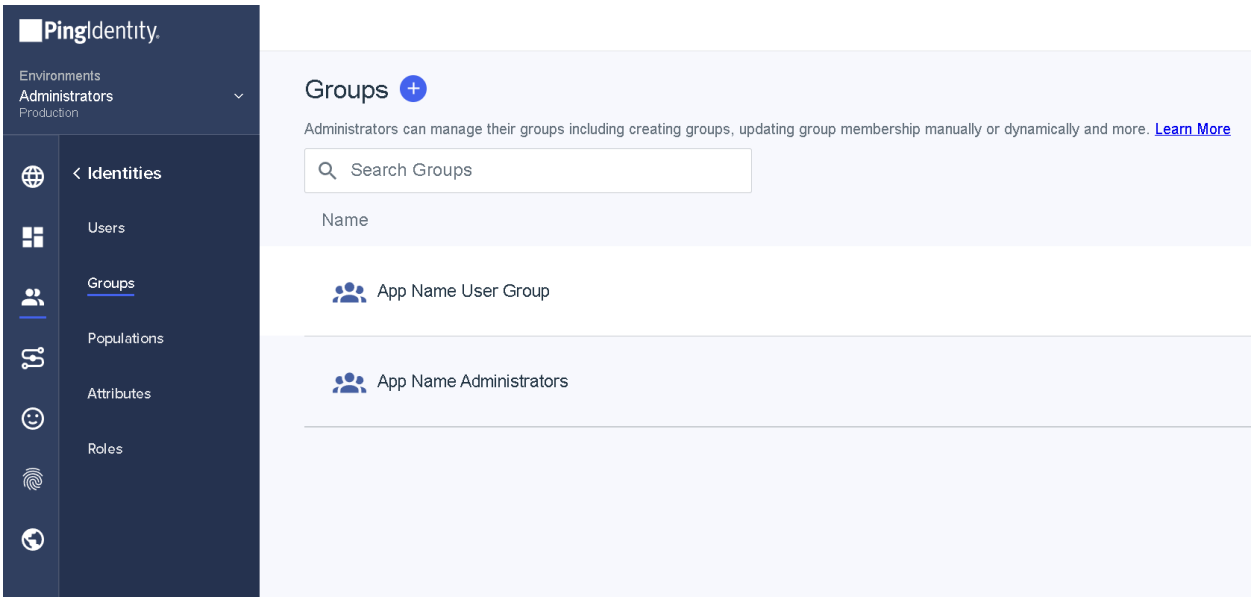
Overview:

- **2-1 Sign up for Ping One Online – A trial may work**
- **2-2 Capture Environment ID & Organization ID**
- **2-3 Configure User Groups**
- **2-4 Configure Populations**
- **2-5 Configure Authentication Policies**
- **2-6 Configure Application**
- **2-7 Optional: Configure Experiences: Log-on branding & Authentication Communication**
- **2-8 Optional: Configure MFA & Custom Password Policies**
- **2-9 Optional: Configure Two Application test users: User & Administrator**

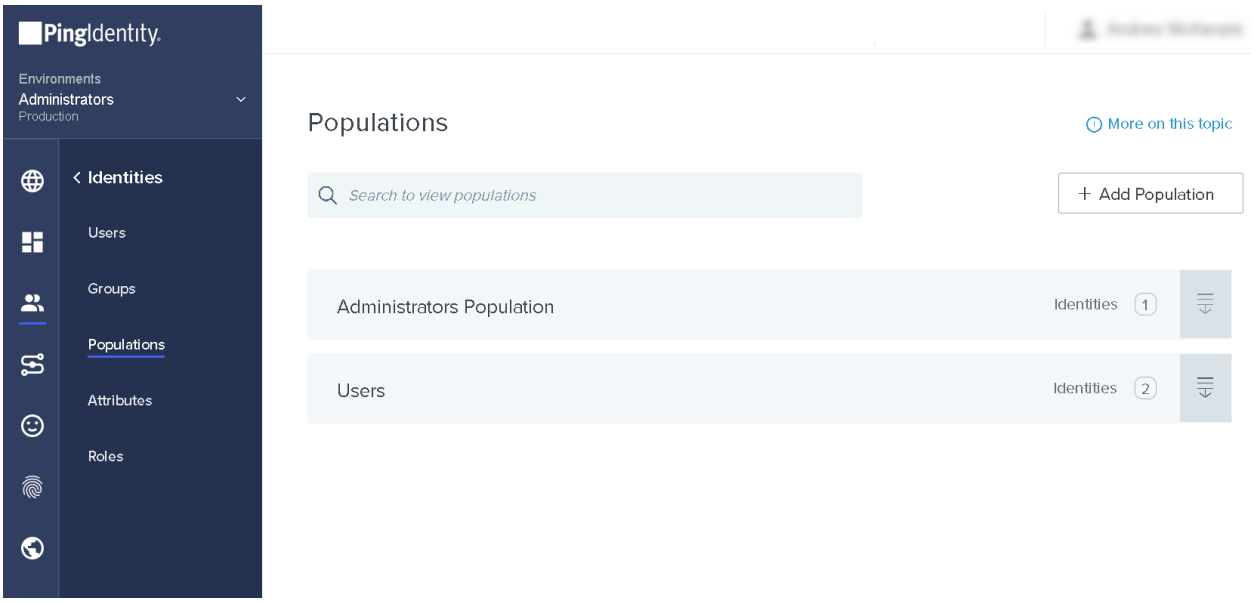
2-2 Capture Environment ID & Organization ID



2-3 Configure User Groups



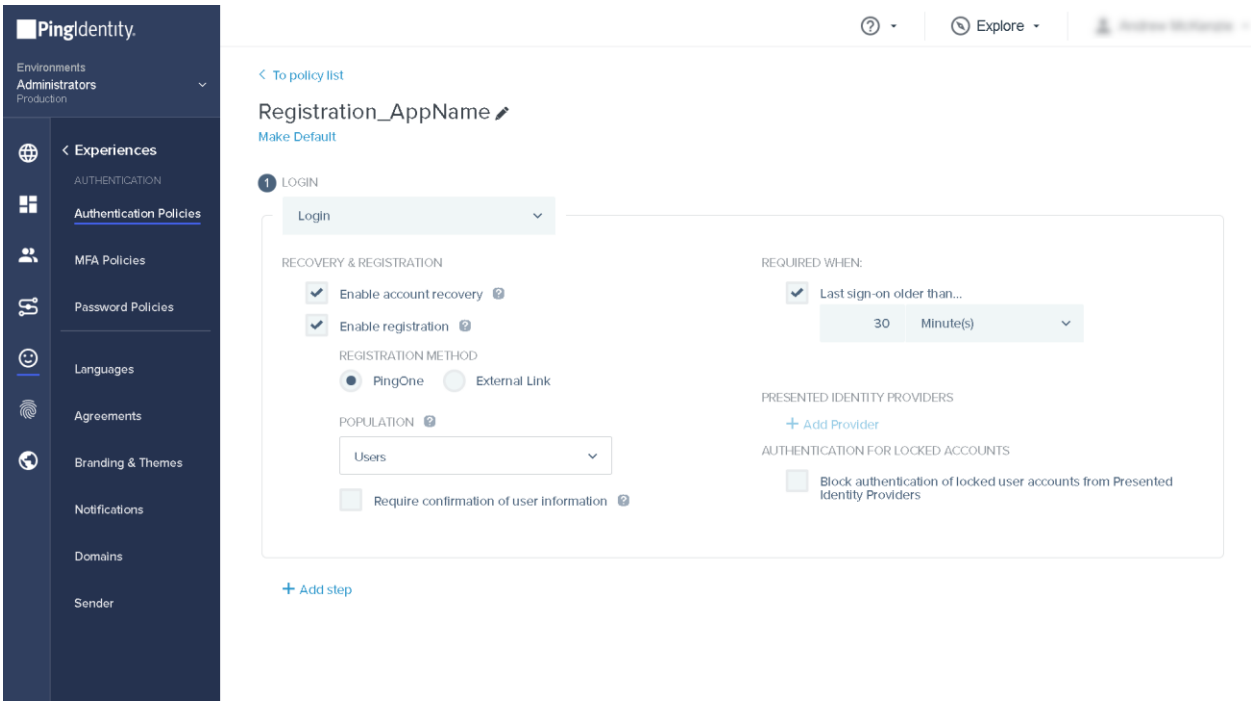
2-4 Configure Populations



2-5 Configure Authentication Policy

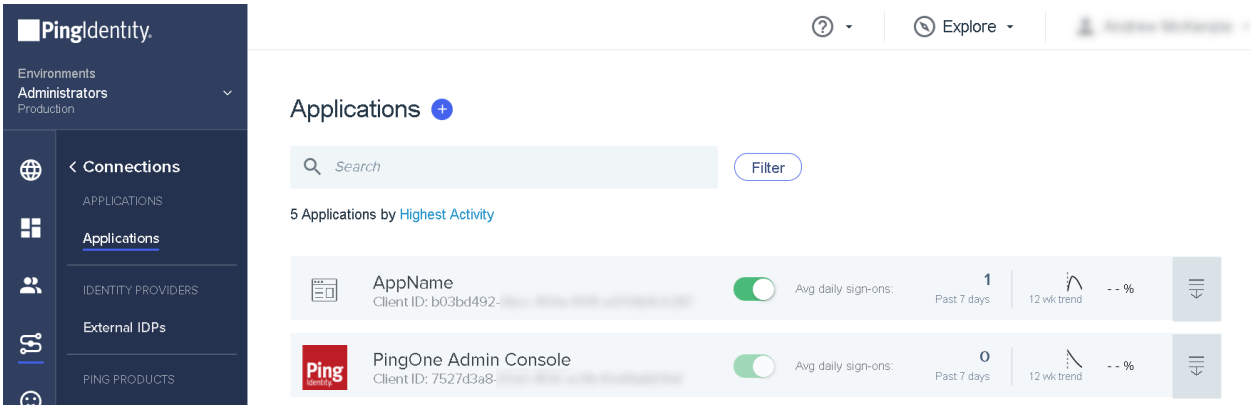
The provided integration assumes registration will be provisioned through integration with Ping One directly, via selections:
- Enable Registration checked; and
- Registration Method “PingOne” selected; and
- Population “Users” (from previous step) selected

This is a required step to utilize this module in its default form, however this configuration may be replaced by custom configuration of this module, which may either take the form of a registration API partner facilitation through the Mendix application or via Registration Method “External Link” below.



