

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

Environments

Administrators

Production

< Environment

Properties

Audit

Alerts

ORGANIZATION NAME

XXXXXXXXXXXXXXX

NAME

Administrators

DESCRIPTION

This is the administrator environment created when the organization was provisioned.

LICENSE

ADMIN

ENVIRONMENT ID

869f36ce-68ce-XXXX-XXXX-XXXXXX

ORGANIZATION ID

c7a7e923-56a3-XXXX-XXXX-XXXXXX

TYPE

Production

REGION

North America (US)

CREATED

2021-09-26T19:XXXX:XXXX:XXXXZ

CONSOLE LOGIN URL ?

[https://console.pingone.com/?env=869f36ce-68ce-XXXX-XXXX-XXXXXX](#)

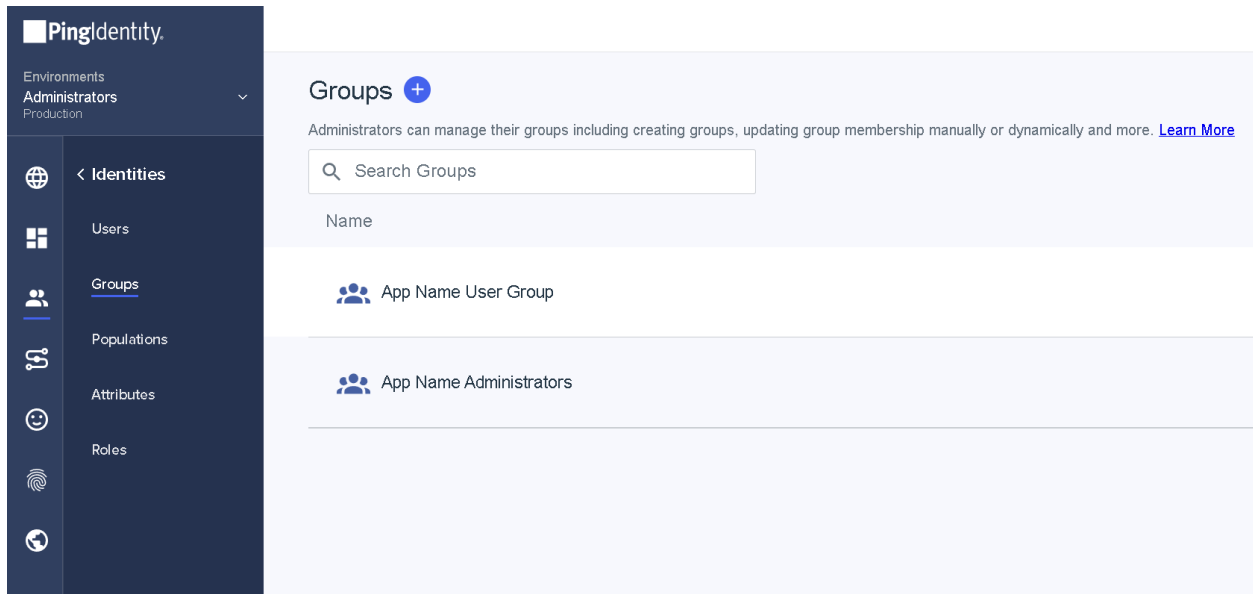
SERVICE LOGIN URL ?

[https://apps.pingone.com/869f36ce-XXXX-XXXX-XXXX-XXXXXX](#)

APPLICATION PORTAL URL ?

