

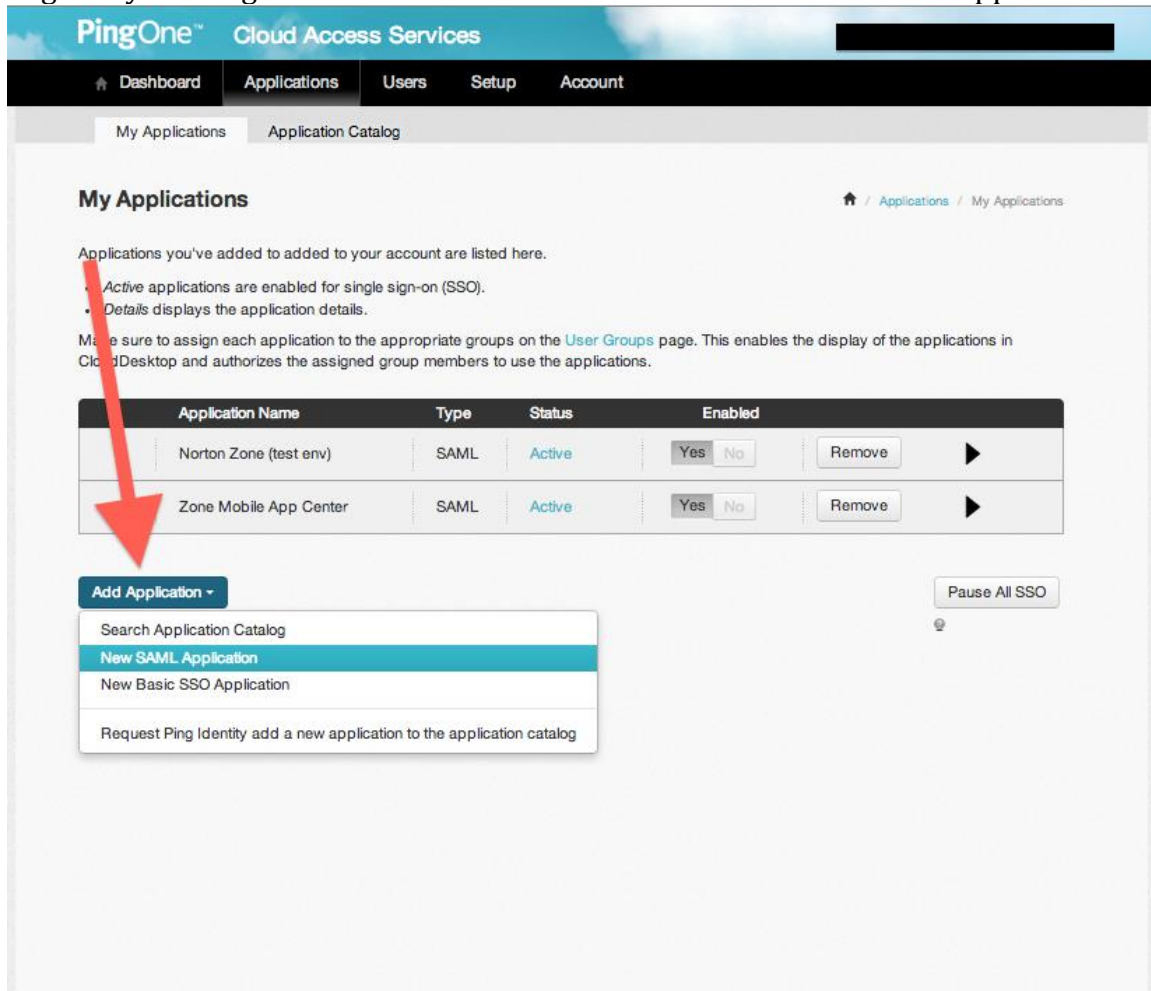
How to Configure PingOne with Symantec Mobility Suite

Abstract:

This document will provide high-level steps for configuring Ping One as an External Identity Provider for Symantec App Center. This article does not cover group mapping, and is based on the internal user-store of PingOne. For further configuration info, such as how to pass group membership information, please contact your Symantec sales specialist or PingOne support.

Step 1:

Log into your PingOne administration console and “Add” a new SAML application



The screenshot shows the PingOne Cloud Access Services administration console. The top navigation bar includes 'Dashboard', 'Applications', 'Users', 'Setup', and 'Account'. The 'Applications' tab is selected, and the 'My Applications' sub-tab is active. The 'My Applications' page displays a list of applications. A red arrow points to the 'Add Application' button, which has a dropdown menu open showing options: 'Search Application Catalog', 'New SAML Application', 'New Basic SSO Application', and 'Request Ping Identity add a new application to the application catalog'.

