# Configuration Guides

June 4, 2025



CONFIGURATION GUIDES

# Copyright

All product technical documentation is Ping Identity Corporation 1001 17th Street, Suite 100 Denver, CO 80202 U.S.A.

Refer to https://docs.pingidentity.com for the most current product documentation.

#### Trademark

Ping Identity, the Ping Identity logo, PingAccess, PingFederate, PingID, PingDirectory, PingDataGovernance, PingIntelligence, and PingOne are registered trademarks of Ping Identity Corporation ("Ping Identity"). All other trademarks or registered trademarks are the property of their respective owners.

### Disclaimer

The information provided in Ping Identity product documentation is provided "as is" without warranty of any kind. Ping Identity disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Ping Identity or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Ping Identity or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

# **Table of Contents**

Con	figuration Guide Overview6
Ado	be Creative Suite
	Configuring SAML SSO with Adobe Creative Cloud and PingFederate
Aha	! Ideas
	Configuring SAML SSO with Aha! Ideas and PingOne
Atla	issian Cloud
	Configuring SAML SSO with Atlassian Cloud and PingFederate
	Configuring SAML SSO with Atlassian Cloud and PingOne for Enterprise
Ama	azon
	Configuring SAML SSO with AWS IAM and PingFederate
	Configuring SAML SSO with AWS IAM and PingOne for Enterprise
	Configuring SAML SSO with Amazon Managed Service for Grafana and PingOne 47
	Configuring SAML SSO with AWS Client VPN and PingOne
Asa	na
	Configuring SAML SSO with Asana and PingOne
Ban	nbooHR
	Configuring SAML SSO with BambooHR and PingFederate
	Configuring SAML SSO with BambooHR and PingOne for Enterprise
Box	
	Configuring SAML SSO with Box and PingFederate
	Configuring SAML SSO with Box and PingOne for Enterprise
Clou	udflare
	Configuring SAML SSO with Cloudflare and PingFederate
Cou	ipa
	Configuring SAML SSO with Coupa and PingFederate
_	Configuring SAML SSO with Coupa and PingOne for Enterprise
Dat	adog
	Configuring SAML SSO with Datadog and PingOne
Doc	cuSign
	Configuring SAML SSO using DocuSign and PingFederate
_	Configuring SAML SSO with DocuSign and PingOne for Enterprise
Dro	pbox
	Configuring SAML SSO with Dropbox and PingFederate
_	Configuring SAML SSO with Dropbox and PingOne for Enterprise
Egn	yte
	Configuring SAML SSO with Egnyte and PingFederate
	Configuring SAML SSO with Egnyte and PingOne for Enterprise

Everno	te	
	Configuring SAML SSO with Evernote and PingFederate	166
	Configuring SAML SSO with Evernote and PingOne for Enterprise	167
Freshw	orks	
	Configuring SAML SSO with Freshworks and PingOne	172
GitHub		
	Configuring SAML SSO with GitHub Cloud and PingFederate	186
	Configuring SAML SSO with GitHub Cloud and PingOne for Enterprise.	188
	Configuring SAML SSO with GitHub Enterprise Server and PingFederate	193
	Configuring SAML SSO with GitHub Enterprise Server and PingOne for Enterprise	195
Greenh	nouse	
	Configuring SAML SSO with Greenhouse and PingOne	202
Heap		
	Configuring SAML SSO with Heap and PingOne	215
HubSpo	ot	
	Configuring SAML SSO with HubSpot and PingFederate	229
	Configuring SAML SSO with HubSpot and PingOne for Enterprise	232
lamf		
Jann	Configuring SAML SSO with lamf Pro and PingFederate	238
	Configuring SAME SSO with Jam Pro and PingOne for Enterprise	241
lira/Cor		
Jil d/ COI	Configuring SAMI SSO with lina/Confluence and PingEederate	248
	Configuring SAME SSO with Jira/Confluence and PingOne for Enterprise	249
live		215
JIVC	Configuring SAML SSO with live and PingEederate	257
	Configuring SAME SSO with live and PingOne for Enterprise	258
Lookou		250
LUUKUU	Configuring SAML SSO with Lookout Secure Access	267
Markot		207
Market	U	271
		2/1
Microco		212
WICTOS	UIL 300 Carafirmaria e CANN SSO with Misses of 200 and Dia Eardanata	275
	Configuring SAML SSO with Microsoft 365 and PingFederate	275
N 4:	Configuring SAME SSO with Microsoft 365 and PingOne for Enterprise	278
Mimeca	ast	
	Configuring SAML SSO with Mimecast and PingFederate.	284
	Configuring SAML SSO with Mimecast and PingOne	285
Namely	/	
	Configuring SAML SSO with Namely and PingFederate	289
_	Configuring SAML SSO with Namely and PingOne	291
Osano		
	Configuring SAML SSO with Osano and PingOne	295

RingCentral	
Configuring SAMI SSO with RingCentral and PingEederate	298
	250
Configuring SAMI SSO with Salesforce and PingEederate	300
Configuring SAME SSO with Salesforce and PingOne for Enterprise	300
	507
Configuring SAML SSO with SAD Notwoover and DingEodorate	210
Configuring SAME SSO with SAP Netwoaver and PingOpe for Enterprise	210
	519
ServiceNow	227
Configuring SAML SSO with ServiceNow and PingOne for Enterprise	327
SIACK	
Configuring SAML SSO with Slack and PingFederate	347
Configuring SAML SSO with Slack and PingOne for Enterprise	354
Splunk	
Configuring SAML SSO with Splunk Cloud and PingFederate	363
Configuring SAML SSO with Splunk Cloud and PingOne for Enterprise	370
SuccessFactors	
Configuring SAML SSO with SuccessFactors and PingFederate	388
Configuring SAML SSO with SuccessFactors and PingOne for Enterprise	392
SumoLogic	
Configuring SAML SSO with SumoLogic and PingFederate	401
Tableau	
Configuring SAML SSO with Tableau and PingOne	407
Configuring SAML SSO with Tableau and PingFederate	410
Configuring SCIM 2.0 provisioning with Tableau and PingFederate	414
Terraform	
Configuring SAML SSO with Terraform and PingOne	419
UltiPro	
Configuring SAML SSO with UltiPro and PingFederate	423
Configuring SAML SSO with UltiPro and PingOne for Enterprise	424
Workato	
Configuring SAML SSO with Workato and PingFederate	429
Configuring SAML SSO with Workato and PingOne	431
Workday	
Configuring SAML SSO with Workday and PingFederate	435
Configuring SAML SSO with Workday and PingOne for Enterprise	443
Workplace by Facebook	
Configuring SAML SSO with Workplace by Facebook and PingOne for Enterprise	456
Wrike	
Configuring SAML SSO with Wrike and PingOne.	462
Zendesk	
Configuring SAML SSO with Zendesk and PingFederate	466

	Configuring SAML SSO with Zendesk and PingOne	474
Zoho		
	Configuring SAML SSO with Zoho and PingOne	491

# **Configuration Guide Overview**

. .

PingIdentity.

Ping Identity supports standards-based identity and access management (IAM) integrations with a wide range of business applications.

These configuration guides cover SAML single sign-on for PingFederate and PingOne. To search and discover more integrations, find downloads, and read documentation, visit the Ping Identity Integration Directory <sup>[2]</sup>.