2-6 Configure Application

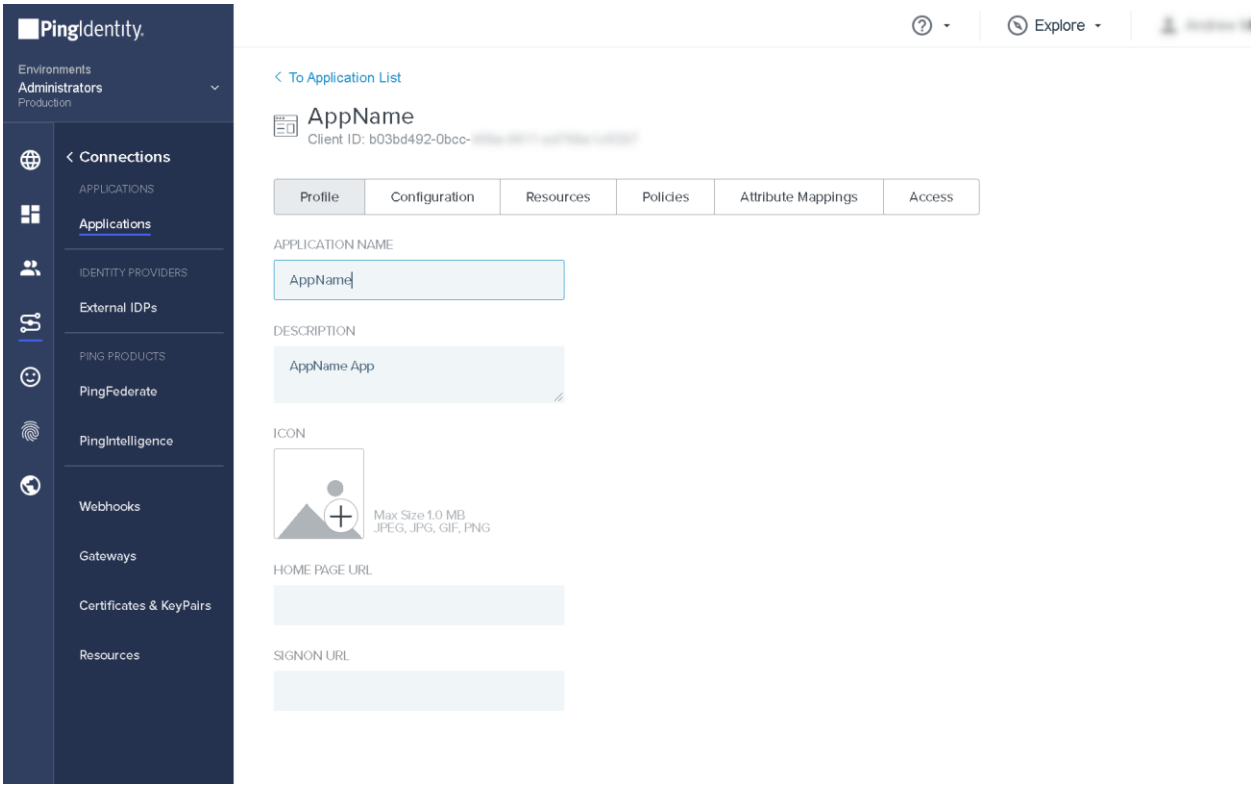
Create/Update Application in Ping One Console



This step has 6 Ping One Console Application setting subsections which are detailed through images and captions qualifying the example and required settings for your application for the default use of this module:

- **2-6-1 Profile**
- **2-6-2 Configuration**
- **2-6-3 Resources**
- **2-6-4 Policies & IDP Partners**
- **2-6-5 OIDC & Ping One API Attribute Mappings**
- **2-6-6 Access**

2-6-1 Configure Application: Profile

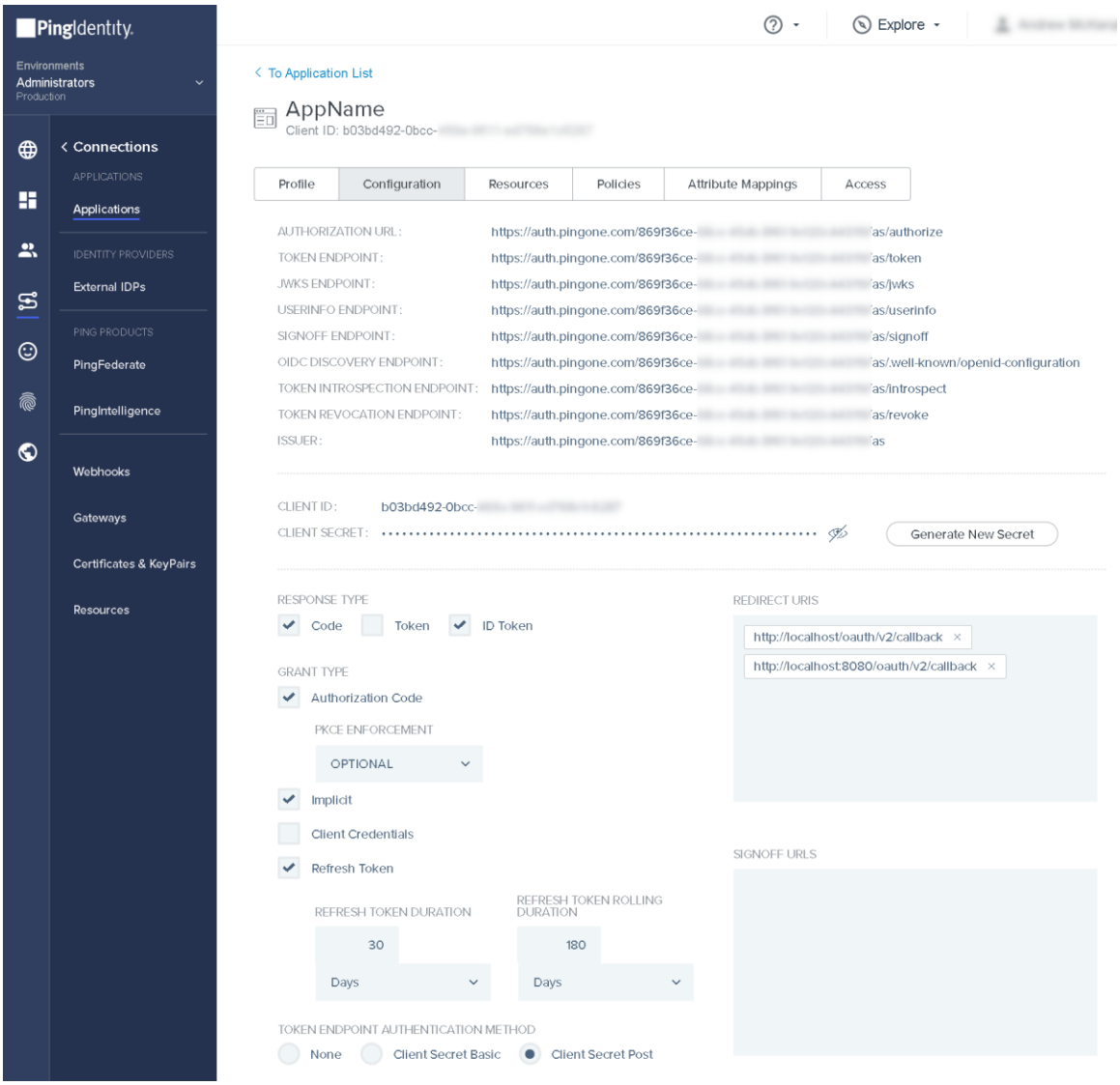


2-6-2 Configure Application: Configuration

- Note down all of the URL and endpoint URI/URLs from this section.
- Set the Response type checkboxes and selections as depicted
- Set your own redirect URIs in the format “URL” + /oauth/v2/callback (http://<your-app-url>/oauth/v2/callback)