Application Name	Type	Status	Enabled	
Norton Zone (test env)	SAML	Active	<input type="checkbox"/> Yes <input type="checkbox"/> No	<button>Remove</button> ▶
Zone Mobile App Center	SAML	Active	<input type="checkbox"/> Yes <input type="checkbox"/> No	<button>Remove</button> ▶

Start Application Configuration – part 1

The next screen should provide fields for providing the application a name as well as a description – you must fill out both fields before proceeding to the next step. These fields are arbitrary, but you should probably pick a meaningful name.

My Applications Application Catalog

My Applications

Applications you've added to added to your account are listed here.

- *Active* applications are enabled for single sign-on (SSO).
- *Details* displays the application details.

Make sure to assign each application to the appropriate groups on the [User Groups](#) page. This enables the display of the applications in CloudDesktop and authorizes the assigned group members to use the applications.

Application Name	Type	Status	Enabled	
Norton Zone (test env)	SAML	Active	<input type="checkbox"/> Yes <input type="checkbox"/> No	Remove
New Application	SAML	Incomplete	<input type="checkbox"/> Yes <input type="checkbox"/> No	

1. Application Details

Application Name:

Application Description:

Max 500 characters

Graphics Application Logo

For use on CloudDesktop

[Change](#)

Max Size: 400px x 112px

Application Icon

For use on mobile CloudDesktop

[Change](#)

Max Size: 256px x 256px

NEXT: [Application Configuration](#)

[Cancel](#) [Continue to Next Step](#)

[Add Application](#) [Pause All SSO](#)

Start Application Configuration – Part 2

In this step, we will exchange meta-data between App Center and PingOne. Click the “Download” hyperlink next to “SAML Metadata” area of the configuration screen. The file name is typically “saml2-metadata-idp.xml” – we will need to edit this file later.

New Application

SAML

Incomplete

Yes

No

2. Application Configuration

I have the SAML configuration

I have the SSO URL

You will need to download this SAML metadata to configure the application:

SAML Metadata

Download

Provide SAML details about the application you are connecting to:

Protocol Version

☒ SAML v 2.0

☐ SAML v 1.1

Upload Metadata

☒ Uploaded file:zonemobile.appcenterhq.com-sp-metadata.xr

Select File

Or use URL

Assertion Consumer Service (ACS)

https://zonemobile.appcenterhq.com/appstore/saml2/cons

Entity ID

https://zonemobile.appcenterhq.com

Application URL

Single Logout Endpoint

example.com/slo.endpoint

Single Logout Response Endpoint

example.com/sloresponse.endpoint

Single Logout Binding Type

☒ Redirect

☐ Post

Verification Certificate

Choose File

No file chosen

saml20metadata.cer

Force Re-authentication

☒

Keep the following in mind when creating your connection:

- Both SP- and IdP-Initiated SSO are allowed
- Map SAML_SUBJECT in your attribute contract, plus any attributes (configure them in PingOne later)
- Allow outbound POST or redirect bindings
- Allow inbound POST

NEXT: SSO Attribute Mapping

Cancel

Back

Continue to Next Step

Add Application

Pause All SSO

Please ensure that the "SAML 2.0" option is selected in the "Protocol Version" area. In the "Upload Metadata" section, you will need to upload the App Center SAML metadata to PingOne. You can get this metadata file by logging into your App Center as an Administrator and going to "Settings">"Server Configuration". In the "SP Partner ID" and "SP Entity ID" fields, simply use the root URL for your App Center server – in this case "https://zonemobile.appcenterhq.com". Once you fill out those fields click the "Download SP Metadata File" button. The resulting file should be named something like <servername>.appcenterhq.com-sp-metadata.xml. Use this file for the "Upload Metadata">"Select File" section of PingOne.

Once this file is uploaded, PingOne will automatically populate the “Assertion Consumer Service (ACS)” and “Entity ID” fields for you.

It is suggested that you check the “Force Re-Authentication” box.

Lastly – please note that PingOne requires us to pass the “SAML_SUBJECT” attribute – we will need to remember this field name for the next configuration screen.