# **Adobe Creative Suite**

# Configuring SAML SSO with Adobe Creative Cloud and PingFederate

Learn how to enable Adobe Creative Cloud sign-on from the PingFederate console (IdP-initiated sign-on) and direct Adobe Creative Cloud sign-on using PingFederate (SP-initiated sign-on).

#### Before you begin

- Configure PingFederate to authenticate against an identity provider (IdP) or datastore containing the users requiring application access.
- You must have access to the Adobe Creative Cloud Admin Portal. For this, you must have an Enterprise/Business Plan.
- Populate Adobe Creative Cloud with at least one user to test access.
- You must have administrative access in PingFederate.

#### Create a directory within the Adobe admin portal

- 1. Sign on to the Adobe admin portal.
- 2. Click the **Settings** tab.
- 3. Select Identity and click Create Directory.

Directories Domains Trustees			
Q Search	All Statuses	Create Direc	ctory

- 4. Enter a name for the **Directory** and select **Federated ID**.
- 5. Click Next.
- 6. Select Other SAML Providers.

elect the identity provider that your or	ganization uses to authenticate users.	
	G	(STA)
_		$\sim$
Microsoft Azure	Google	Other SAML Providers
Select this option if you are	Select this option if you are	Select this option if you need
using Microsoft Azure Active	using G Suite SCIM 2.0	to configure an identity
Directory SCIM 2.0 capabilities	capabilities for your single	provider (IdP) using SAML.
for your single sign-on (SSO)	sign-on (SSO) needs.	
needs		

#### 7. Click Next.

8. Download the Copy and note the Entity ID and ACS URL values.

# Create a PingFederate service provider (SP) connection for Adobe Creative Cloud

- 1. Sign on to the PingFederate administrative console.
- 2. Configure using Browser SSO profile SAML 2.0.
- 3. Set Partner's Entity ID to the entity ID value that you copied previously.
- 4. Enable the following SAML Profiles:
  - IdP-Initiated SSO
  - SP-Initiated SSO
- 5. In Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfillment, map the SAML\_SUBJECT to your email attribute, map the FirstName to your first name attribute, and map the LastName to your last name attribute.
- 6. In **Protocol Settings: Assertion Consumer Service URL**, set **Binding** to **POST** and set **Endpoint URL** to the ACS URL value that you copied previously.
- 7. In Protocol Settings: Allowable SAML Bindings, enable POST.
- 8. In Credentials: Digital Signature Settings, select the PingFederate Signing Certificate.
- 9. Export the metadata file and certificate from PingFederate to upload to the Adobe Admin Console.

# Test the PingFederate IdP-initiated SSO integration

- 1. Go to the PingFederate SSO Application Endpoint for the Adobe Creative Cloud connection.
- 2. Authenticate with PingFederate.

You're redirected to your Adobe Creative Cloud.

#### Test the PingFederate SP-initiated SSO integration

- 1. Go to your Adobe Creative Cloud.
- 2. When you're redirected to PingFederate, enter your PingFederate username and password.

After successful authentication, you're redirected back to Adobe Creative Cloud.

# **Aha! Ideas**

# Configuring SAML SSO with Aha! Ideas and PingOne

Learn how to configure SAML SSO using Aha! Ideas and PingOne.

# About this task

Learn more about Aha! and SAML SSO in Aha! Roadmaps | Account SSO | SAML 2.0<sup>[]</sup> on the Aha! support site.

# **Obtain your SAML configuration from Aha! Ideas**

- 1. Sign on to your Aha! Ideas admin account.
- 2. On the Account settings page, go to Account  $\rightarrow$  Security and single sign-on.

Account settings	
Personal	>
Account Ping Idenity	~
Account Profile	
Security and single sign-on	
External sharing	
All activity	
Billing	
Users	
Billing	

3. In the Single sign-on section, in the Identity provider list, select SAML 2.0.

dentity provider	✓ Disable Single Sign-on	
	SAML 2.0	
Il identity provide	rs di	
elect identity provider f	rom above and configure it to enable	

### The SAML 2.0 Configuration page opens.

Keep this tab open as you will need these settings in the next procedure.

# **Configure Aha! Ideas in PingOne**

1. In a new tab, sign on to your PingOne SSO admin account.

You'll use the settings from the previous procedure to configure Aha! Ideas in PingOne.

2. Go to **Connections**  $\rightarrow$  **Applications** and click the + icon.

P	ingIdentity.		
Enviro Admir Produc	nments nistrators ~ tion	Applications 🛨	
⊕		Q Search	▼ Filter
	Applications	AppDynamics	
*	Application Catalog	Client ID:	
មា	IDENTITY PROVIDERS	Datadog Client ID:	
0	External IDPs	ESRI	
U	PING PRODUCTS	ArcGIS Client ID:	
Ô	PingFederate	Freshworks freshworks Client ID:	

3. On the New Applications page, click Advanced Configuration and on the SAML line, click Configure.

LECT AN APPLICATION TYPE				
602	T T			R
Web applications that are accessed within a browser.	Applications that are stored and run from a device or desktop.	A front-end application that uses an API.	Management API integrations that can perform actions using Roles.	Apps configured by advanced users fro the ground up.
• .NET web apps • Java apps	IOS and Android apps     Desktop apps     Push Authentication	- Angular - Node.js	Non-interactive service integrations     Client Credentials w/Role Assignment     Interactive admin consoles & portals	Your choice     No barriers     Complete flexibility
WEB APP	NATIVE APP	SINGLE PAGE APP	WORKER	ADVANCED CONFIGURATION
	CHOOSE CC	INNECTION TYPE		
	SAML Apps tha	t utilize an Identity Provider (IDP) to authenticate users a	nd provides Service Providers an Authentication Assertio	n. Configure

- 4. On the Create App Profile page, enter:
  - Application Name (Required)
  - Description (Optional)
  - Icon (Optional)

Pers	sonalize your application by creating a unique profile. The description will help
	APPLICATION NAME
	Aha Ideas
	DESCRIPTION
	Aha Ideas SSO Integration
	ICON
	Aha!
	Remove Image

5. On the **Configure SAML Connection** page, in the **Provide App Metadata** section, click **Manually Enter**.

Configure SAML	Connection
SAML is an authentication protoc	that acts as a service provider (SP) to PingOne (the identity provider, or IdP).
PROVIDE APP METADATA	Import From URL Manually Enter

6. On your Aha! Ideas tab, copy the SAML consumer URL and SAML Entity ID values to a text editor.



Read how to configure SAML	single sign-on on the support site.		
Name			
	Give this single sign-on provider a name that will be displayed to users.		
Configure using	Metadata URL O Metadata file O Manual settings		
Metadata URL			
	Enter the SAML metadata configuration URL from the identity provider.		
Logout redirect URL			
	Optional URL that the user will be redirected to when they logout of Aha!		
SAML consumer URL	https://ping-idenity21.aha.io/auth/saml/callback		
	This is the URL that the identity provider will redirect users to after login.		
SAML service provider	https://ping-idenity21.aha.io/auth/saml/metadata		
metadata URL	This URL may be required by some identity providers.		
SAML entity ID	https://ping-idenity21.aha.io/		
	Unique identifier for the service provider (Aha!).		
New user message	Paragraph ▼   B I U 5		
	No access		
	You currently do not have permission to access any products in Aha!		
	Please contact one of the following users in your account to adjust your product permissions:		

7. In your PingOne SSO account, paste the SAML consumer URLvalue into the ACS URLS section and the SAML entity ID value into the Entity ID section.