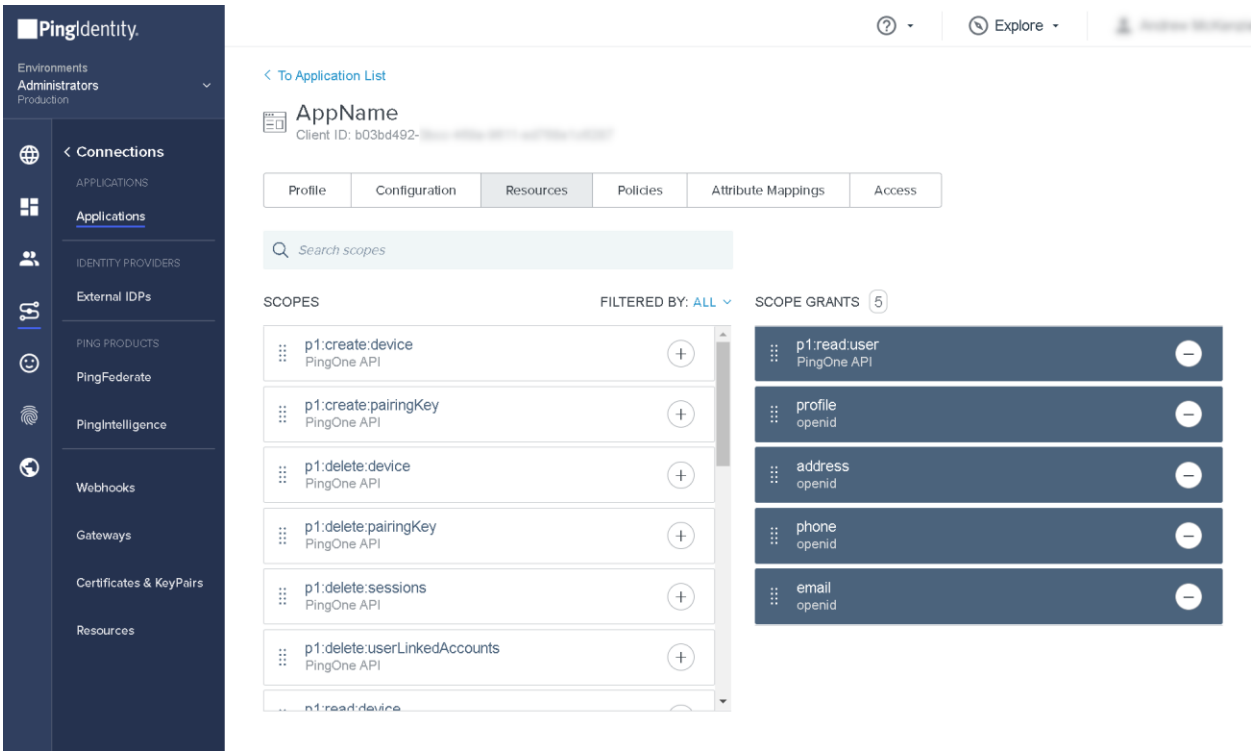
The callback URI you will use for a public facing application will likely be in **https** format for all environments including test and development. In such cases your Mendix application will be set to use TLS in the Mendix developer portal & TLS networking requirements fulfilled by Mendix or Private cloud implementation.

A callback URL of http://localhost/oauth/v2/callback be used to assist development in local implementations in Mendix Studio Pro or where an application is only accessible within a secure domain.



2-6-3 Configure Application: Resources

Add the scope grants as depicted below. When customizing this module for your needs, maintain your scope grants here and ensure the same scope grants set are reflected in the Mendix application as instructed in these instructions.



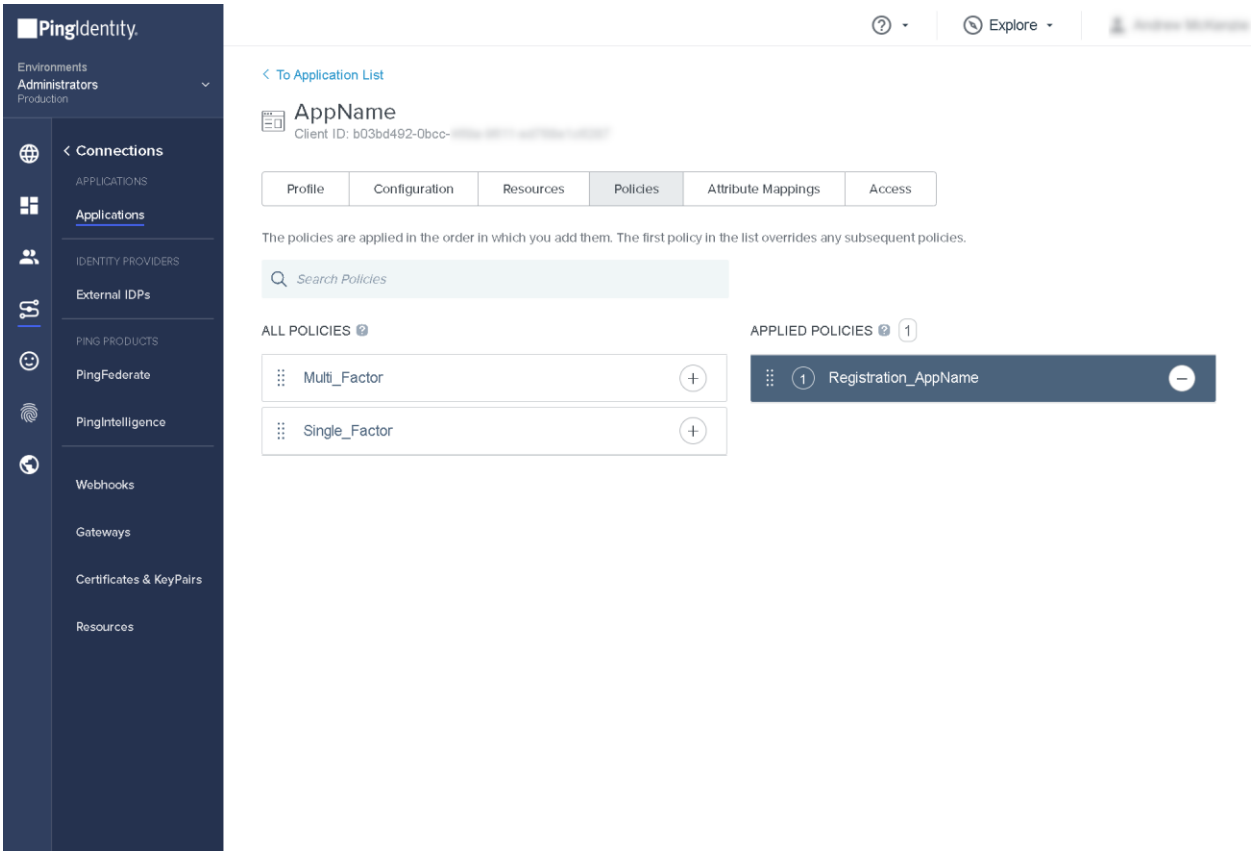
2-6-4 Configure Application: Policies & IDP Providers

Add the login & registration policy you created in Ping Console Step 1.

Optionally add MFA or Single factor policies as required. In some usages, these may be configured without requiring customization of this module as Ping One may facilitate all MFA steps without strictly requiring interaction with the Mendix application.

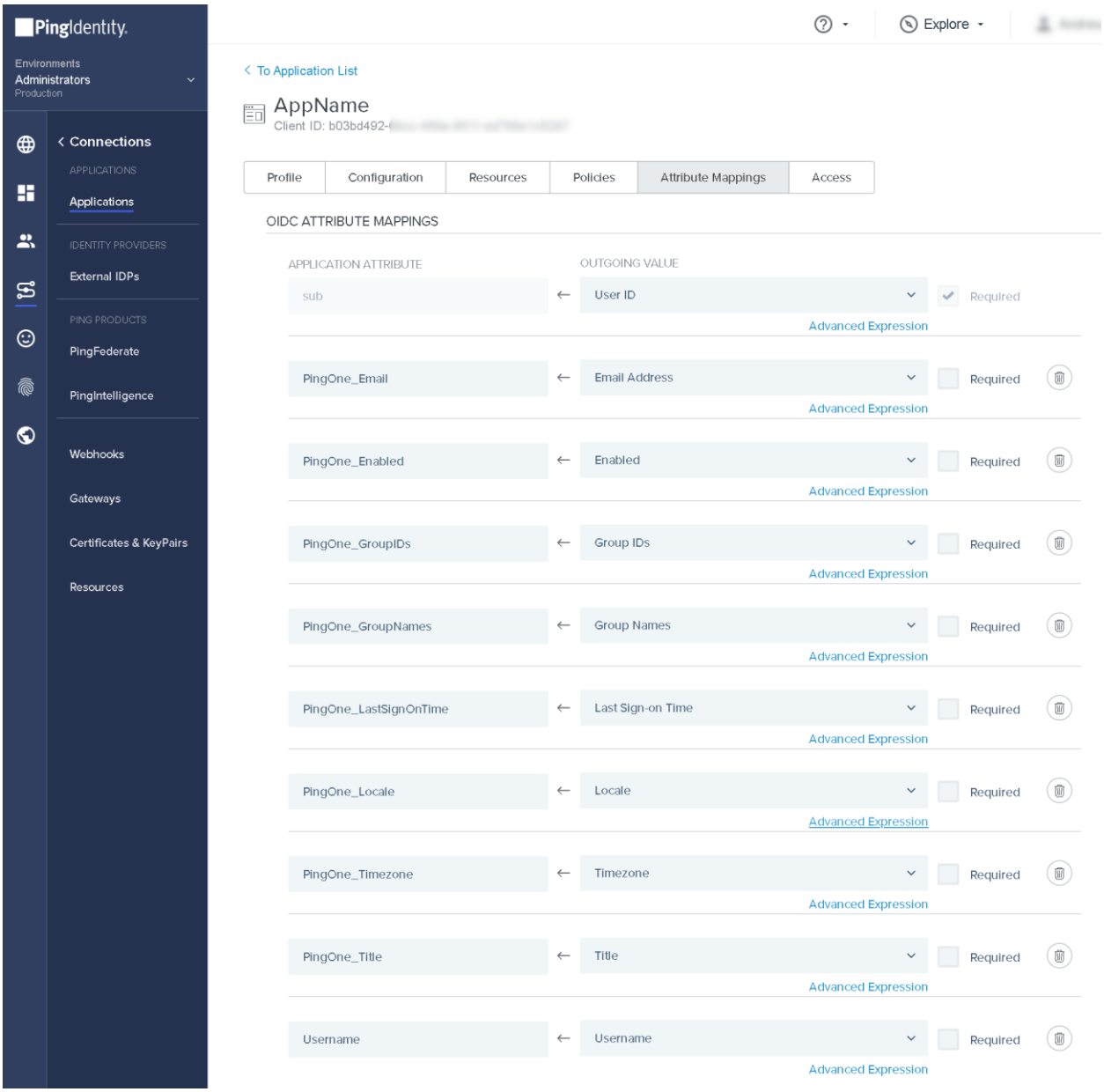
External IDP Partners: E.g. Google sign-on & registration

Under Identity Providers sub menu, you may set relationships with IDPs such as Google to provide other was for users to log in, register for and update personal details on their Ping Account and your Mendix web application.