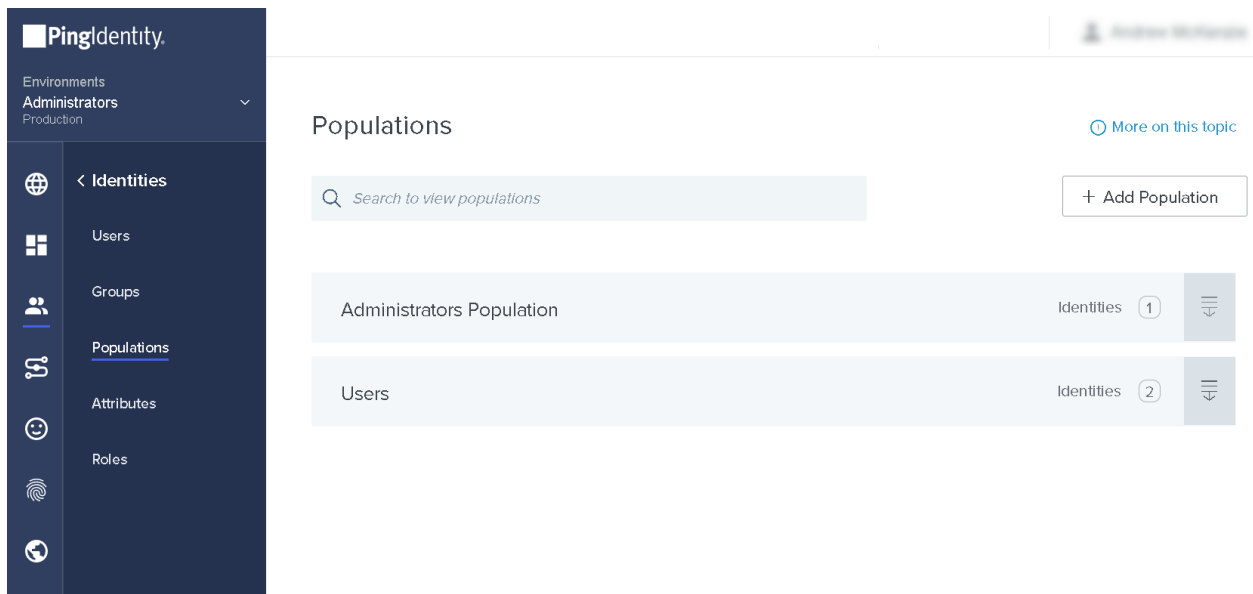
[https://apps.pingone.com/869f36ce-68ce-XXXX-XXXX-XXXXXX](#)

2-3 Configure User Groups



The screenshot shows the PingIdentity Groups configuration page. On the left is a dark blue sidebar with the PingIdentity logo and a menu for 'Identities' including Users, Groups, Populations, Attributes, and Roles. The 'Groups' menu item is highlighted. The main content area has a light blue header with the title 'Groups' and a plus icon. Below the header is a search bar labeled 'Search Groups' and a 'Name' label. The main area displays a list of groups: 'App Name User Group' and 'App Name Administrators', each with a group icon. A 'Learn More' link is present in the header area.

2-4 Configure Populations



The screenshot shows the PingIdentity Populations configuration page. On the left is a dark blue sidebar with the PingIdentity logo and a menu for 'Identities' including Users, Groups, Populations, Attributes, and Roles. The 'Populations' menu item is highlighted. The main content area has a light blue header with the title 'Populations' and a link 'More on this topic'. Below the header is a search bar labeled 'Search to view populations' and a '+ Add Population' button. The main area displays a list of populations: 'Administrators Population' and 'Users', each with a population icon, a count of identities (1 and 2 respectively), and a toggle icon.

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.

The screenshot displays the PingIdentity Administration console interface. On the left is a dark blue sidebar with the PingIdentity logo and a navigation menu. The main content area is white and shows the configuration for a policy named "Registration_AppName".

Sidebar:

- Environments: Administrators, Production
- < Experiences
 - AUTHENTICATION
 - Authentication Policies**
 - MFA Policies
 - Password Policies
 - Languages
 - Agreements
 - Branding & Themes
 - Notifications
 - Domains
 - Sender

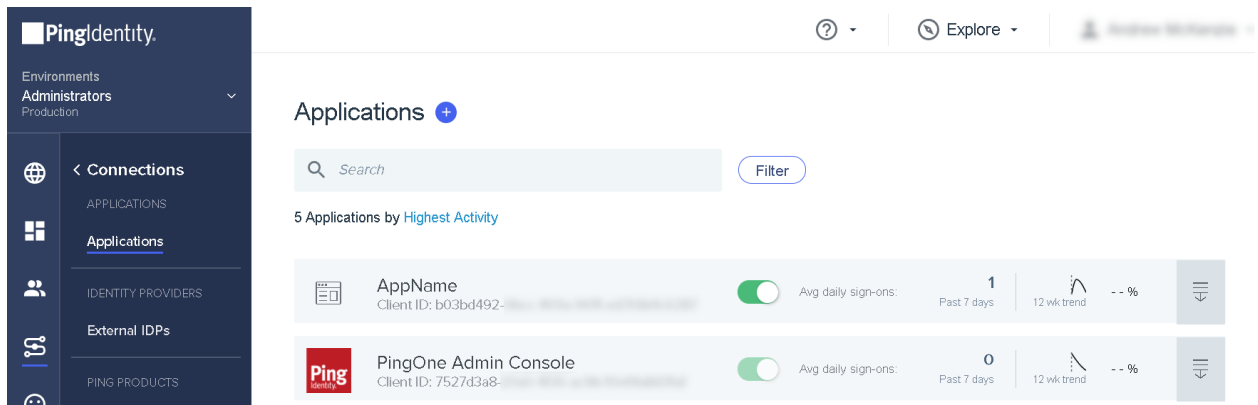
Main Content Area:

- Top bar: ? | Explore | Andrew McNamee
- Navigation: < To policy list
- Policy Name: Registration_AppName (with edit icon)
- Link: Make Default
- Step 1: LOGIN (selected from a dropdown menu)
- Configuration Card:
 - RECOVERY & REGISTRATION**
 - ☒ Enable account recovery
 - ☒ Enable registration
 - REGISTRATION METHOD**
 - ☒ PingOne
 - ☐ External Link
 - POPULATION**
 - Users (selected from dropdown)
 - ☐ Require confirmation of user information
- REQUIRED WHEN:**
 - ☒ Last sign-on older than...
 - 30 Minute(s)
- PRESENTED IDENTITY PROVIDERS**
 - + Add Provider
- AUTHENTICATION FOR LOCKED ACCOUNTS**
 - ☐ Block authentication of locked user accounts from Presented Identity Providers

+ Add step

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

PingIdentity

Environments
Administrators
Production

Connections

Applications

Identity Providers

External IDPs

Ping Products

PingFederate

PingIntelligence

Webhooks

Gateways

Certificates & KeyPairs

Resources

?

Explore

< To Application List

AppName
Client ID: b03bd492-0bcc-

ProfileConfigurationResourcesPoliciesAttribute MappingsAccess

APPLICATION NAME
AppName

DESCRIPTION
AppName App

ICON
Max Size 1.0 MB
JPEG, JPG, GIF, PNG

HOME PAGE URL

SIGNON URL

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.

The screenshot shows the PingIdentity configuration interface for an application named 'AppName'. The left sidebar contains navigation links for Environments, Administrators, Connections, Applications, Identity Providers, Ping Products, PingFederate, PingIntelligence, Webhooks, Gateways, Certificates & KeyPairs, and Resources. The main content area is titled 'AppName' and shows the 'Configuration' tab selected. The configuration includes a table of endpoints, client information, response type settings, grant type settings, PKCE enforcement, refresh token settings, redirect URIs, and token endpoint authentication method.

Profile	Configuration	Resources	Policies	Attribute Mappings	Access
AUTHORIZATION URL:	https://auth.pingone.com/869f36ce-.../as/authorize				
TOKEN ENDPOINT:	https://auth.pingone.com/869f36ce-.../as/token				
JWKS ENDPOINT:	https://auth.pingone.com/869f36ce-.../as/jwks				
USERINFO ENDPOINT:	https://auth.pingone.com/869f36ce-.../as/userinfo				
SIGNOFF ENDPOINT:	https://auth.pingone.com/869f36ce-.../as/signoff				
OIDC DISCOVERY ENDPOINT:	https://auth.pingone.com/869f36ce-.../as/.well-known/openid-configuration				
TOKEN INTROSPECTION ENDPOINT:	https://auth.pingone.com/869f36ce-.../as/introspect				
TOKEN REVOCATION ENDPOINT:	https://auth.pingone.com/869f36ce-.../as/revoke				
ISSUER:	https://auth.pingone.com/869f36ce-.../as				

CLIENT ID: b03bd492-0bcc-...
CLIENT SECRET: [Generate New Secret]

RESPONSE TYPE
☒ Code ☐ Token ☒ ID Token

GRANT TYPE
☒ Authorization Code

PKCE ENFORCEMENT
OPTIONAL

☒ Implicit
☐ Client Credentials
☒ Refresh Token

REFRESH TOKEN DURATION: 30 Days
REFRESH TOKEN ROLLING DURATION: 180 Days

TOKEN ENDPOINT AUTHENTICATION METHOD
☐ None ☐ Client Secret Basic ☒ Client Secret Post

REDIRECT URIS
http://localhost/oauth/v2/callback x
http://localhost:8080/oauth/v2/callback x

SIGNOFF URLS

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.