S	R METADATA FOR YOUR APPLICATION URLS
F	ttps://ping-idenity21.aha.io/auth/saml/metadata ×
	SIGNING KEY PingOne SSO Certificate for Administrators environme  Download Signing Certificate
0	Sign Assertion Sign Response Sign Assertion & Response GNING ALGORITHM
SI	RSA_SHA256 V
SI	
SI	ENCRYPTION

8. Enter a value in the Assertion Validity Duration field, such as 3600, and then click Save and Continue.

SUBJECT NAMEID FORMAT		
um:oasis:namestc:SAML:1tnameid-formatunspecified		
ASSERTION VALIDITY DURATION (IN SECONIDS)		
3600		
TARGET APPLICATION URL		
Enforce Signed Authn Request		
VERIFICATION CERTIFICATE (OPTIONAL)		
None Import Choose from list		
	Cancel	Save and Continue

9. On the Attribute Mapping page, add the following PingOne Attributes:

User Attribute	Application Attribute
Email Address	EmailAddress

User Attribute	Application Attribute
Family Name	LastName
Given Name	FirstName

# (i) Note

Leave the default **User ID** attribute.

PINGONE USER ATTRIBUTE			APPLICATION ATTRIBUTE			
User ID	~	=	saml_subject	~	Required	
PINGONE USER ATTRIBUTE			APPLICATION ATTRIBUTE			
Email Address	~	=	EmailAddress	-	Required	
Family Name	~	=	LastName	<b>v</b>	Required	
PINGONE USER ATTRIBUTE			APPLICATION ATTRIBUTE			
Given Name	~	=	FirstName	~	Required	
ADD ATTRIBUTE						

# 10. Click Save and Close.

The Applications page opens.

# 11. In the **Applications** page:

1. Click the toggle to enable the configuration by selecting the slider.

# 2. On the **Configuration** tab, in the **Download Metadata** section, click **Download**.

You'll upload this in Aha! Ideas in the next step.

Aha! Aha Ideas Client ID:				<b>()</b> : ×
Profile Configuration Attribute Mappings	Policies Access			
Connection Details           Download Metadata           Issuer ID				1
https://auth.pingone.com/	Ō			
Single Logout Service				
https://auth.pingone.com/	,	Ō		
Single Signon Service				
https://auth.pingone.com/		ē		
IDP Metadata URL				
https://auth.pingone.com/				
Initiate Single Sign-On URL				
https://auth.pingone.com/			Ō	

12. On your Aha! Ideas tab, in the **Configure using** section, click **Metadata file** and click **Choose File** to upload the file that you downloaded in the previous step.

Configure using	O Metadata URL 🛛 Metadata file 🛛 Manual settings
Metadata file	Choose File No file chosen Upload a SAML configuration file in XML format.

13. Enter a **Name** for the connection, such as Ping Identity, and click **Enable** to turn on the configuration.

Read how to configure SAME	single sign-on on the support site.
Name	Ping Identity
	Give this single sign-on provider a name that will be displayed to users.
Configure using	O Metadata URL
Metadata file	Choose File No file chosen
	Upload a SAML configuration file in XML format.
Logout redirect URL	
	Optional URL that the user will be redirected to when they logout of Aha!
SAML consumer URL	https://ping-idenity21.aha.io/auth/saml/callback
	This is the URL that the identity provider will redirect users to after login.
SAML service provider	https://ping-idenity21.aha.io/auth/saml/metadata
metadata URL	This URL may be required by some identity providers.
SAML entity ID	https://ping-idenity21.aha.io/
	Unique identifier for the service provider (Ahal).
New user message	Paragraph ▼   A ▼   ≣ ▼   !≡ ▼   + ▼   *
	No access
	You currently do not have permission to access any products in Aha!
	Please contact one of the following users in your account to adjust your product permissions:
	When new users log in, they may not have access to any products in Aha! yet. If so, this messag will be displayed in-app to tell them how to request access.
Certificate fingerprint	SHA1 V
algorithm	The algorithm used to generate the certificate fingerprint (default is SHA1).

# Create and assign identities

If you've already assigned identities and groups in PingOne, move on to Test the integration.

- 1. In PingOne, go to **Identities**  $\rightarrow$  **Groups** and click the + icon next to **Groups**.
- 2. On the **Create New Group** page, enter values for the following:
  - Group Name (Required)
  - Description (Optional)
  - Population (Optional)
- 3. Click Finish & Save.

Groups       Image: Comparison of the second s	X Create New Group Groups provide application access for users. Enter Profile Data Group Name Description
	Population Administrators Population

4. To add identities to the group, on the **Identities** tab, go to **Users**  $\rightarrow$  + Add User.

P	ingldentity.			② • ③ Explore • La Ryan Schafer •
Enviro Admir Produc	nments listrators ~ tion	Users		
<b>#</b>	< Identities	Q Search or SCIM Query	Filters ~	+ Add User
5	Users		Example SCIM Queries	
2	Groups	4 users by Family Name 🗸		
e e	Populations			
	Attributes			
e	Roles			The second secon
Ø		Test, Adam edamtest		
S				
		Test, Joe joetest		€

5. On the **Add User** page, enter in all the necessary information for a user.

Varify that the email address is correct as this is the value passed in the SAML assertion	()	> Important
Verify that the email address is correct, as this is the value passed in the SAML assertion.		Verify that the email address is correct, as this is the value passed in the SAML assertion.

6. Click Save.

Add User			$\otimes$
COUNTRY CODE	LOCALITY	REGION	
ZIP CODE			
COMPANY INFORMATION			
ACCOUNT ID		POPULATION	
		Administrators Population	
USERNAME			
1			
ТҮРЕ			
TITLE			
PREFERENCES			
PREFERRED LANGUAGE	1	OCALE Ø	
None	~	None ~	
TIMEZONE Select a timezone ~			
Save Cancel			

7. To assign the user that you created to the group that you created previously, locate the user you created and:

- 1. Expand their section.
- 2. Select the Groups tab.
- 3. Click **+ Add**.

Test, Adam adamtest								Reset Password	5 3
Profile	Roles	Authentication	Groups	Consent	API	Sync Status	Credentials		
Group Mer	mberships 1	+ Add							6
Apps									
									Ţ

8. In the Available Groups section, select the group that you created and click the 🕒 icon to add it to the user's group memberships. Click Save.

< Back to Use	s									 
Adam Te	st									
Profile	Roles	Authentication	Groups	Ì						
① Groups det	ine a collectio	on of users using memb	ership or by dy	namic filtering crite	ria. Groups can be	used to assign application	n access to user	s.		
Q Search A	vailable Grou	ips								
AVAILABLE GR	OUPS							GR	OUP MEMBERSHIPS	
ii Admin							÷	:	Apps Administrators Population	$\overline{}$

- 9. On the **Connections** tab, for the Aha! Ideas application:
  - 1. Click the **Access** tab.
  - 2. Click the **Pencil** icon to edit the configuration.