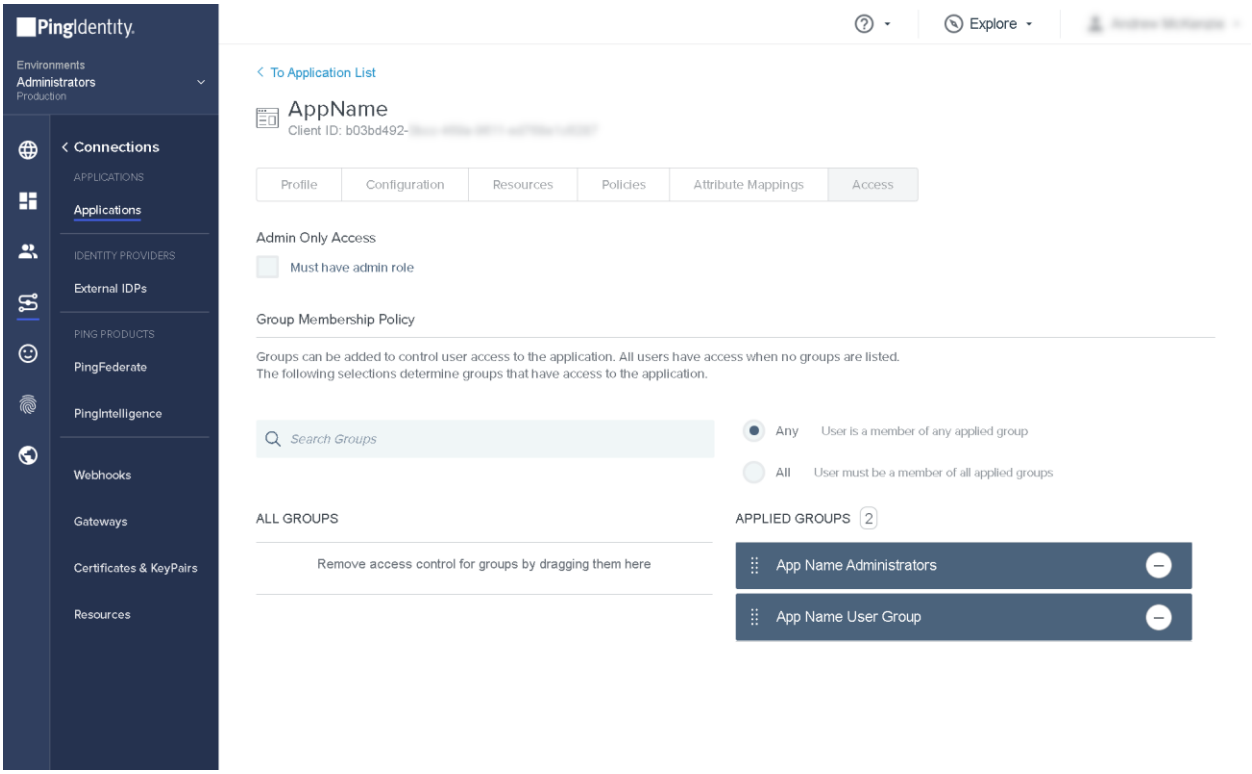
2-6-5 Configure Application: OIDC & Ping API Attribute Mappings

Configure attribute mappings as required. Note that additional fields will only be leveraged in your mendix app if the Ping One Module “Update User” and “Logon P14C” user provisioning & update microflows are customized to map these variables.



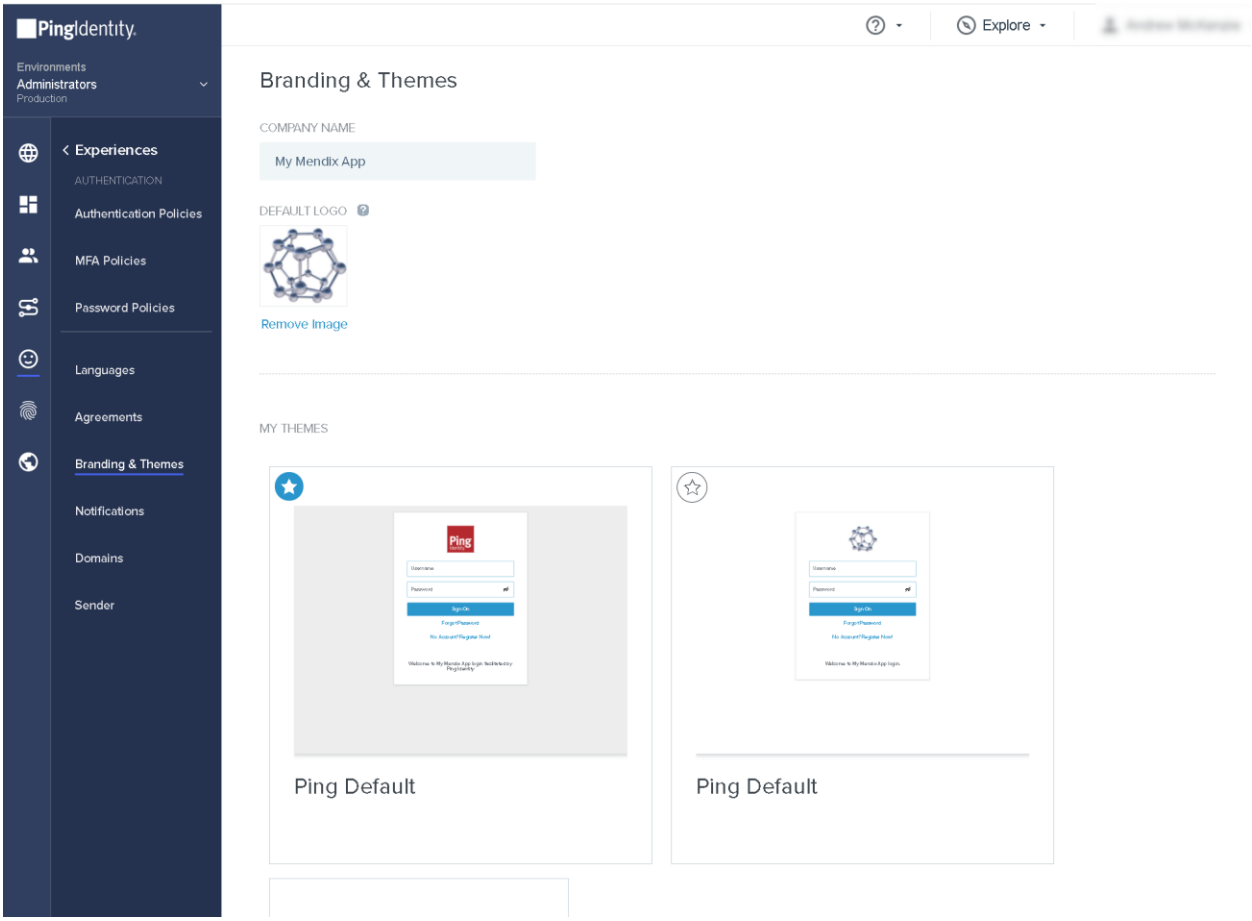
2-6-6 Configure Application: Access

Add the groups you created in Ping One Console Step 1 to Applied groups as depicted below.

