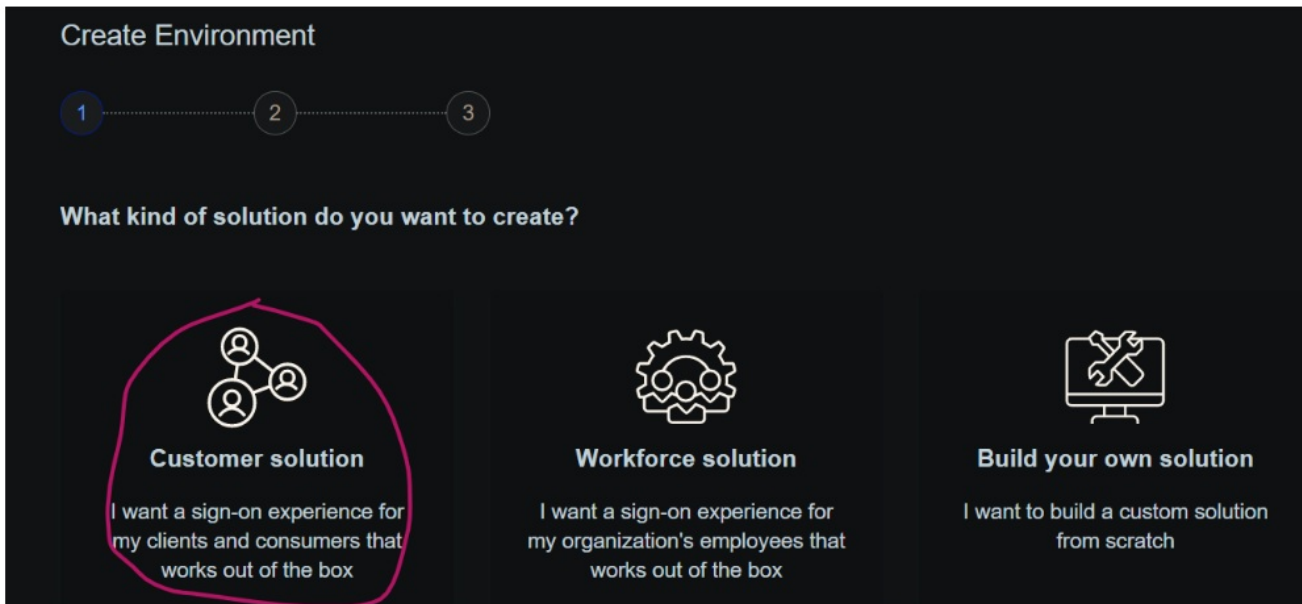
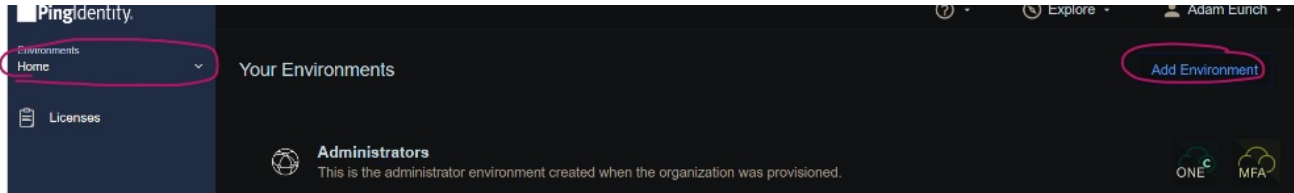


Manitou Single Sign-on - Ping Identity

09/17/2024 2:31 pm EDT

Create an Environment

A PingOne for Customers environment is created and named Manitou PingOne for Customers.




Create Environment


1

2


3

Select a complete solution or individual services

Cloud Solutions   



PingOne for Customers
Cloud identity for customers



Customer360
Advanced capabilities for customer identity that can be deployed anywhere

Create an Application

Select the environment created. From there, click on Connections and Add Application.

- .NET web apps
- Java apps

WEB APP

- iOS and Android apps
- Desktop apps
- Push Authentication

NATIVE APP

- Angular
- Node.js

SINGLE PAGE APP

- Non-integrations
- Client OAuth
- Assignments
- Interactions & portals

CHOOSE CONNECTION TYPE

SAML

Apps that utilize an Identity Provider (IDP) to authenticate users and provides Service Providers an Authentication Assertion.

Configure

OIDC

Employs Universal Login and redirect users to the login page.