The screenshot displays the PingIdentity console interface. On the left, a dark sidebar contains the navigation menu with 'Applications' selected. The main content area shows the configuration for an application named 'AppName' (Client ID: b03bd492-...). The 'Resources' tab is active, showing a list of scopes and a list of scope grants.

Scopes:

- p1:create:device (PingOne API)
- p1:create:pairingKey (PingOne API)
- p1:delete:device (PingOne API)
- p1:delete:pairingKey (PingOne API)
- p1:delete:sessions (PingOne API)
- p1:delete:userLinkedAccounts (PingOne API)
- p1:read:device (PingOne API)

Scope Grants:

- p1.read:user (PingOne API)
- profile (openid)
- address (openid)
- phone (openid)
- email (openid)

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.

The screenshot displays the Pingidentity console interface. On the left is a dark blue sidebar with the Pingidentity logo and a navigation menu. The menu includes 'Environments' (Production), 'Administrators', 'Connections' (selected), 'Applications' (with a sub-menu 'Applications'), 'Identity Providers' (with a sub-menu 'External IDPs'), 'Ping Products' (PingFederate, PingIntelligence), 'Webhooks', 'Gateways', 'Certificates & KeyPairs', and 'Resources'. The main content area is titled '< To Application List' and shows the configuration for 'AppName' (Client ID: b03bd492-0bcc-...). Below the application name are tabs for 'Profile', 'Configuration', 'Resources', 'Policies' (active), 'Attribute Mappings', and 'Access'. A note states: 'The policies are applied in the order in which you add them. The first policy in the list overrides any subsequent policies.' There is a search bar labeled 'Search Policies'. Below this, the 'ALL POLICIES' section lists 'Multi_Factor' and 'Single_Factor', each with a '+' button to add it. The 'APPLIED POLICIES' section shows '1 Registration_AppName' with a '-' button to remove it.

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.

The screenshot displays the PingIdentity console interface. On the left is a dark blue sidebar with the PingIdentity logo and a navigation menu. The main content area is white and shows the configuration for an application named 'AppName' (Client ID: b03bd492-...). The 'Attribute Mappings' tab is selected, showing a table of OIDC attribute mappings. The table has two columns: 'APPLICATION ATTRIBUTE' and 'OUTGOING VALUE'. Each row represents a mapping, with a 'Required' checkbox and a trash icon for deletion. Below each mapping is a link for 'Advanced Expression'.

APPLICATION ATTRIBUTE	OUTGOING VALUE	Required	Advanced Expression
sub	User ID	<input checked="" type="checkbox"/>	Advanced Expression
PingOne_Email	Email Address	<input type="checkbox"/>	Advanced Expression
PingOne_Enabled	Enabled	<input type="checkbox"/>	Advanced Expression
PingOne_GroupIDs	Group IDs	<input type="checkbox"/>	Advanced Expression
PingOne_GroupNames	Group Names	<input type="checkbox"/>	Advanced Expression
PingOne_LastSignInTime	Last Sign-on Time	<input type="checkbox"/>	Advanced Expression
PingOne_Locale	Locale	<input type="checkbox"/>	Advanced Expression
PingOne_Timezone	Timezone	<input type="checkbox"/>	Advanced Expression
PingOne_Title	Title	<input type="checkbox"/>	Advanced Expression
Username	Username	<input type="checkbox"/>	Advanced Expression

2-6-6 Configure Application: Access

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

The screenshot displays the Ping Identity console interface. On the left is a dark blue sidebar with the 'PingIdentity.' logo and a navigation menu. The menu includes 'Environments' (with sub-items 'Administrators' and 'Production'), 'Connections', 'APPLICATIONS' (with sub-item 'Applications'), 'IDENTITY PROVIDERS' (with sub-item 'External IDPs'), 'PING PRODUCTS' (with sub-items 'PingFederate', 'PingIntelligence', 'Webhooks', 'Gateways', 'Certificates & KeyPairs', and 'Resources'). The main content area is titled 'AppName' with a client ID of 'b03bd492-...'. It features a tabbed interface with 'Access' selected. The 'Access' tab shows 'Admin Only Access' with a checkbox for 'Must have admin role'. Below this is the 'Group Membership Policy' section, which explains that groups can be added to control user access. It includes a search bar for 'Search Groups' and two radio button options: 'Any' (selected) and 'All'. At the bottom, the 'APPLIED GROUPS' section shows two groups: 'App Name Administrators' and 'App Name User Group', each with a minus icon for removal.