Profile Configuration Attribute Mappings Policies Access GROUP MEMBERSHIP POLICY	Client ID:
GROUP MEMBERSHIP POLICY	Configuration Attribute Mappings Policies Access
	DUP MEMBERSHIP POLICY

10. Select the group that you created and add it to the **Applied Groups** section. Click **Save**.

Aha! Aha Ideas > Edit Access	×
Admin Only Access Must have admin role	
Group Membership Policy Groups can be added to control user access to the application. All u The following selections determine groups that have access to the a	isers have access when no groups are listed. application.
Q Search Groups	
ALL GROUPS	APPLIED GROUPS 1
ii Admin (+)	Here a constraints and the second sec

# Test the integration

1. In the PingOne admin console, go to **Dashboard**  $\rightarrow$  **Environment Properties**.

2. Right-click on the Application Portal URL and open it in a private browser session.



3. In your private browser window, sign on as the test user that you created and click the Aha! Ideas tile.



You're now signed on to the user's Aha! Ideas account.

# **Atlassian Cloud**

# **Configuring SAML SSO with Atlassian Cloud and PingFederate**

#### About this task

The following table details the required and optional attributes to be configured in the assertion attribute contract.

Attribute Name	Description	Required / Optional
SAML_SUBJECT	Email Address	Required
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	First Name	Required
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	Surname	Required
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	ID (not email)	Required

The following table details the references that are used within this guide that are environment specific. Replace these with the suitable value for your environment.

Reference	Description
TenantSSOID	Tenant single sign-on (SSO) ID, retrieved from Atlassian Cloud SAML Single Sign-on configuration as part of EntityID and Assertion Consumer Service (ACS) URL.

# **Create a PingFederate SP connection for Atlassian Cloud**

# γ Νote

The following configuration is untested, and is provided as an example. Additional steps might be required.

- 1. In Atlassian Cloud, go to Security → SAML Single Sign-on and sign on to Atlassian Cloud as an administrator.
- 2. Make a note of the Entity ID and ACS URL values.

You will need these later.

- 3. Sign on to the PingFederate administrative console.
- 4. Using the details retrieved from the application UI:
  - Configure using Browser SSO profile SAML 2.0.

- Enable the IDP-Initiated SSO SAML profile.
- Enable the **SP Initiated SSO** SAML profile.
- In Assertion Creation → Attribute Contract, set the Subject Name Format to urn:oasis:names:tc:SAML:
   2.0:attrname-format:emailAddress.
- Add the following attributes as type urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified:
  - http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
  - http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
  - http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
- In Assertion Creation → Attribute Contract Fulfilment:
  - Map attribute **SAML\_SUBJECT** to the attribute **mail**.
  - Map attribute **givenname** to the attribute **givenName**.
  - Map attribute **surname** to the attribute **sn**.
  - Map attribute **name** to the non-email unique identifier, such as **uid**.
- In **Protocol Settings**:
  - For Assertion Consumer Service URL, enter the consumer service URL retrieved from Atlassian and configure as index 0.
  - For Allowable SAML Bindings, enable Redirect and POST.
- 5. Export the signing certificate public key.

	The first set										-		×
Ľ		nt secure L ni	ina I	+	ofederate/ann#/onCr	opportions					~	• 0	
		or secore   pr	a ye	A CONTRACTOR OF THE CONTRACTOR	greater and a part of the		65 61 ID ID			_	R	~ 0	
P	Pingrederate			AUT	HENTICATION		SECURITY	51	rstem		Q	0	Ð
	< Integratio	n si	РC	Connections									
•	SP Connect	ons On	n this	s screen you can man	age connections to y	our partner SPs.							
	SP Adapter						Search	Clear	Narrow By	~			
1	Target URL Mapping	0	onn	ection Name 🔿	Connection ID		Virtual ID	Protoc	ol Enabled	Action			
	SP Default (	RLs	) All	lassian				SAML 2	0	Select Action ~			
	Policy Cont Adapter Mappings	act	Cre	sate Connection	Import Connectio	n							
	Adapter-to- Adapter Mappings												

# Configure the PingFederate IdP connection for Atlassian Cloud

# ) Νote

The following configuration is untested and is provided as an example. Additional steps might be required.

- 1. Sign in to Atlassian Cloud as an administrator.
- 2. Go to Security  $\rightarrow$  SAML Single Sign-on.
- 3. Click Add SAML Configuration.
- 4. Enter the following details:
  - In the Identity Provider Entity ID field, enter the Issuer value for your PingFederate environment configuration.
  - In the Identity Provider SSO URL field, enter the SSO URL for your PingFederate environment configuration.
  - In a text editor, open the certificate you downloaded during the PingFederate and paste the contents of the certificate into the **Public x509 Certificate** field.
- 5. Click Save Configuration.

# Configuring SAML SSO with Atlassian Cloud and PingOne for Enterprise

About this task

The following table details the required and optional attributes to be configured in the assertion attribute contract.

Attribute Name	Description	Required / Optional
SAML_SUBJECT	Email Address	Required
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	First Name	Required
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	Surname	Required
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	ID (not email)	Required

The following table details the references that are used within this guide that are environment specific. Replace these with the suitable value for your environment.

Reference	Description
TenantSSOID	Tenant single sign-on (SSO) ID, retrieved from Atlassian Cloud SAML Single Sign-on configuration as part of EntityID and Assertion Consumer Service (ACS) URL.

# Create a PingOne for Enterprise Application for Atlassian Cloud

# γ Νote

The following configuration is untested, and is provided as an example. Additional steps might be required.

- 1. In Atlassian Cloud, go to **Security** → **SAML Single Sign-on** and sign on to Atlassian Cloud as an administrator.
- 2. Make a note of the **Entity ID** and **ACS URL** values.
- 3. Sign on to PingOne for Enterprise and go to **Applications**  $\rightarrow$  **Application Catalog**.
- 4. On the SAML tab, in the Add Application list, select Search Application Catalog.

PingOne - My Applications X +				-		×
$\leftarrow$ $\rightarrow$ C ( $\hat{\mathbf{a}}$ admin.pingone.com/web-portal/cas	/connections#/			☆	θ	:
PingOne'	DASHBOARD APPLICATIONS US		0	Sign Of	ו	Î
My Applications Application Catalog	PingID SDK Applications OAu	th Settings				
My Applications						
Applications you've added to your account • Active applications are enabled for sin • Details displays the application details	are listed here. You can search by a gle sign-on (SSO).	application name, description or en	lityid			
Application Name	Type Status	Enabled				
Add Application +			Pause All SSO	0		
Search Application Catalog New SAML Application						ł
Request Ping Identity add a new applic	ation to the application catalog					

5. Search for Atlassian and then click the Atlassian Cloud row.

C & admin.pingone.cor	m/web-portal/cas/application	catalog					☆ <b>券</b>	
<b>'ing</b> One'	DASHBOAI		USERS SETUP	ACCOUNT		•	Sign O	1
My Applications Appl	lication Catalog PingID SI	K Applications O	Auth Settings					
<ul> <li>PingOne - Application Catalog</li> <li>★ → C ▲ admin.pingone.com/web-portal/cas/applicationcatalog</li> <li>PingOne Applications Application Catalog</li> <li>My Applications Application Catalog</li> <li>Browse for the application you want to add or search for it by name. Don't see the application you're looking for? Find Attassian Cloud</li> <li>Application Name ▲ Type</li> <li>Attassian Cloud</li> </ul>		Applications	Application Catalog					
Browse for the application yo	ou want to add or search for it b	y name. Don't see the	application you'r	e looking for? Fill out o	ur Application Reques	t Form.		
Atlassi	s	earch						
							n Catalog	
A	pplication Name	* Туре					n Catalog	
	Atlassian Cloud	ortal/cas/applicationcatalog       OMENDOARD     APPLICATIONS     USDER     SELUP     ACCOUNT     Implicition       Catalog     PingID SDK Applications     OAuth Settings         Implicition     Catalog         Implicition     Search         Implicition     Type         Implicition     SAML with Provisioning (API)						

# 6. Click Setup.

- 7. In the **Signing Certificate** list, select the appropriate signing certificate.
- 8. Review the steps, and make a note of the PingOne SaaS ID, IdP ID, Single Sign-On URL, and Issuer values shown.