Configure

Pingidentity ? Explore Adam Eurich

Environments
Manitou PingOne for Customers

Connections

- APPLICATIONS
- IDENTITY PROVIDERS
- EXTERNAL IDPs
- PING PRODUCTS
- PROVISIONING
- Webhooks

Applications

3 Applications | By Application Name


Filters + Add Application

	Manitou SSO Client ID: e044da12-1530-4d26-9bb7-452118c9111	<input checked="" type="checkbox"/>	Avg daily sign-ons: 10 Past 7 days	12 wk trend: --%	
	PingOne Admin Console Client ID: f2750b0d-1dfa-4b31-ad4e-3b4e25e406ed	<input checked="" type="checkbox"/>	Avg daily sign-ons: 0 Past 7 days	No data yet: --%	
	PingOne Self-Service - MyAccount Client ID: b8b8b65c-2fcc-40c0-e642-c7073f25e883	<input checked="" type="checkbox"/>	Avg daily sign-ons: 0 Past 7 days	No data yet: --%	

New Application

Adding a new application to your environment allows your customers controlled access to it. There are several different application technologies to choose from that accommodate the majority of applications.


SELECT AN APPLICATION TYPE



Web applications that are accessed within a browser.

- .NET web apps
- Java apps


WEB APP



Applications that are stored and run from a device or desktop.

- iOS and Android apps
- Desktop apps
- Push Authentication


NATIVE APP



A front-end application that uses an API.

- Angular
- Node.js


SINGLE PAGE APP



Management API integrations that can perform actions using Roles.

- Non-interactive service integrations
- Client Credentials w/Role Assignment
- Interactive admin consoles & portals

WORKER



Apps configured by advanced users from the ground up.

- Your choice
- No barriers
- Complete flexibility

ADVANCED CONFIGURATION

Create App Profile

Personalize your application by creating a unique profile. The description will help your customers identify the purpose of the application and provide important information to misguiding connections.

APPLICATION NAME

Manitou IDP

DESCRIPTION

Manitou Identity Provider

ICON



Max Size 1.0 MB
JPEG, JPG, GIF, PNG

PROGRESS

1 Create App Profile

Personalize your application

2 Configure

Add a Redirect URL

3 Grant Resource Access

Provide your application access to resources.

4 Map Attributes

Provide access to your application for customers to authenticate.

Cancel

Next

For the redirect URLs, enter <https://{siteName}/Manitou/Login?ws=1>. Mine is . You can enter multiple redirect URLs if you have multiple machines hosting the Manitou Web Client.

The screenshot shows the 'Configure' step of the application setup wizard. At the top, the application name is 'Manitou IDP', the type is 'Web App', and the protocol is 'OpenID Connect'. The main heading is 'Configure' with the instruction: 'Configure your application by adding one or more redirect URLs.' Below this, there is a 'REDIRECT URLS' section with a text input field containing the URL 'https://dev-12.boldgroup.int/Manitou/Login?ws=1'. At the bottom right, there are 'Cancel' and 'Save and Continue' buttons. On the right side, a 'PROGRESS' sidebar shows four steps: 1. Create App Profile (Personalize your application), 2. Configure (Add a Redirect URL - current step), 3. Grant Resource Access (Provide your application access to resources), and 4. Map Attributes (Provide access to your application for customers to authenticate).

The screenshot shows the 'Grant Resource Access to Your Application' step of the application setup wizard. At the top, the application name is 'Manitou IDP', the type is 'Web App', and the protocol is 'OpenID Connect'. The main heading is 'Grant Resource Access to Your Application' with the instruction: 'Applications are granted OAuth scopes so they can access our resources. On the left is a list of OAuth scopes by resource type that can be added to the Scope Grants column on the right. After moving the desired scopes to the Scope Grants column you can save your selections.' Below this, there is a search bar for scopes. The 'SCOPES' section is filtered by 'ALL' and lists three scopes: 'p1:reset:userPassword PingOne API', 'p1:update:device PingOne API', and 'p1:update:user PingOne API'. The 'SCOPE GRANTS' section (indicated by a '1' in a circle) contains two selected scopes: 'profile' and 'openid'. A pink oval highlights the 'SCOPE GRANTS' section. At the bottom right, there are 'Cancel' and 'Save and Continue' buttons. On the right side, a 'PROGRESS' sidebar shows four steps: 1. Create App Profile (Personalize your application), 2. Configure (Add a Redirect URL), 3. Grant Resource Access (Provide your application access to resources - current step), and 4. Map Attributes (Provide access to your application for customers to authenticate).

Attribute Mapping

Map your PingOne user defined attributes to the corresponding Application attribute for accessibility between users and this app.

OIDC ATTRIBUTES

PINGONE USER ATTRIBUTE

User ID

=

APPLICATION ATTRIBUTE

sub

Required

+ ADD ATTRIBUTE

- PingOne Attribute
- Static Attribute

OIDC ATTRIBUTE MAPPINGS

PINGONE USER ATTRIBUTE

User ID

=

APPLICATION ATTRIBUTE

sub

Required

PINGONE USER ATTRIBUTE

Group IDs

=

APPLICATION ATTRIBUTE

groups

Required



+ ADD ATTRIBUTE

Click Save and Close. Next, edit your application.