Environments
Administrators
Production

< Connections

APPLICATIONS
Applications

IDENTITY PROVIDERS
External IDPs

PING PRODUCTS
PingFederate
PingIntelligence
Webhooks
Gateways
Certificates & KeyPairs
Resources

[To Application List](#)

AppName
Client ID: b03bd492-...

Profile Configuration Resources Policies Attribute Mappings **Access**

Admin Only Access
☐ Must have admin role

Group Membership Policy

Groups can be added to control user access to the application. All users have access when no groups are listed. The following selections determine groups that have access to the application.

☒ Any User is a member of any applied group
☐ All User must be a member of all applied groups

ALL GROUPS

Remove access control for groups by dragging them here

APPLIED GROUPS 2

- App Name Administrators
- App Name User Group

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.

The screenshot displays the PingIdentity Admin Console interface. On the left is a dark blue sidebar with the PingIdentity logo at the top. Below the logo, the sidebar lists 'Environments' (Administrators, Production) and a menu of options: Experiences, Authentication Policies, MFA Policies, Password Policies, Languages, Agreements, Branding & Themes (highlighted), Notifications, Domains, and Sender. The main content area is titled 'Branding & Themes'. It includes a 'COMPANY NAME' field with the value 'My Mendix App'. Below this is a 'DEFAULT LOGO' section showing a molecular structure icon and a 'Remove Image' link. A horizontal dotted line separates this from the 'MY THEMES' section. Under 'MY THEMES', there are two theme cards, both labeled 'Ping Default'. Each card features a star icon in the top-left corner and a preview of a login form. The login form contains fields for 'Username' and 'Password', a 'Sign On' button, and links for 'Forgot Password' and 'No Account? Register Now!'. At the bottom of the preview, it says 'Welcome to My Mendix App Sign On! PingIdentity'.

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

The screenshot shows the 'Notifications' configuration page in the PingIdentity administrator interface. The left sidebar contains the 'Experiences' menu with sub-items: Authentication Policies, MFA Policies, Password Policies, Languages, Agreements, Branding & Themes, Notifications (selected), Domains, and Sender. The main content area is titled 'Notifications' and includes a '+ Add Notification' button. Below this, there are five notification types, each with a description and a list of supported channels:

- DEVICE PAIRING**: Users will receive this message to pair their device for strong authentication. Channels: Default, EMAIL, SMS, VOICE.
- PASSWORD RECOVERY**: Users who need to reset their password will receive this message. Channels: Default, EMAIL.
- STRONG AUTHENTICATION**: Users will receive this message for strong authentication. Channels: Default, PUSH, SMS, EMAIL, VOICE.
- TRANSACTION**: Users will receive this message for transaction approval. Channels: Default, SMS, EMAIL, PUSH, VOICE.
- VERIFICATION CODE**: Users will receive this message to verify their email address. Channels: Default, EMAIL.

The screenshot shows the 'Sender' configuration page in the PingIdentity administrator interface. The left sidebar is identical to the previous screenshot, with 'Sender' selected under the 'Experiences' menu. The main content area is titled 'Sender' and includes tabs for 'Email' (selected) and 'SMS/Voice'. Under the 'EMAIL SENDER' section, there are two radio buttons: 'Ping Server' (selected) and 'Custom Server'. Below this, there is a text box with instructions: 'Send notifications using Ping's email server. You can also send emails from your own domain. Simply [set up your email domain](#) and then configure it here.' The configuration fields are as follows:

- DOMAIN**: A dropdown menu showing 'pingidentity.com (Default)'.
- FROM NAME**: A text input field containing 'PingOne'.
- FROM ADDRESS**: A text input field containing 'noreply@pingidentity.com'.
- REPLY-TO NAME**: A text input field containing 'PingOne'.
- REPLY-TO ADDRESS**: A text input field containing 'noreply@pingidentity.com'.

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.

Pingidentity.