PI PingOne	- Application Catalog	× +			-			×
$\leftrightarrow \rightarrow c$	admin.pingo	ne.com/web-portal/cas/applicati	oncatalog		☆	*	θ	:
	1. SSO Instruc	tions						-
	Signi	ing Certificate PingOne Acc	ount Origination Certificate (2021) V Download					
		For reference, ple	ase note the following configuration parameters:					
		SaaS ID						
		IdP ID						
	Initiate Si	ingle Sign-On https://sso.co (SSO) URL e	nnect pingidentity.com/sso/sp/initsso?					
		Issuer https://pingon	e.com/idp/					
		To configure Sing	le Sign-On for Atlassian Cloud, follow the steps below:					
	Security >	SAML Single Sign-On						
	Log In to th	he SaaS Provider						1
		Label	Description					
	1	Atlassian Cloud Setup: Login	Sign on to Atlassian Cloud as an administrator.					
	2	Atlassian Cloud Setup: Access SSO Configuration	Navigate to Security > SAML Single Sign-on					
	з	Atlassian Cloud Setup: Entity Id	Note your Entity ID for later use during configuration in PingOne.					
	4	Atlassian Cloud Setup: ACS URL	Note your ACS URL for later use during configuration in PingOne.					
	-	PingOne Setup: Download	Onlost and developed your similar partition in factors configuration in Atlanta	an Olaud				

# 9. Click Continue to Next Step.

10. Enter the following.

Attribute	Directions	URL
ACS URL	Enter the ACS URL from step 1b.	https://auth.atlassian.com/login/ callback?connection=saml- <i>tenantSSOID</i>
Entity ID	Enter the Entity ID from step 1b.	https://auth.atlassian.com/saml/ tenantSSOID

	_							2	~	
1	<b>P</b> 1	PingOn	e - Application Catalog X +					1	Ŷ	
÷		$\rightarrow$ (	admin.pingone.com/web-portal/cas/application	pricatalog	☆		*	θ	ł	
			2. Connection Configuration							*
			Assign the attribute values for single sig	n-on (SSO) to the application.						
			Upload Metadata @	Select File Or use URL						
			ACS URL	https://auth.atlassian.com/login/calibac * your configuration information.						
			Entity ID	https://auth.atlassian.com/saml/dev						
			Target Resource @	https://start.atlassian.com						
			Single Logout Endpoint @	example.com/slo.endpoint						
			Single Logout Response Endpoint @	example.com/sloresponse.endpoint						
			Primary Verification Certificate @	Choose File No file chosen						
			Secondary Verification Certificate e	Choose File No file chosen						
			Force Re-authentication @	0						
			Encrypt Assertion @	0						
			Signing @	e Sign Assertion ○ Sign Response						
			Signing Algorithm @	RSA_SHA255 V						
_	_					_	_		_	_

12. Configure the **Attribute Mapping** section.

Application Attribute	Identity Bridge Attribute or Literal Value
SAML_SUBJECT	Select a suitable attribute containing the email address.
givenname	Select a suitable attribute containing the user's first name.
surname	Select a suitable attribute containing the user's last name.
name	Select a suitable attribute containing the user's unique ID.
	Note     This should not be the email address.

Pi	PingOne	- Application	Catalog	× +		- 0	×
÷	→ C	🗎 🗎 adr	min.ping	one.com/web-portal/cas/applicationcatalog?x=R3v9CTxTtgM		* * <del>0</del>	:
				Application Name   Typ	ve	_	-î
				Atlassian Cloud S	AML with Provisioning (API)		T
		3. Attr	ribute M Iap you	apping r identity bridge attributes to the attributes required by the appli	cation.		
				Application Attribute	Description	Identity Bridge Attribute or Literal Value	
			1	SAML_SUBJECT*	Email address of the authenticated principal	SAML_SUBJECT	ן
			2	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givennam *	e User's first name.	First Name	
			3	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/sumame	User's last name.	Last Name	
			4	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name *	Internal id for the user that will not change. Note that this id should NOT be the user's email address.	Username As Uteral Advanced	
							,

14. Update the Name, Description, and Category fields as required.

P	PingOne	- Application Catalog × +		-			×
÷	→ C	admin.pingone.com/web-portal/cas/application	atalog2x=R3v9CTxTtgM	☆	*	θ	:
		Application Name	* Туре				1
		Atlassian Cloud	SAML with Provisioning (API)				
		4. PingOne App Customization - Atlassian Cloud	1				ļ
		lcon ⊕					
		Name @	Select image Atlassian Cloud				
		Description ⊕	Atlassian Cloud Enterprise. The new enterprise plan supports unlimited users in the cloud to help you scale the growing collaboration needs of teams across your organization, and deliver enhanced				
		Category @	Information Technology ~				
		NEXT: Group Access	Cancel Back Continue to Next Step				÷

16. Add the user groups for the application.

PI	PingO	ne - A	pplicati	on Catalog 🗙	+															-			×
÷	$\rightarrow$	С	Ĥ a	dmin.pingone	.com/web-p	ortal/cas/appl	licationcatalo	g?x=R3v9C	9CTxTt	tgM										☆	3	Θ	1
			٨		Atlas	sian Cloud				SAM	fL with	h Provis	ioning (	API)							1		_
			5. G	roup Access Select all use see this appl	er groups the	at should have eir personal do	access to thi ock.	is applicatio	ation. U	Jsers	that a	are men	nbers of	f the ad	ded grou	os will be	able to	SSO N	o this a	pplicatio	n and	will	ļ
				Group1,	Group2, etc	:		Search	1														
				Group Nar	ne																		
				Domain Ad	dministrators	s@directory														Rem	ove		
				Users@dir	rectory															Rem	ove		
			N	EXT: Review So	etup													١	Conti	nue lo N	lext S	lep	

- 18. Review the settings.
- 19. Copy the Single Sign-On (SSO) URL value to a temporary location.

This is the IdP-initiated SSO URL that you can use for testing.

20. Make a note of the PingOne Issuer and PingOne idpid values.

You will use these in the Atlassian Cloud configuration.