The screenshot displays the PingOne administration interface. On the left, the 'Settings' menu is visible, with 'Server Configuration' selected. The main panel shows the 'Server Configuration' form. At the top, a progress bar indicates the steps: Server Configuration (checked), Auth. Options, Group Options, and Enable IDP. The form includes the following fields:

- Type:** SAML
- Name:** zonemobile
- IDP Metadata:** Choose File | No file chosen. Below this, a link states: "You can download Symantec O3 Sample IDP Metadata File from Downloads section".
- IDP Contact Info:** HTTP-POST: <https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=2c0ee629-337d-4254-9169-09f32a2ffe4d>; HTTP-Redirect: <https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=2c0ee629-337d-4254-9169-09f32a2ffe4d>
- SP Partner ID:** <https://zonemobile.appcenterhq.com>
- SP Entity ID:** <https://zonemobile.appcenterhq.com>

A red box highlights the 'SP Partner ID' and 'SP Entity ID' fields. A red arrow points from this box to the 'Download SP Metadata File' button.

Start Application Configuration – Part 3

Now that we have uploaded our App Center meta-data to PingOne, we need to map our SAML attributes. Using the screenshot below enter the values in the “Application Attribute” column verbatim. For the “Identity Bridge Attribute”, since we are using the PingOne internal user store, the values should also be identical. Check the boxes as indicated below for the “required” attributes.

My Applications

Application Catalog

My Applications

[Applications](#) / [My Applications](#)

Applications you've added to added to your account are listed here.

- *Active* applications are enabled for single sign-on (SSO).
- *Details* displays the application details.

Make sure to assign each application to the appropriate groups on the [User Groups](#) page. This enables the display of the applications in CloudDesktop and authorizes the assigned group members to use the applications.

Application Name	Type	Status	Enabled		
Norton Zone (test env)	SAML	Active	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	<input type="button" value="Remove"/>	<input type="button" value="▶"/>
New Application	SAML	Incomplete	<input type="button" value="Yes"/> <input type="button" value="No"/>		

3. SSO Attribute Mapping

Map the necessary application provider (AP) attributes to attributes used by your identity provider (IdP).

	Application Attribute	Identity Bridge Attribute or Literal Value		Required	
1	<input type="text" value="FirstName"/>	<input type="text" value="First Name"/> <input type="checkbox"/> As Literal <input type="button" value="Advanced"/>	<input checked="" type="checkbox"/>	<input type="button" value="✕"/>	
2	<input type="text" value="LastName"/>	<input type="text" value="Last Name"/> <input type="checkbox"/> As Literal <input type="button" value="Advanced"/>	<input checked="" type="checkbox"/>	<input type="button" value="✕"/>	
3	<input type="text" value="EmailAddress"/>	<input type="text" value="Email"/> <input type="checkbox"/> As Literal <input type="button" value="Advanced"/>	<input checked="" type="checkbox"/>	<input type="button" value="✕"/>	
4	<input type="text" value="SAML_SUBJECT"/>	<input type="text" value="Email"/> <input type="checkbox"/> As Literal <input type="button" value="Advanced"/>	<input type="checkbox"/>	<input type="button" value="✕"/>	

NEXT: Review Setup

Add Application ▾

Once your “SSO Attribute Mapping” is complete, select the “Advanced” button in the row that contains the “SAML_SUBJECT” attribute. You should see a screen similar to the one below. The “Name ID Format to Send to SP” field should be set to “urn:oasis:names:tc:SAML:2.0:nameid-format:transient” – this is a requirement. The allowed values will automatically drop down from the field area, if the “transient” format option is not showing up, simply finish the configuration, but go back after you save/publish, and edit the field before attempting to log on the first time.

• Active applications are enabled for single sign-on (SSO).
Details describe the application details.

Advanced Attribute Options

Advanced Attribute Options for SAML_SUBJECT

Advanced Attribute Options

NameFormat ⓘ

Name ID Format to send to SP:

Attribute Mapping

You can build an attribute mapping using multiple source attributes, literals and transformation functions.