Environments
Administrators
Production

< Experiences
AUTHENTICATION
Authentication Policies
MFA Policies
Password Policies
Languages
Agreements
Branding & Themes
Notifications
Domains
Sender

Allowed Authentication Methods

Enhance your MFA with advanced authentication methods
Give your customers a more secure, more seamless user experience. [Unlock](#)

☒ **Mobile Applications**

Passcode Failure Limit ? Block Duration ? Minutes Passcode Refresh Duration ?

☒ **Authentication App (TOTP)**

Passcode Failure Limit ? Block Duration ? Minutes

☒ **Email**

Passcode Failure Limit ? Block Duration ? Minutes Passcode Lifetime ?

☐ **SMS**

☐ **Voice**

☒ **Fido2 Biometrics**

☒ **Security Key**

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.

The screenshot shows the Ping Identity administration console. On the left is a dark blue sidebar with the Ping Identity logo and a menu. The menu includes 'Environments' (Production), 'Administrators', and a list of categories: 'Experiences' (selected), 'Authentication Policies', 'MFA Policies', 'Password Policies', 'Languages', 'Agreements', 'Branding & Themes', 'Notifications', 'Domains', and 'Sender'. The main content area is titled 'Password Policy'. It features a section 'CHOOSE YOUR PASSWORD POLICY TYPE' with three radio buttons: 'Standard' (selected), 'Basic', and 'Passphrase'. Below this are two text input fields: 'NAME' with the value 'Standard' and 'DESCRIPTION' with the value 'A standard policy that incorporates industry best practices'. At the bottom is a section header 'PASSWORD REQUIREMENTS'.

Pingidentity

Environments
Administrators
Production

< Experiences

AUTHENTICATION

Authentication Policies

MFA Policies

Password Policies

Languages

Agreements

Branding & Themes

Notifications

Domains

Sender

Password Policy

CHOOSE YOUR PASSWORD POLICY TYPE

☒ Standard ☐ Basic ☐ Passphrase

NAME

Standard

DESCRIPTION

A standard policy that incorporates industry best practices

PASSWORD REQUIREMENTS

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

PingIdentity

Environments
Administrators
Production

< Identities

Users

Groups

Populations

Attributes

Roles

?

Explore

Andrew Wilkinson

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

Toggle

Profile	Roles	Authentication	Groups	Consent	API	Sync Status
PERSONAL		CONTACT				
GIVEN NAME: Joshua		EMAIL ADDRESS: jgoldsworthy@company.com				
MIDDLE NAME: R		TIMEZONE: PDT - US (21:49)				
FAMILY NAME: Goldsworthy		LAST UPDATED: 2020-06-26 10:00:00				
NICKNAME: Goldsworthy		CREATED DATE: 2020-06-26 10:00:00				
PHOTO: 						
COMPANY INFORMATION						
USERNAME: jgoldsworthy						
POPULATION: Users						

PingIdentity

Environments
Administrators
Production

< Identities

Users

Groups

Populations

Attributes

Roles

?

Explore

Andrew Wilkinson

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

Toggle

Profile	Roles	Authentication	Groups	Consent	API	Sync Status
Group Memberships 1 <div>+ Add</div>						
App Name User G...						

Example Application Administrator User Configuration

Environments

Administrators

Production

< Identities

Users

Groups

Populations

Attributes

Roles

?

Explore

Andrew Wilkinson

Users

Search or SCIM Query

Filters

+ Add User

[Example SCIM Queries](#)

3 users by Family Name

Ben Wilkinson

Ben Wilkinson

Toggle

Menu

Goldsworthy, Joshua

jgoldsworthy

Toggle

Menu

Goldsworthy, Joshua

Goldsworthy, Joshua

Reset Password

Toggle

Menu

Profile

Roles

Authentication

Groups

API


Sync Status

Credentials

PERSONAL

GIVEN NAME: Joshua

FAMILY NAME: Goldsworthy

PHOTO: 

CONTACT

EMAIL ADDRESS: jgoldsworthy@acme.com

LAST UPDATED: 2020-09-22 09:00:00

CREATED DATE: 2020-09-22 09:00:00

COMPANY INFORMATION

USERNAME: jgoldsworthy

POPULATION: Administrators Population

✎

🗑️

?