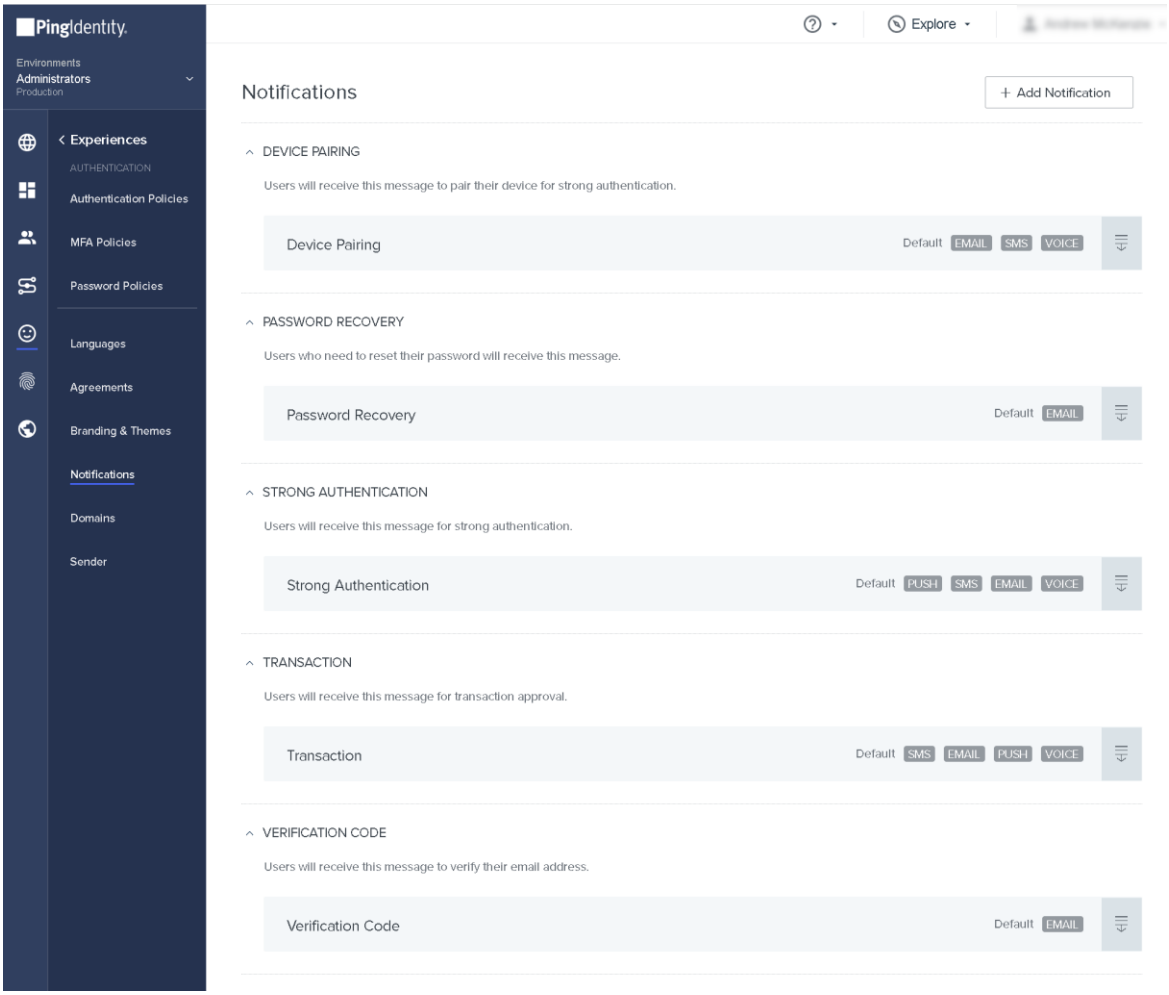


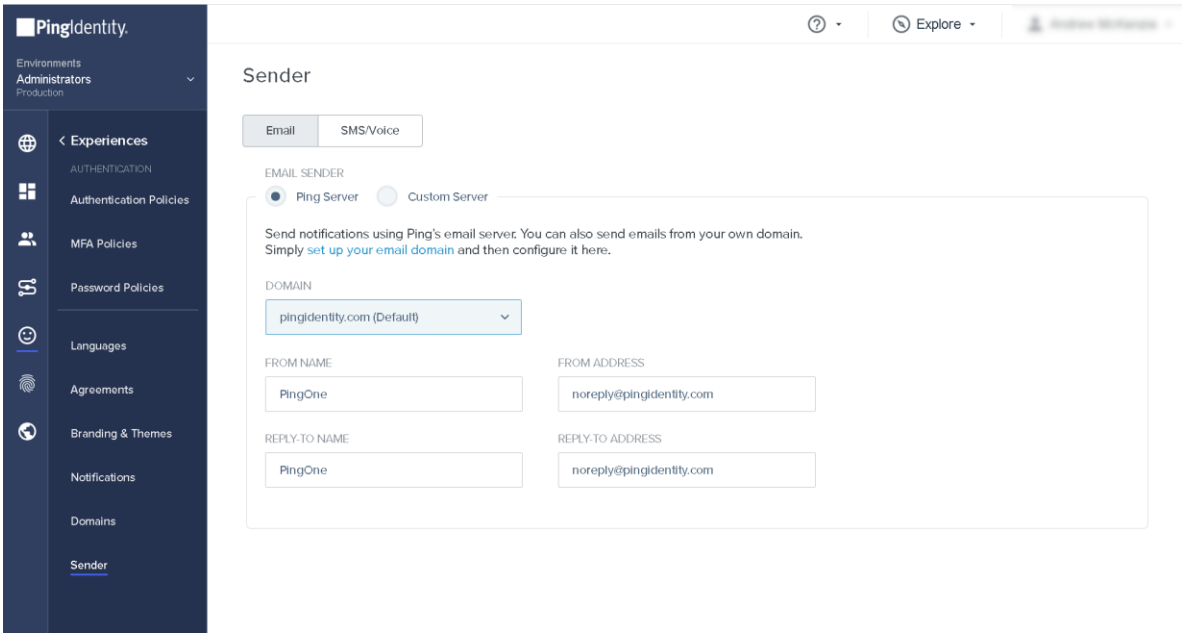
2-7 Optional: Configure Experiences: Log-on branding & Authentication Communication

Under the Experiences menu you may configure Log-on branding and customize aspects of user communication for log on and registration flows. Under sender, you are able to alter the apparent email sender to match your application.



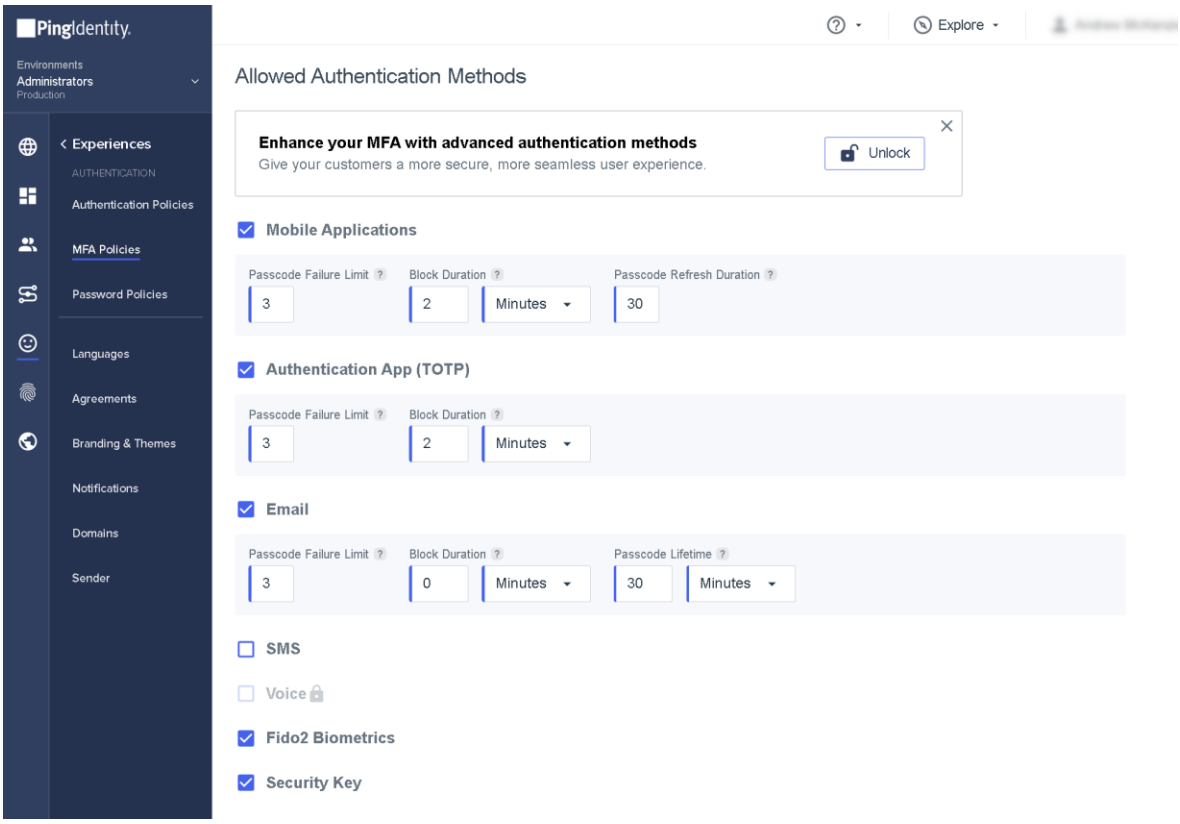
2-7 Optional: Configure Experiences: Log-on branding & Authentication Communication





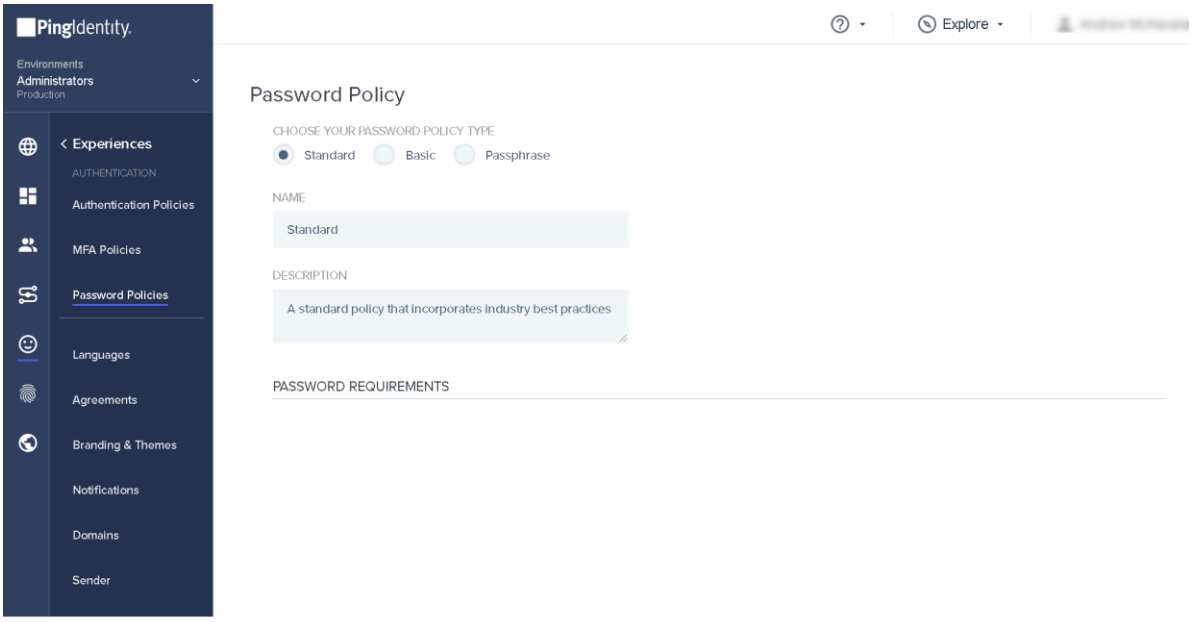
2-8 Optional: Configure MFA & Custom Password Policies

MFA: If you have configured the MFA policy and applied it to your application policies in the Ping One console the following section will need to be set per your needs.