ľ	Pı	PingO	ne - A	plication Catalog × +		-		1	×
	÷	$\rightarrow$	С	admin.pingone.com/web-portal/cas/application	ncatalog?x=R3v9CTxTtgM	¢	*	θ	÷
				6. Review Setup					^
				Test your connection to the application					
				Icon (					Ì
				Name	Atlassian Cloud				
				Description (	Atlassian Cloud Enterprise. The new enterprise plan supports unlimited users in the cloud to help you scale the growing collaboration needs of teams across your organization, and deliver enhanced capabilities across security, governance, data privacy, and administration. Atlassian cloud products include Jira Software, Jira Service Desk, Confluence, Bitbucket, Trello.				1
ł.				Category (	Information Technology				
				Connection II					
				You may need to configure these conn	ection parameters as well.				
				saasid	1				
				idpi					
				Issue	r https://pingone.com/idp/				
				Signing (	Accortion				*

21. On the Signing Certificate line, click Download. Click Finish.

- U = aon	mapingon	example of the second s			н	~	0	í
		Signing Certificate Download						
		SAML Metadata Download						
		SAML Metadata URL https://admin-api.pingone.com/late	est/metadata/					
		Application Attribute	Description	ldentity Bridge Attribute or Literal Value				
	1	SAML_SUBJECT*	Email address of the authenticated principal	SAML_ SUBJE CT				
	2	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	User's first name.	First Na me				
	3	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/sumame *	User's last name.	Last Na me				
	4	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name *	Internal Id for the user that will not change. Note that this Id should NOT be the user's email address.	Usema me				
	Indicates	a required attribute.						

You will use this in the Atlassian Cloud configuration.

< → C	admin.pingone	e.com/web-portal/cas/conne	ections#/				¢	*	(
Appl - /	ications you've ad Active applications Details displays the	ded to your account are liste are enabled for single sign e application details.	ed here. You can search -on (SSO).	by application name, d	escription or entityid				
		Application Name	Туре	Status	Enabled				
	A	Atlassian Cloud	SAML	Active	Yes	Remove			
	۴b	BambooHR	SAML	Active	Yes	Remove			
	xx	Box	SAML	Active	Yes	Remove			
		Confluence	SAML	Active	Yes	Remove			
	÷	Dropbax	SAML	Active	Yes	Remove			
		simpleSAMLphp	SAML	Active	Yes	Remove			
		Snowflake	SAML	Active	Yes	Remove			
	>	Splunk Cloud	SAML	Active	Yes	Remove			

# Configure the PingOne for Enterprise IdP connection for Atlassian Cloud

# i) Note

The following configuration is untested and is provided as an example. Additional steps might be required.

1. In Atlassian Cloud, go to **Security** → **SAML Single Sign-on** and sign on to Atlassian Cloud as an administrator.

#### 2. Click Add SAML Configuration.

- 3. Enter the following:
  - In the Identity Provider Entity ID field, enter the Issuer value from the PingOne for Enterprise configuration.
  - In the **Identity Provider SSO URL** field, enter https://sso.connect.pingidentity.com/sso/idp/SSO.sam12? idpid=idpid, replacing *idpid* with the one from the PingOne for Enterprise configuration.
  - In a text editor, open the certificate you downloaded during the PingOne for Enterprise configuration, and paste the contents of the certificate into the **Public x509 Certificate** field.
- 4. Click Save Configuration.
# Amazon

# **Configuring SAML SSO with AWS IAM and PingFederate**

Enable Amazon Web Services (AWS) sign-on from a PingFederate URL (IdP-initiated sign-on).

### Before you begin

- Configure PingFederate to authenticate against an identity provider (IdP) or datastore containing the users requiring application access.
- Populate AWS with at least one user to test access.
- You must have administrative access to PingFederate and AWS.

### **Create the PingFederate SP Connection for AWS**

- 1. Sign on to the PingFederate administrative console.
- 2. Configure using Browser SSO profile SAML 2.0.
- 3. Set Partner's Entity ID to urn:amazon:webservices.
- 4. Enable the IdP-Initiated SSO SAML profile.
- 5. Enable the SP Initiated SSO SAML profile.
- 6. In Assertion Creation → Attribute Contract:
  - Extend the contract to add the attributes SAML\_NAME\_FORMAT and https://aws.amazon.com/SAML/Attributes/ Role.
  - Set https://aws.amazon.com/SAML/Attributes/Role to have an Attribute Name Format of urn:oasis:names:tc:S
     AML:2.0:attrname-format:uri.
- 7. In Assertion Creation → Authentication Source Mapping → Attribute Contract Fulfillment:
  - Map SAML\_SUBJECT to an attribute containing the username value.
  - Map SAML\_NAME\_FORMAT to a text value of urn:oasis:names:tc:SAML:2.0:nameid-format:persistent.
  - Map https://aws.amazon.com/SAML/Attributes/Role to a fixed value or your attribute holding the user's AWS role name.
  - In Protocol Settings → Assertion Consumer Service URL, set Binding to Post and set Endpoint URL to https://signin.aws.amazon.com/saml.
    - In Protocol Settings → Allowable SAML Bindings, enable POST.

■ In Credentials → Digital Signature Settings, select the PingFederate Signing Certificate.

- 8. Save the configuration.
- 9. Export the signing certificate.
- 10. Export the metadata file, open it in a text editor, and copy the value of the **entityID** and the **Location** entry (https://your value/idp/SSO.saml2).

# Add the PingFederate IdP connection to AWS

- 1. Sign on to your AWS console as an administrator.
- 2. In the Security, Identity, & Compliance section, select the IAM service.

Al	l services				
	And mutation running		nno compare opennee		Quickaight 🖆
	AWS Snow Family		Resource Groups & Tag Editor		Data Pipeline
	DataSync		Amazon Grafana		AWS Data Exchange
			Amazon Prometheus		AWS Glue
୍ଦ୍ଧ	Networking & Content Delivery		AWS Proton		AWS Lake Formation
	VPC				MSK
	CloudFront	<b>و</b> م	Media Services		AWS Glue DataBrew
	Route 53		Kinesis Video Streams		
	API Gateway		MediaConnect	0	Security, Identity, & Compliance
	Direct Connect		MediaConvert		IAM
	AWS App Mesh		MediaLive		Resource Access Manager
	AWS Cloud Map		MediaPackage		Cognito

- 3. Go to Access Management  $\rightarrow$  Identity Providers.
- 4. Click Add Provider.

ê₩5 Services ▼	Q. Search for services, features, mar	ketplace products, and doce	(Option+8)	\$		• Global •	Support
Identity and Access X Management (IAM)	IAM > Identity providers						
Dashboard	Identity providers (2) Use an identity provider (IdP) to manage your user identities outside of	f AWS, but grant the user identiti	ies permissions to use AWS	De	lete	Add provider	
▼ Access management	resources in your account.						
Groups	Q, Filter properties by property or value					1 > 6	Ð
Usors			-				
Roles	Provider	· 1	Type	Creation time			~
Policies							
Identity providers							
Account settings							

5. Set the following:

Provider Type	SAML
Provider Name	PingFederate

### Metadata Document

Select the PingFederate metadata download file you downloaded previously.

- 6. Continue through to the final page and click **Create**.
- 7. Copy the **ARN** value of the provider.