An example of a possible SAML_SUBJECT attribute is:

	IDP Attribute Name or Literal Value	As Literal	Function
1	<input type="text" value="Email"/>	<input type="checkbox"/> As Literal	<input type="text"/>

Start Application Configuration – Part 4

Review the settings on the next page and click “finish”

Application Name	Type	Status	Enabled	
Norton Zone (test env)	SAML	Active	Yes No	Remove ▶
New Application	SAML	Incomplete	Yes No	

4. Review Setup

Test your connection to the application

Logo

Icon

Name Zone Mobile App Center

Description Zone Mobile
zonemobile.appcenterhq.com

(Optional) Click the link below to invite this SaaS Application's Administrator to register their SaaS Application with PingOne.
[Invite SAAS Admin](#)

These parameters may be needed to configure your connection

saasid 3bded6e6-8ba7-4614-a232-51f2bf89799e

Idpid 2c0ee829-337d-4254-9169-09f32a2ffe4d

Protocol Version SAML v 2.0

ACS URL https://zonemobile.appcenterhq.com/appstore/saml2/consumer

entityid https://zonemobile.appcenterhq.com

Initiate Single Sign-On (SSO) URL https://sso.connect.pingidentity.com/sso/sp/initssso?saasid=3bded6e6-8ba7-4614-a232-51f2bf89799e&idpid=2c0ee829-337d-4254-9169-09f32a2ffe4d

Single Sign-On (SSO) Relay State https://pingone.com/1.0/3bded6e6-8ba7-4614-a232-51f2bf89799e

Certificate [Download](#)

SAML Metadata [Download](#)

Single Logout Endpoint

Single Logout Response Endpoint

Force Re-authentication true

Click the link below to open the Single Sign-On page:
[Single Sign-On](#)

Back Finish

Add Application ▾ Pause All SSO

Configuring PingOne Meta-Data for App Center

Now that PingOne has been configured, we need to make a few edits to the PingOne (IDP) meta-data file so that App Center can consume assertions properly. Referring back to the PingOne meta-data file (typically "saml2-metadata-idp.xml") look for the following text/"attribute" nodes:


```
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="PingOne.AuthenticatingAuthority"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"/>
```

```
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="PingOne.idpid"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"/>
```

Replace the above text with the following text:

```
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="FirstName"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"/>
<saml:Attribute
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="LastName" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"/>
<saml:Attribute
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="EmailAddress"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"/>
```

Once you have made those changes, save the file.

Uploading meta-data and mapping attributes in App Center

Log into your App Center as an Administrator, and go to “Settings”>”Server Configuration”. Upload the “saml2-metadata-idp.xml” file we just changed using the “Choose File” button near the “IDP Metadata” file.

Home

Settings

Apps

App Policy

Content

Content Policy

Users

Devices

Device Policy

Downloads

Account

Reports

Settings

User Authentication

Password Lockout

Admin Password Policy

User Password Policy

Offline PIN Policy

Device Clients

iOS Client

Android Client

BlackBerry Client

Mobile User Invitation Email

External Identity Provider

Server Configuration

Authentication Options

Group Options

Device Management

Notifications

Server Configuration

Save

Server Configuration Auth. Options Group Options Enable IDP

Type SAML

Name zonemobile

IDP Metadata Choose File No file chosen
You can download Symantec O3 Sample IDP Metadata File from Downloads section

IDP Contact Info:
HTTP-POST: <https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=2c0ee829-337d-4254-9169-09f32a2ffe4d>
HTTP-Redirect: <https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=2c0ee829-337d-4254-9169-09f32a2ffe4d>

SP Partner ID <https://zonemobile.appcenterhq.com>

SP Entity ID <https://zonemobile.appcenterhq.com> Download SP Metadata File

On the next screen, we need to map the values we just added to the Meta-Data file to the internal values in App Center. Notice that we map “EmailAddress” to both the “Username Attribute” and “Email Attribute” fields – this is not required, but is simple as we do not need to make any custom field types in PingOne.

Also note we are leaving the “Group Attribute” as “Choose an Attribute”. While this disables “Group Mapping” you can still manually add newly provisioned PingOne users to App Center groups.

Symantec | Symantec App Center

English | Messages (0) | End-User Portal | Logout
kyle champlin

Settings

- iOS Client
- Android Client
- BlackBerry Client
- Mobile User Invitation Email
- External Identity Provider
- Server Configuration
- Authentication Options**
- Group Options

Authentication Options [Save]

Server Configuration [✓] **Auth. Options** [●] Group Options [S] Enable IDP [✓]

Username Attribute [EmailAddress]

First Name Attribute [FirstName]

Last Name Attribute [LastName]

Email Attribute [EmailAddress]

Group Attribute [Choose an attribute]

Click “Save” and skip any configuration options for the “Group Options” screen and finally “Enabled IDP” at the very end.

You should now be able to type in your App Center URL (for this example “https://zonemobile.appcenterhq.com”) and it will bring you to the PingOne login page.