2-8 Optional: Configure MFA & Custom Password Policies

Password Policy: The standard Policy Type may be swapped out for a custom set of requirements in the Experiences – Password policies section. Ensure that any custom policies defined here are included in your Ping One application configuration policies section.



2-9 Optional: Add two test users

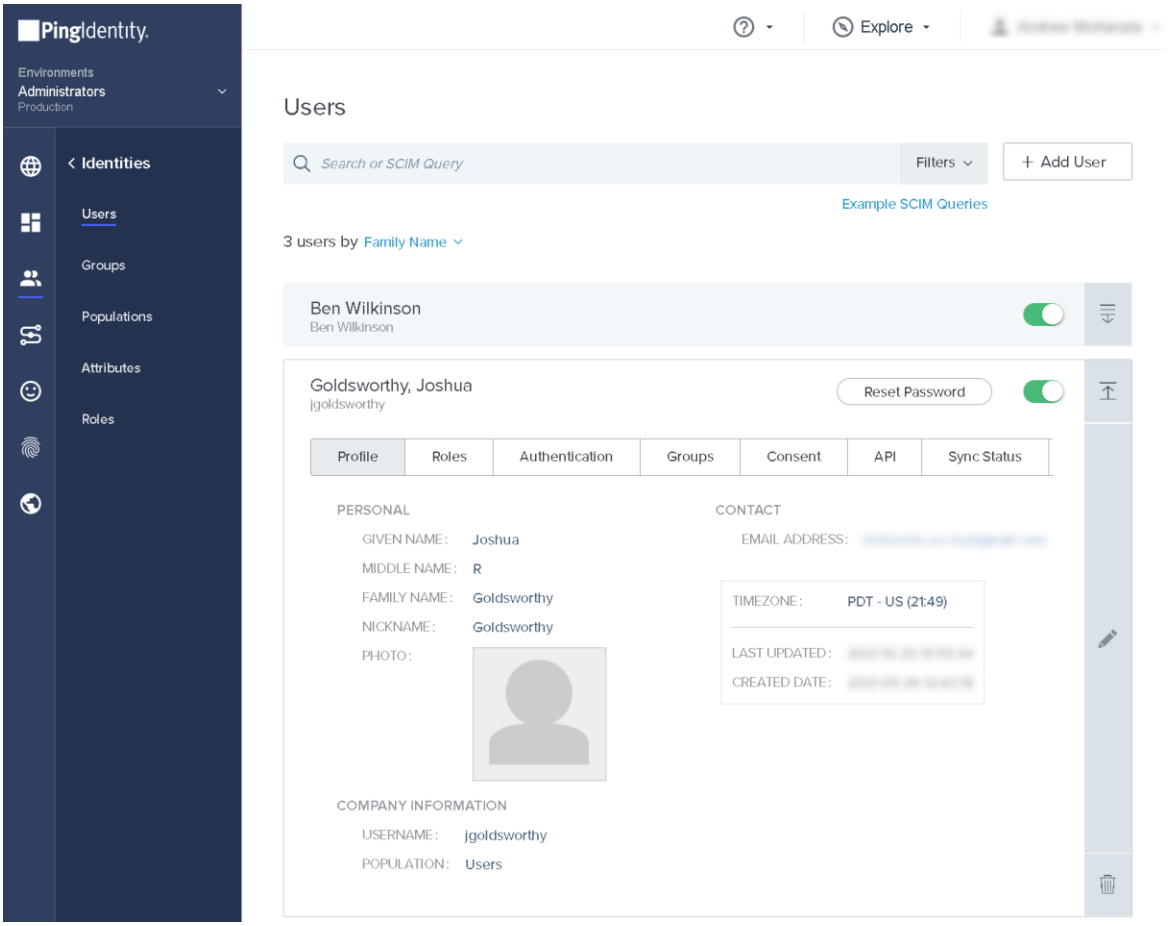
Adding an admin and application user directly via the Ping One Administration Console will assist testing and configuration of your mendix application:

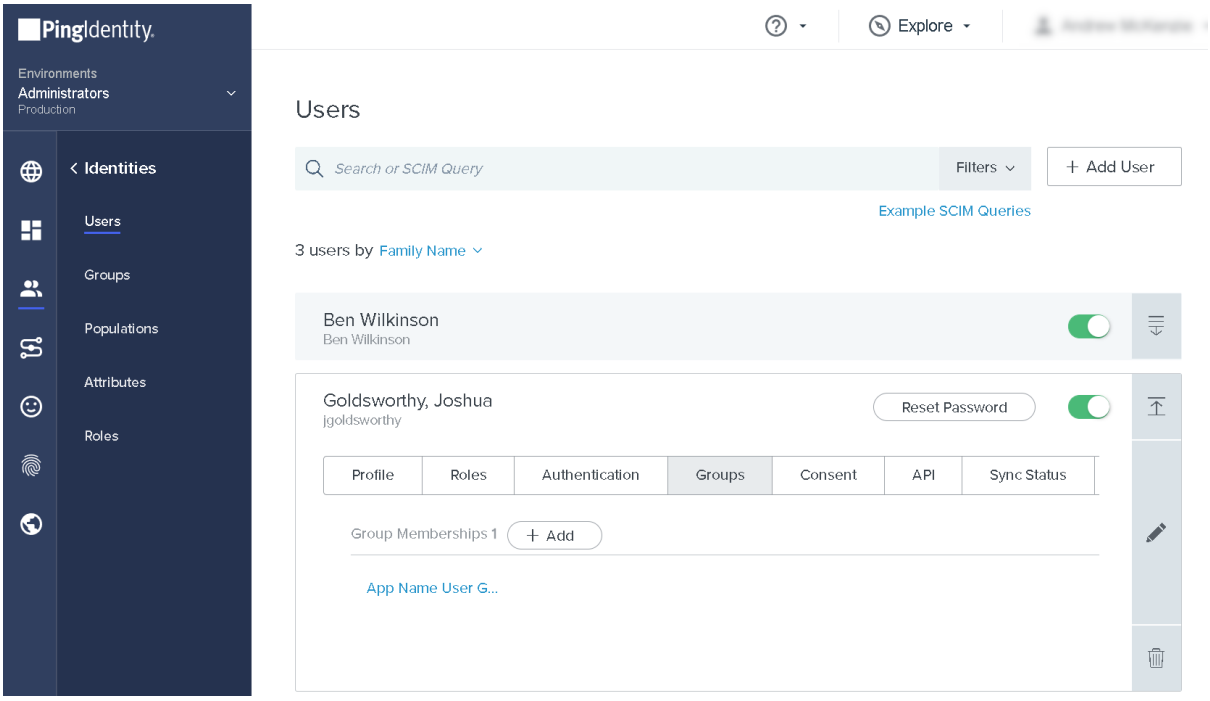
> **User** – Assign group “App Name User Group” and population “Users Population”
>
> **Administrator** – Assign groups “App Name User Group” & “App Name Administrators”, population “Administrators Population” and user roles per image.

Ensure both the user and admin accounts are created with a valid email, first name, last name, username, local and time zone.

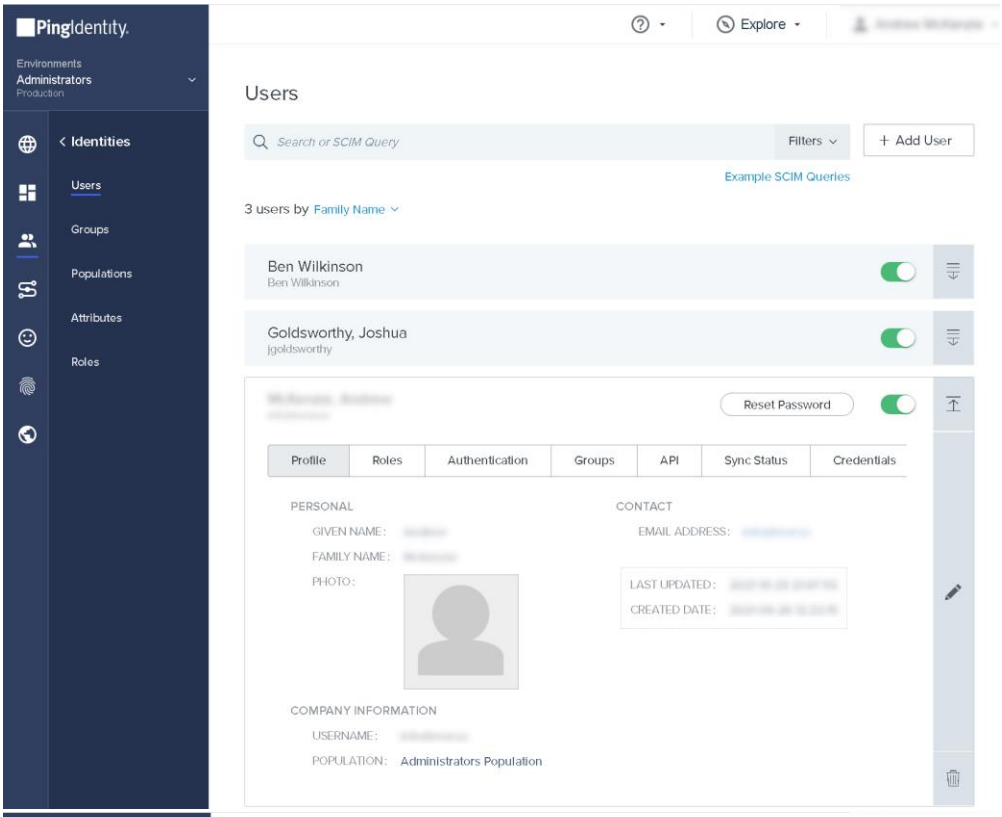
These example groups and users will help provide information to your Mendix application customize automatic mapping to user/login security contexts or other mapping functionality for user access control and application behavior.