3W5 Services ▼		Q. Search for services, features, m	arketplace products, and docs	[Option+5]	4	• •	Globel 🔻	Support
Identity and Access × Management (IAM)	IAM > Identity providers >	_						
Dashboard						Assign role	Delet	•
▼ Access management	Summary							
Groups Usars Policies Ndevtity providers Account settings	Provider proofici.com ARN © Emtawa iem-	ni-providen); (com	Type SAML		Creation time March 06, 17:44 (UTC)			
Access reports     Access analyzer     Ansive rules     Analyzers     Bettings     Credential report     Organization activity     Benvice control policies (SCIPa)	Metadata document The document is issued by your liti? It ind Issuer URL ② https://dentity	tudes the issuer's name, expiration infor ly 550.sam12	nation and keys.			Summary	XML	

### 8. In the side menu, select **Roles**.

- 9. Select the role that PingFederate SSO should have access to and then click the **Trust relationships** tab.
- 10. Click Edit Trust Relationship.

aws Services ▼		<b>Q</b> S	earch for se	rvices, features, mark	etplace products, and doc	s [Option+S]
Identity and Access Management (IAM)	Roles > Summary					
Dashboard			Role ARN	arn:aws:iam::	:role/	2
<ul> <li>Access management</li> </ul>		Role	description	Edit		
Groups		Instance Pr	ofile ARNs	ළු		
Users			Path	/		
Roles		Cri	eation time	2020-01-30 14:2	6 UTC	
Policies		L	ast activity	2021-02-19 11:2	6 UTC (6 days ago)	
Identity providers		Maximum sessio	on duration	1 hour Edit		
Account settings	Permissions	Trust relationships	Tags	Access Advisor	Revoke sessions	
	You can view the	tructed entities that ea	n anguma th	o role and the accord	conditions for the role. Cl	haw policy document
Access analyzer	fou can view the	trusted enuties that ca	n assume th	e role and the access	conditions for the role. Si	now policy document
Archive rules	Edit trust relat	lionship				

11. Add the provider ARN value you copied previously to the policy for this role.

Permissions	Trust relationships	Tags	Access Advisor	Revoke sessions						
You can view the trusted entities that can assume the role and the access conditions for the role. Show policy document										
Edit trust re	Edit trust relationship									
Trusted entit	ies					Conditions				
The following to	rusted entities can assum	e this role.				The following conditions define how and when trusted entities can assume the			ssume the ro	
Trusted entitie	15					Condition	Key	Value		
amawsiamal	:saml-provi	der/j	com			StringEquals	SAML:aud	https://signin.aws.amazon.com/saml		

### Test the PingFederate IdP-initiated SSO integration:

- 1. Go to the PingFederate SSO Application Endpoint for the AWS SP connection.
- 2. Complete the PingFederate authentication.

You are redirected to your AWS domain.

aws	Services <b>v</b>	Q, Bearch for service	rs, features, marketplace products, and	decs [Ait+5]	ØŶ	♥ QNa	o 🔻 Support 🛡	
	AWS	5 Manager	ment Console	2				
	AWS se	ervices				Stay connected to your AWS resources on-the-go		
	▼ Rece ① ₩	ntly visited services MM WS Organizations	<ul> <li>EC2</li> <li>Systems Manager</li> </ul>	الا Lambda کی S3		AWS Console Mobile App now supports four additional regions. Download the AWS Console Mobile App to your IOS or Android mobile device. Learn more C		
	► All s	ervices				Explore AWS		
	Build a Get started	Build a solution Get started with simple wizards and automated workflows.				Build Apps Faster with GraphQL AWS AppSync uses GraphQL APIs to query data from multiple data sources in a single request.		
	Launch a With EC2 2-3 minu	a virtual machine	Build a web app With Elastic Beanstalk 6 minutes	Build using virtual server With Lightsail 1-2 minutes	5	Get started 🖸		
	Ċ,	]	ි			Get access to 500+ self-paced online courses covering AWS products and services. Learn more ⊉		
Feedback	English (US) 🔻			© 2008 - 2021, Am	aton web Services, Inc. or	rits attitutes. All rights reserved. Privacy Policy Terms of Use	Cookie preferences	

# Configuring SAML SSO with AWS IAM and PingOne for Enterprise

Enable AWS sign-on from the PingOne for Enterprise console (IdP-initiated sign-on).

### Before you begin

- Link PingOne for Enterprise to an identity repository containing the users that require application access.
- Populate AWS with at least one user to test application access.
- You must have administrative access to PingOne for Enterprise and AWS.

# Set up the AWS Application in PingOne for Enterprise and extract the metadata

- 1. Sign on to PingOne for Enterprise and go to **Applications**  $\rightarrow$  **Application Catalog**.
- 2. In the Application Catalog, search for Amazon Web Services.
- 3. Click the right arrow to expand the Amazon Web Services entry and then click Setup.

Application Catalog	ń	/ Applications / Application Catalog
Browse for the application you want to add or search fo	y name. Don't see the application you're looking for? Fill out our Ap	plication Request Form.
amazon w	earch	
Application Name	* Туре	
a. Amazon Web Services	SAML with Provisioning (API)	

- 4. Click Continue to Next Step twice.
- 5. Map **SAML\_SUBJECT** to the attribute containing the username value.

3. Attribute Mapping Map your identity bridge attributes to the attributes	s required by the application.	
Application Attribute	Description	Identity Bridge Attribute or Literal Value
1 SAML_SUBJECT *	Map this value to the username. Select "Advanced". Under "NameldFormat to send to SP:" select "urn:oasis:names:tc:SAML:2.0:nameid- format:persistent"	SAML_SUBJECT

- 6. Click Advanced.
- 7. Set Name ID Format to sent to SP to urn:oasis:names:tc:SAML:2.0:nameid-format:persistent.



### 8. Click Save.

9. Map the AWS Role attribute to a fixed value or your attribute holding the user's AWS role name.

	Application Attribute	Description	Identity Bridge Attribute or Literal Value
1	SAML_SUBJECT *	Map this value to the username. Select "Advanced". Under "NameldFormat to send to SP:" select "urn:oasis:names:tc:SAML:2.0:nameid- format:persistent"	SAML_SUBJECT
2	https://aws.amazon.com/SAML/Attributes/Role *	Map this to the attribute that matches Role. Select "Advanced". Under "Name Format" select "urn:oasis:names:tc:SAML:2.0:attrname- format:uri". The expected format is: arn:aws:iam::[account- number]:role/[role-name],arn:aws:iam:: [account-number]:saml- provider/[provider-name]	MyRole ⊖As Literal Advanced
3	https://aws.amazon.com/SAML/Attributes/RoleSessionNam	(Optional) Map this to an attribute that will represent the user's display name after logging into AWS.	Name or Literal
4	https://aws.amazon.com/SAML/Attributes/SessionDuration	(Optional) Literal value, in seconds, to designate the duration of the AWS session. Minimum value of	Name or Literal

### 10. Click Advanced.

11. Set NameFormat to urn:oasis:names:tc:SAML:2.0:attrname-format:uri.

Advanced Attri	oute Options			×
Advanced https://aw	Attribute Options for s.amazon.com/SAML/Attributes/Role			
Advanced Att	ibute Options			- 1
Attribute Map	bing			- 1
You can build an a For example, SAN	tribute mapping using multiple source attributes, literals and transformation functions SUBJECT can be (where each attribute value is a separate entry):			- 1
subject = firs	Name + "." + lastName + "@" + domainName			
https://a	s.amazon.com/SAML/Attributes/Role = MyRole			
IDP Attrib	te Name or Literal Value As Literal Function			
1 MyRole	As Literal	Θ		-
			Close	Save

### 12. Click Save.

- 13. Click Continue to Next Step twice.
- 14. Click **Add** for each user group that you want to have access to AWS.