Explore

Andrew Wilkinson

Users

Search or SCIM Query

Filters

+ Add User

[Example SCIM Queries](#)

3 users by Family Name

Ben Wilkinson

Ben Wilkinson

Toggle

Menu

Goldsworthy, Joshua

jgoldsworthy

Toggle

Menu

Goldsworthy, Joshua

Goldsworthy, Joshua

Reset Password

Toggle

Menu

Profile

Roles

Authentication

Groups

API

Sync Status

Credentials

Roles

▼ CLIENT APPLICATION DEVELOPER

1 Environment

▼ ENVIRONMENT ADMIN

1 Organization

▼ IDENTITY DATA ADMIN

1 Environment

▼ ORGANIZATION ADMIN

1 Organization

✎

🗑️

PingIdentity.

Environments
Administrators
Production

< Identities

Users

Groups

Populations

Attributes

Roles

Users

Search or SCIM Query

Filters

+ Add User

Example SCIM Queries

3 users by Family Name

Ben Wilkinson
Ben Wilkinson

Toggle

Menu

Goldsworthy, Joshua
jgoldsworthy

Toggle

Menu

McKenzie, Andrew
amckenzie

Reset Password

Toggle

Menu

Profile	Roles	Authentication	Groups	API	Sync Status	Credentials
Group Memberships 2 + Add						
App Name User G... App Name Admini...						

Menu

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.

Properties of Entity 'PingOne_Integration.PingClientConfiguration'

General

Name
PingClientConfiguration

Generalization
(none) Select...

Image
(none) Select...

Persistable
☒ Yes ☐ No
Objects of this entity can only be stored in the database if it is persistable.

System members

☒ Store 'createdDate'
☒ Store 'changedDate'
☒ Store 'owner'
☒ Store 'changedBy'

Documentation

Represents a single OIDC client registration.

Attributes Associations Validation rules Event handlers Indexes Access rules

New Edit Delete

Name	Type	Owner	Parent	Child
PingClientConfiguration_ClientConfiguration	Reference	Both	PingOne_Integration.PingClientConfig...	OIDC.ClientConfiguration

?

OK Cancel

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.

General

Application title

Ping One Custom

Edit...

Application icon

Atlas_UI_Resources.Content.Mendix

Select...

Show

Home pages

Default home page

PingOne_Integration.NavigateToHome_P14C

Select...

Show

Role-based home pages

Anonymous

Edit...

Authentication

Sign-in page

(none)

Select...

Page title

☐ Override page title

Menu

New item

New subitem

Edit

Delete

Go to target

Expand all

Collapse all

Role-based view

Caption	Action	User Roles
Admin		
PingOne	Open page 'PingOne_Integration.OIDC_Client_OverviewPING'	Administrator
User Accounts	Open page 'Administration.Account_Overview'	Administrator

Project Security

Security level

Security level

☐ Off ☐ Prototype / demo ☒ Production

Full security is applied. Configure administrator and anonymous access and define user roles and security for forms, microflows, entities, and reports.

Check security

☒ Yes ☐ No

If there are no other errors, Mendix Studio Pro checks per user role whether forms that are accessible for a certain role only refer to attributes and associations that are accessible for that same role. This assumes that each user role is independent and that users do not need two or more roles to access functionality in your application.

Project status

☒ Incomplete

Module status

User roles

Administrator

Demo users

Anonymous users

Password policy

New

Edit

Delete

Name	Module roles
Administrator	Administration.Administrator, DeepLink.Admin, DeepLink.User, MxModelReflection.ModelAdministrator, OIDC.Administrator, XLSReport.Configurator, System.Administrator, PingOne_Integration.Administrator
Anonymous	DeepLink.User, OIDC.Anonymous, System.User, PingOne_Integration.Anonymous
User	Administration.User, DeepLink.User, MxModelReflection.ReadOnly, OIDC.User, XLSReport.ReadOnly, System.User, PingOne_Integration.User
WebServiceUser	System.User, PingOne_Integration.WebServiceUser

?

OK

Cancel

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.

Configuration

Issued Tokens

General

Alias

P14C

Client ID

b03bd492-0bcc-46f1-8000-000000000000

Secret Hidden - Click to change

Active

☒ Yes ☐ No

Provider supports custom URL schemes

☒ Yes ☐ No

Endpoints / URLs

If you have the OpenID well-known/config URL for your OIDC Provider, use it here to auto-populate your endpoints.