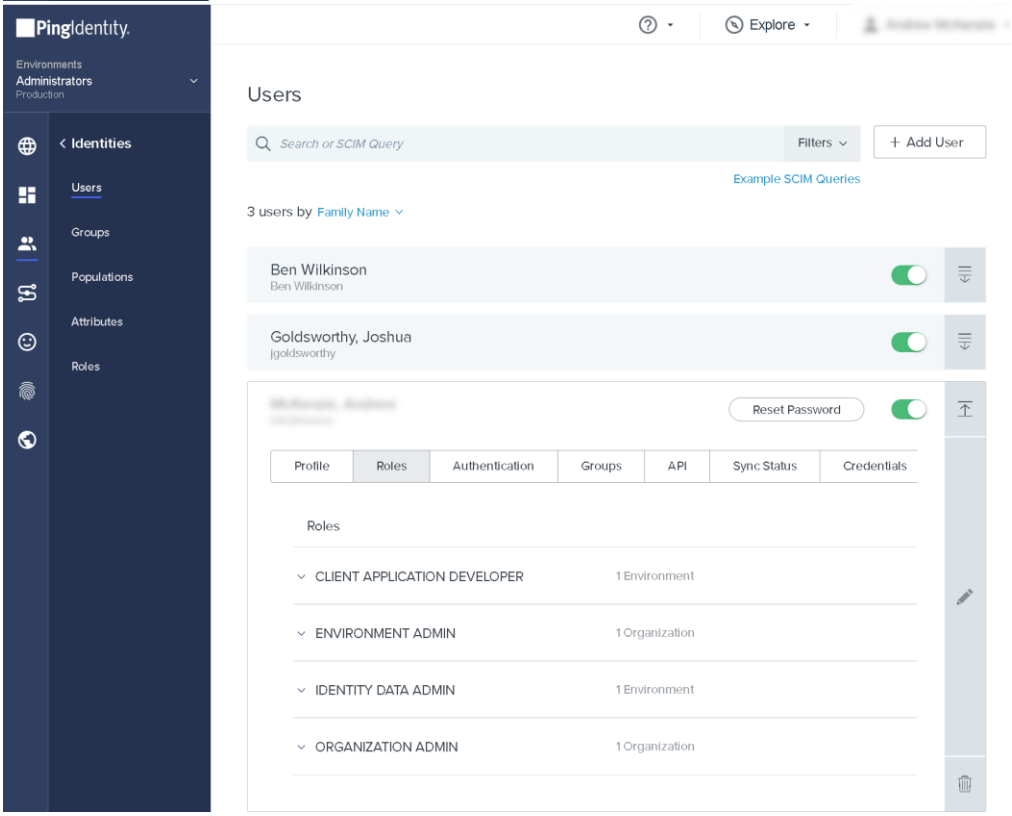
Example Application User Configuration

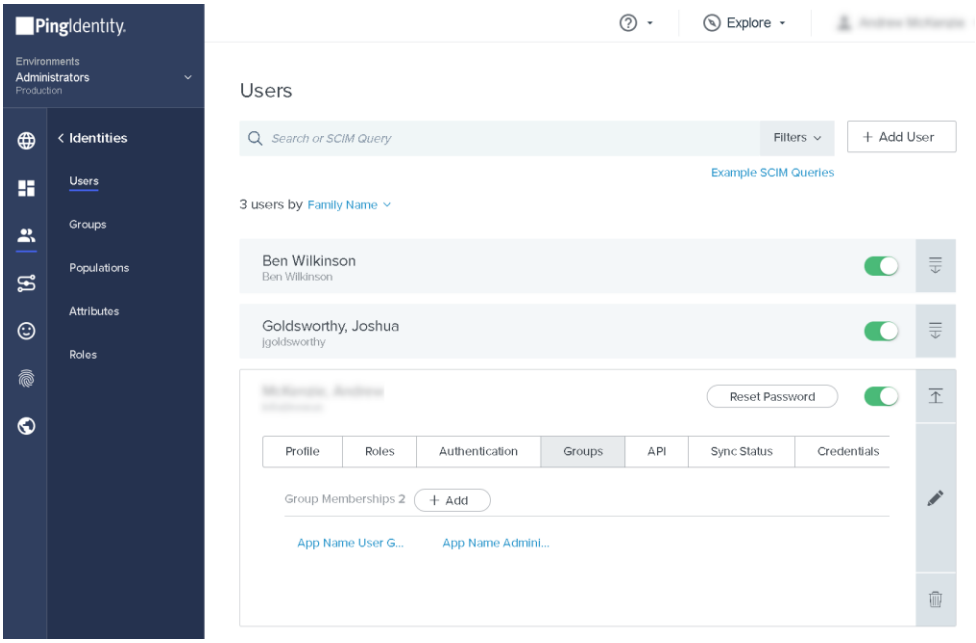




Example Application Administrator User Configuration





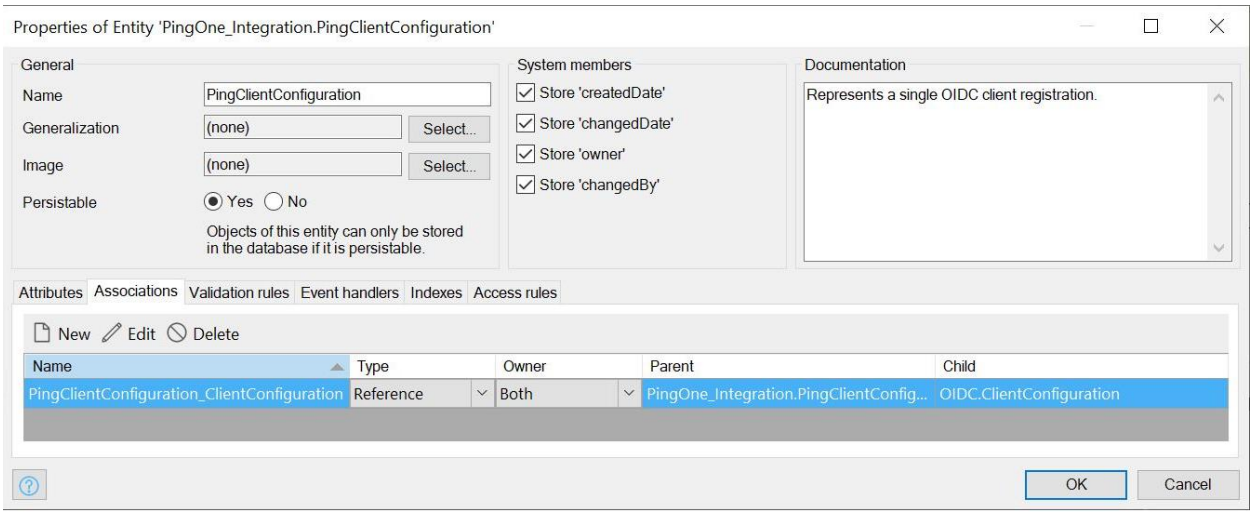

PingIdentity.
Environments
Administrators
Production
Identities
Users
Groups
Populations
Attributes
Roles
Explore
Users
Search or SCIM Query
Filters
Add User
Example SCIM Queries
3 users by Family Name
Ben Wilkinson
Ben Wilkinson
Goldsworthy, Joshua
jgoldsworthy
Reset Password
Profile
Roles
Authentication
Groups
API
Sync Status
Credentials
Group Memberships 2
Add
App Name User G...
App Name Admini...

3. Ping One Integration Module – Module Configuration:

In your Ping One Admin Console, you will provision a new OpenID client application, configure users, user access and registration policies.