Applications

Search Filters ▾ + Add Application

4 Applications | By Application Name ▾

	Manitou IDP Client ID: 57d2ed4b-e91c-4ccd-a6a8-4e595bf078e0		Avg daily sign-ons: Past 7 days	0 No data yet	-- %	⋮
	Manitou SSO Client ID: e044da12-1530-4d26-9bb7-f52118cf9f11		Avg daily sign-ons: Past 7 days	8 12 wk trend	-- %	⋮

Manitou SSO
Client ID: e044da12-1530-4d26-9bb7-f52118cf9f11

Avg daily sign-ons: 8 Past 7 days | 12 wk trend | -- %

- Profile
- Configuration
- Resources
- Policies
- Attribute Mappings
- Access

APP TYPE: Web App (OpenID Connect)

DESCRIPTION: Manitou SSO

CLIENT ID: e044da12-1530-4d26-9bb7-f52118cf9f11

HOME PAGE URL: No Home Page Configured

SIGNON URL: Default Signon Page

Go to the Configuration tab.

Manitou SSO
Client ID: e044da12-1530-4d26-9bb7-f52118cf9f11

- Profile
- Configuration**
- Resources
- Policies
- Attribute Mappings
- Access

AUTHORIZATION URL: https://auth.pingone.com/01cdee6b-5594-41dc-8eb0-b553636d061b/as/authorize

TOKEN ENDPOINT: https://auth.pingone.com/01cdee6b-5594-41dc-8eb0-b553636d061b/as/token

JWKS ENDPOINT: https://auth.pingone.com/01cdee6b-5594-41dc-8eb0-b553636d061b/as/jwks

USERINFO ENDPOINT: https://auth.pingone.com/01cdee6b-5594-41dc-8eb0-b553636d061b/as/userinfo

SIGNOFF ENDPOINT: https://auth.pingone.com/01cdee6b-5594-41dc-8eb0-b553636d061b/as/signoff

OIDC DISCOVERY ENDPOINT: https://auth.pingone.com/01cdee6b-5594-41dc-8eb0-b553636d061b/as/.well-known/openid-configuration

TOKEN INTROSPECTION ENDPOINT: https://auth.pingone.com/01cdee6b-5594-41dc-8eb0-b553636d061b/as/introspect

TOKEN REVOCATION ENDPOINT: https://auth.pingone.com/01cdee6b-5594-41dc-8eb0-b553636d061b/as/ revoke

ISSUER: https://auth.pingone.com/01cdee6b-5594-41dc-8eb0-b553636d061b/as

CLIENT ID: e044da12-1530-4d26-9bb7-f52118cf9f11

CLIENT SECRET: Generate New Secret

Make sure these settings are set the following way:


RESPONSE TYPE

Code Token ID Token

GRANT TYPE

Authorization Code

PKCE ENFORCEMENT

OPTIONAL 

Implicit

Client Credentials

Refresh Token

TOKEN ENDPOINT AUTHENTICATION METHOD

None Client Secret Basic Client Secret Post

ADVANCED Only experts beyond this point

Allow unsigned JWT requests

Once saved, edit the application and add a SignOff URL. It should be <https://yourManitouSiteName/manitou/Login>. Mine is <https://dev-12.boldgroup.int/manitou/Login>.

RESPONSE TYPE

Code Token ID Token

GRANT TYPE

Authorization Code

PKCE ENFORCEMENT

OPTIONAL

Implicit

Client Credentials

Refresh Token

TOKEN ENDPOINT AUTHENTICATION METHOD

None Client Secret Basic Client Secret Post

REDIRECT URIS

<https://dev-12.boldgroup.int/manitou/Login?ws=1> x

SIGNOFF URLs

<https://dev-12.boldgroup.int/manitou/Login> x

Once saved, make sure you enable your application.

PingIdentity

Environments
Manitou PingOne for Customers

Connections

APPLICATIONS

Applications

IDENTITY PROVIDERS

External IDPs

PING PRODUCTS

PingFederate

Provisioning

Webhooks

Certificates & KeyPairs

Resources

Applications

Search Filters + Add Application

4 Applications | By Application Name

Application Name	Client ID	Enabled	Avg daily sign-ons	Period	Last Sign-on	Success Rate	Actions
Manitou IDP	57d2ed4b-e91c-4ccd-a6a8-4e595bf078e0	<input checked="" type="checkbox"/>	0	Past 7 days	No data yet	-- %	⋮
Manitou SSO	e044da12-1530-4d26-9bb7-f52118cf9f11	<input checked="" type="checkbox"/>	10	Past 7 days	17 wk trend ↑	-- %	⋮
PingOne Admin Console	f2750b06-1dfe-4b3f-ad4a-3b4e25a406ad	<input checked="" type="checkbox"/>	0	Past 7 days	No data yet	-- %	⋮
PingOne Self-Service - MyAccount	b8b8b65c-2fcc-40c0-a642-c7073f25aa83	<input checked="" type="checkbox"/>	0	Past 7 days	No data yet	-- %	⋮

Open [Ping Identity](#) to follow the rest of the process.