Use [[ENV]] to insert the Environment ID into the URLs

Environment ID

869f36ce-68ce-4000-0000-000000000000

Automatic Configuration URL

https://auth.pingone.com/869f36ce-68ce-4000-0000-000000000000/.well-known/openid-configuration

Authorization endpoint

https://auth.pingone.com/869f36ce-68ce-4000-0000-000000000000/authorize

Token endpoint

https://auth.pingone.com/869f36ce-68ce-4000-0000-000000000000/token

JWKS uri

https://auth.pingone.com/869f36ce-68ce-4000-0000-000000000000/jwks

Issuer

https://auth.pingone.com/869f36ce-68ce-4000-0000-000000000000/

Display

Import Configuration

Current URLs are listed below. Please click save to see Environment ID updated.

Automatic Configuration URL

https://auth.pingone.com/869f36ce-68ce-4000-0000-000000000000/.well-known/openid-configuration

Authorization endpoint

https://auth.pingone.com/869f36ce-68ce-4000-0000-000000000000/authorize

Token endpoint

https://auth.pingone.com/869f36ce-68ce-4000-0000-000000000000/token

JWKS uri

https://auth.pingone.com/869f36ce-68ce-4000-0000-000000000000/jwks

Issuer

https://auth.pingone.com/869f36ce-68ce-4000-0000-000000000000/

Scopes

Available Scopes

DELETEME Reset scopes

Add

1 to 6 of 6

Scope

openid

profile

email

address

phone

p1:read:user

Selected Scopes

Add Remove

1 to 4 of 4

Value

openid

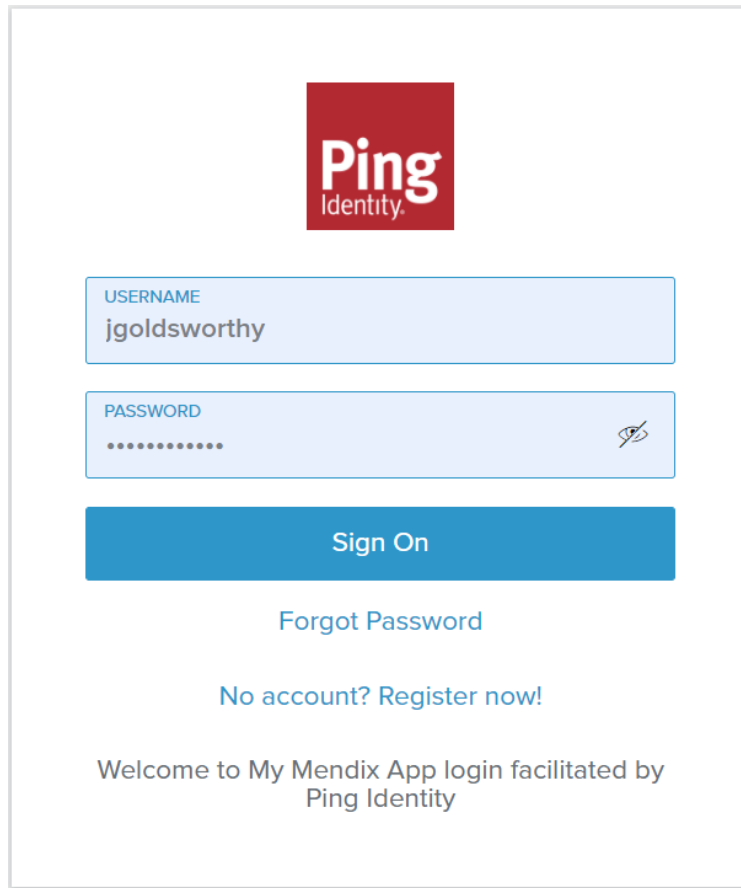
profile

email

p1:read:user

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.



The image shows a login page for Ping Identity. At the top center is the Ping Identity logo, which consists of a red square with the word "Ping" in white and "Identity." in smaller white text below it. Below the logo are two input fields. The first field is labeled "USERNAME" in blue text and contains the text "jgoldsworthy". The second field is labeled "PASSWORD" in blue text and contains a series of dots, with a small eye icon to its right. Below these fields is a large blue button with the text "Sign On" in white. Under the button is a link that says "Forgot Password" in blue. Below that is another link that says "No account? Register now!" in blue. At the bottom of the form area, there is a message that says "Welcome to My Mendix App login facilitated by Ping Identity" in a smaller, grey font.



Welcome Joshua Goldsworthy
jgoldsworthy

[Sign out](#)