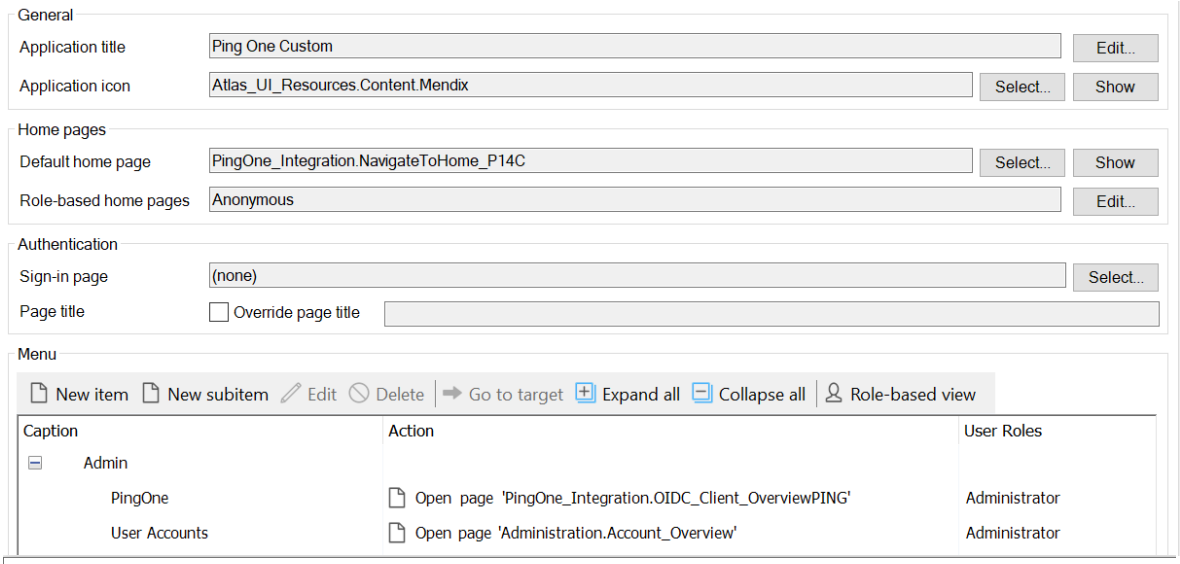
3-1 Domain Model Changes

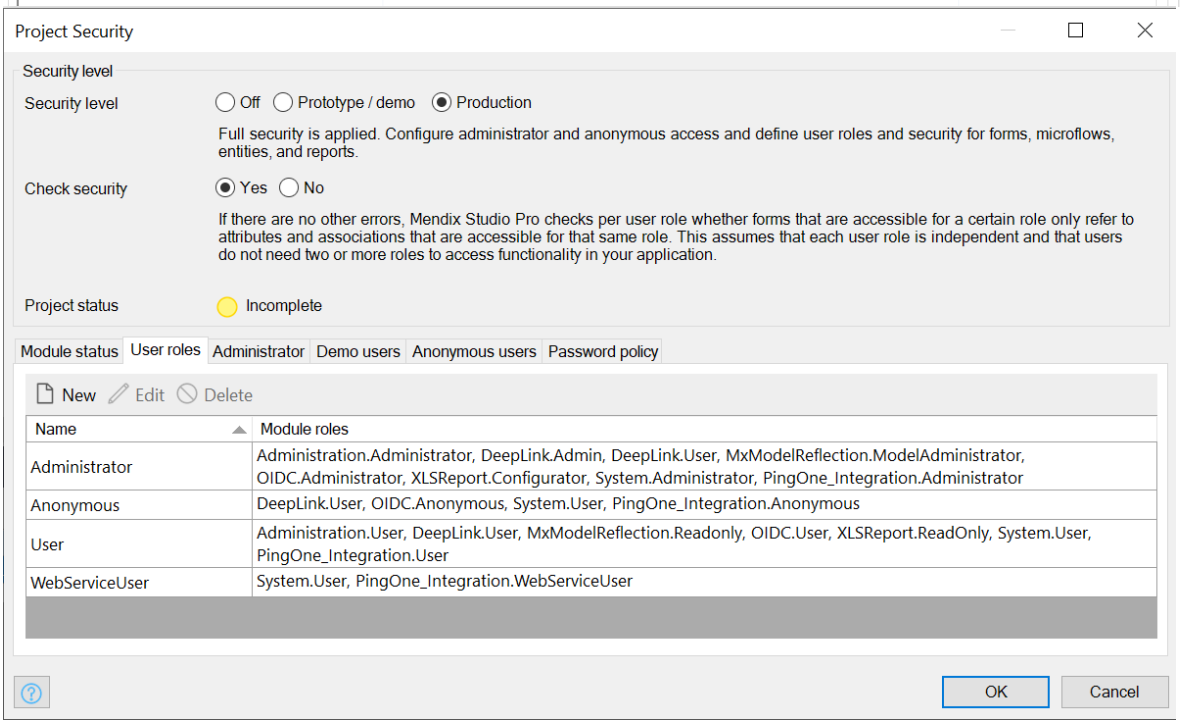
Establish a 1:1 association from PingOne_Integration.ClientConfiguration to OIDC.ClientConfiguration named PingClientConfiguration_ClientConfiguration. Administrator users in the Ping One Integration module should have read and write access to this association without xpath constraint.



3-2 Project Changes

1. Enable Anonymous Users
2. Add Role-Based home page for Anon Users microflow "NavigateToHome_P14C"
3. Add Ping One Admin setting to open page for Administrators, showing "OIDC_Client_OverviewPING"
4. Update Security for Anonymous users to the primary app module, Ping One Integration and OIDC modules.
5. Update Security for Administrators, granting Ping One Integration Module's Administrator access to configuration pages OIDC_Client_OverviewPING.
6. Update Security for Administrators, granting OIDC Administrator rights to provide access to the ClientConfiguration_Overview page.

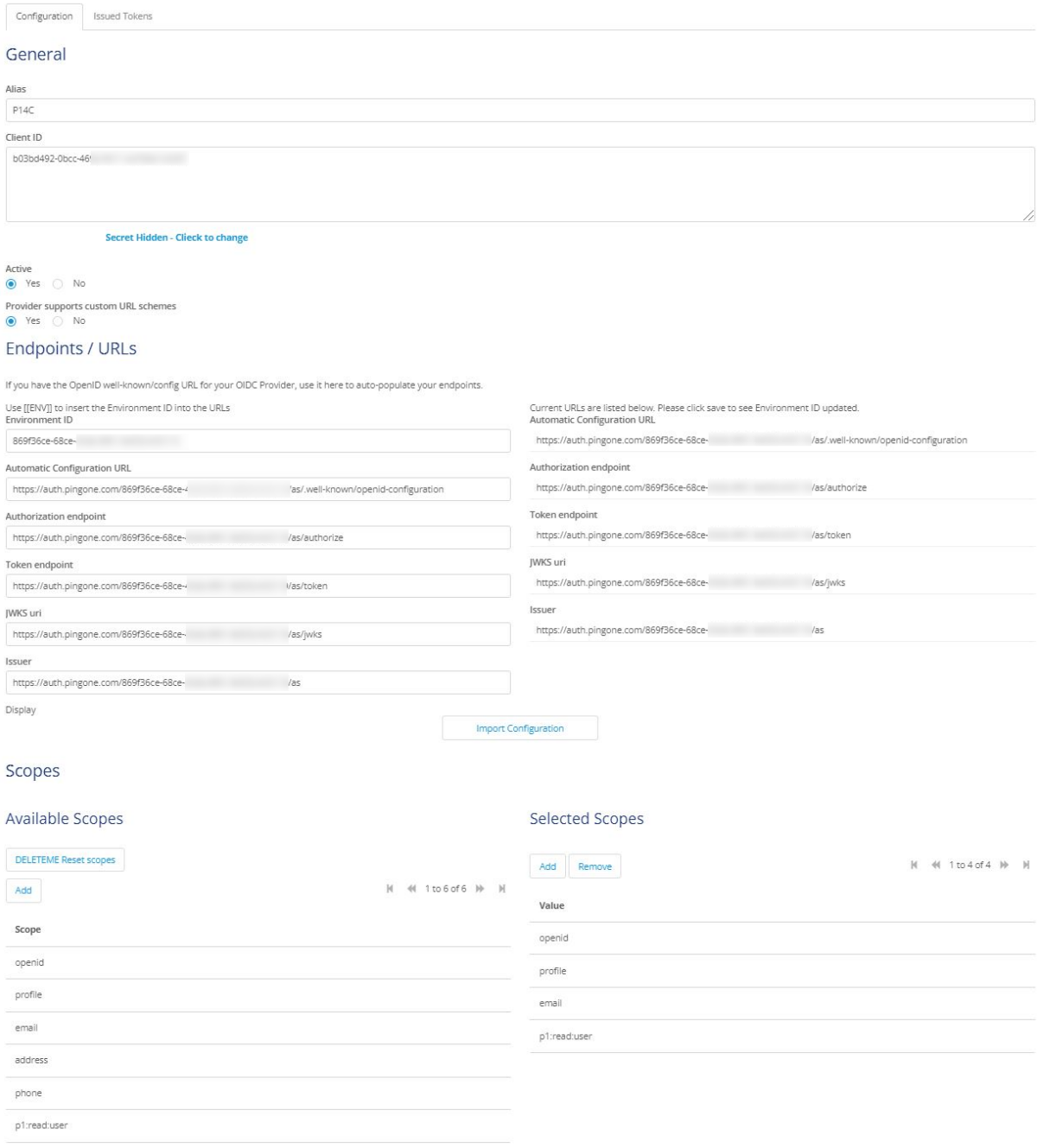




3-3 Mendix Application - Module Configuration

1. Start your app, log in as an admin, and access the Ping One Setup page.

2. From the values noted down during previous steps 1-3 & 2-6-2 during configuration of your Ping One Application. Add a new client configuration with the ClientID, ClientSecret, endpoints and scope grants provided by the application details in the Ping One Administration Console. You may also need to set the environment ID in the OIDC module's Client Configuration page, a separate page provided by the OIDC module.



3. Set the configuration to active & try the following

- **log on** as one of the example users created in Step 2-9
- **register** a new user using the link on the login page below
- **reset** a password using the forgot password flow, per login page below
- **explore** the JWT**,** AppUser entities and Update User microflows that provision users in your application. Consider using the Group IDs to link up your administrator rights to the administrator user you created by creating a PingOne_Integration_Customization module.