5. Group Access	
Select all user groups that should have access to this application. Users that are members of the added groups will be able to SSO to this application on their personal dock.	olication and will
Group1, Group2, etc Search	
Group Name	
Users@directory	Remove
Domain Administrators@directory	Add

15. Download the metadata.



16. Click Finish.

# Add the PingOne for Enterprise IdP connection to AWS

- 1. Sign on to your AWS console as an administrator.
- 2. Select the IAM service.

All services		
личэ папэгсі ганіку	rate compare optimizer	Quickolyne 🗠
AWS Snow Family	Resource Groups & Tag Editor	Data Pipeline
DataSync	Amazon Grafana	AWS Data Exchange
	Amazon Prometheus	AWS Glue
😞 Networking & Content Delivery	AWS Proton	AWS Lake Formation
VPC		MSK
CloudFront	වේ Media Services	AWS Glue DataBrew
Route 53	Kinesis Video Streams	
API Gateway	MediaConnect	<ol> <li>Security, Identity, &amp; Compliance</li> </ol>
Direct Connect	MediaConvert	IAM
AWS App Mesh	MediaLive	Resource Access Manager
AWS Cloud Map	MediaPackage	Cognito

3. Go to Access Management → Identity Providers and click Add Provider.

aws Services ▼	Q Search for service	as, features, marketplace products, and docs [Option+	3]	¢	▼ Giobal ▼ Support
Identity and Access × Management (IAM)	IAM > Identity providers				
Dashboard	Identity providers (2) Use an identity provider (IdP) to manage your user iden	ntitles outside of AWS, but grant the user identities permissi	ins to use AWS	Delete	Add provider
<ul> <li>Access management</li> </ul>	resources in your account.				
Groups	Q Filter properties by property or value				< 1 > @
Users					
Roles	Provider	▽ Туре	$\bigtriangledown$	Creation time	$\bigtriangledown$
Policies					
Identity providers					
Account settings					

- 4. Set the following:
  - Provider Type: SAML

- Provider Name: PingOne for Enterprise
- Metadata Document: Select the PingOne for Enterprise metadata download file
- 5. Continue through to the final screen and click **Create**.
- 6. Copy the **ARN** value of the provider.

aws Services ▼	Q Search for services, features,	marketplace products, and docs [Option	+S]	\$ <b>•</b>	Global 🔻 Suppor
Identity and Access X Management (IAM)	IAM > Identity providers >			Assign role	Delete
Access management     Groups	Summary				
Users Roles	Provider proofid.com	Type SAML	Creation time March 06,, 17:44 (UTC	)	
Policies Identity providers	ARN 안 <mark>am:aws:iam:: :sami-provider/; .com</mark>				
Account settings     Access reports     Access analyzer	Metadata document This document is issued by your IdP. It includes the issued's name, expiration info	prmation and keys.		Summary	XML
Archive rules Analyzers Settings	Issuer URL 2 https://identity				
Credential report Organization activity	Valid until 순 03/06/2120				
Service control policies (SCPs)	SSO service location				

- 7. Select **Roles** from the side menu, and then select the role that you want PingOne for Enterprise SSO to have access to.
- 8. Click the Trust Relationship tab.
- 9. Click Edit Trust Relationship.

aws Services ▼		Q Search for se	rvices, features, mark	etplace products, and doc	s [Option+S]
Identity and Access Management (IAM)	<sup>Roles →</sup>				
Dashboard		Role ARN	arn:aws:iam::	:role/	2
<ul> <li>Access management</li> </ul>		Role description	Edit		
Groups	Ins	tance Profile ARNs	42		
Users		Path	/		
Roles		Creation time	2020-01-30 14:2	6 UTC	
Policies		Last activity	2021-02-19 11:2	6 UTC (6 days ago)	
Identity providers	Maximu	m session duration	1 hour Edit		
Account settings	Permissions Trust relation	ships Tags	Access Advisor	Revoke sessions	
	You can view the trusted entities	s that can assume th	e role and the access	conditions for the role. St	now policy document
Access analyzer		s that can assume th		conditions for the fole. Of	low policy document
Archive rules	Edit trust relationship				

10. Add the provider ARN value that you copied previously to the policy for the role.

Permissions       Trust relationships       Tags       Access Advisor       Revoke sessions         You can view the trusted entities that can assume the role and the access conditions for the role. Show policy document       Image: Conditions of the role and the access conditions for the role. Show policy document         Edit trust relationship       Trusted entities       Conditions         Trusted entities       Conditions define how and when trusted entities can as         Trusted entities       Condition       Key         arn:aws:iam:       :saml-provider/									
You can view the trusted entities that can assume the role and the access conditions for the role. Show policy document          Edit trust relationship         Trusted entities       Conditions         The following trusted entities can assume this role.       The following conditions define how and when trusted entities can as         Trusted entities       The following conditions define how and when trusted entities can as         arn:aws:iam:       :saml-provider/,com	Permissions	Trust relationships	Tags	Access Advisor	Revoke sessions				
Edit trust relationship       Conditions         Trusted entities       Conditions         The following trusted entities can assume this role.       The following conditions define how and when trusted entities can as         Trusted entities       Condition       Key       Value         arn:aws:iam::       StringEquals       SAML:aud       https://signin.aws.amazon.com/saml	You can view th	e trusted entities that car	n assume the	e role and the access	s conditions for the role.	. Show policy c	locument		
Trusted entities     Conditions       The following trusted entities can assume this role.     The following conditions define how and when trusted entities can as       Trusted entities     Condition       arn:aws:iam::     SAML:aud       https://signin.aws.amazon.com/saml	Edit trust rel	ationship							
The following trusted entities can assume this role.     The following conditions define how and when trusted entities can as       Trusted entities     Condition     Key     Value       arn:aws:iam::     SAML:aud     https://signin.aws.amazon.com/saml	Trusted entit	ies					Conditions		
Trusted entities         Condition         Key         Value           arn:aws:iam::         :saml-provider/; ``l.com         StringEquals         SAML:aud         https://signin.aws.amazon.com/saml	The following tr	usted entities can assum	e this role.				The following	conditions de	fine how and when trusted entities can a
arn:aws:lam:: saml-provider/com StringEquals SAML:aud https://signin.aws.amazon.com/saml	Trusted entitie	35					Condition	Key	Value
	arn:aws:iam::	saml-provic	der/; .c	om			StringEquals	SAML:aud	https://signin.aws.amazon.com/saml

# Test PingOne for Enterprise IdP-initiated SSO

1. Go to your Ping desktop as a user with AWS access.



You can find the Ping desktop URL in the Admin console at Setup  $\rightarrow$  Dock  $\rightarrow$  PingOne Dock URL

2. Authenticate with PingOne for Enterprise.

	Ping Sign On	
USERNAME		
PASSWORD		
	Hemember Me	
	Forgot Password	

You're redirected to your AWS domain.

aws	Service	Q βearch for servic	es, features, marketplace products, and do	s [Alt+S]	D 4	▼ Ohio ▼ Support V	-
		AWS Manager	ment Console				
		AWS services				Stay connected to your AWS resources on-the-go	
		Recently visited services     IAM     AWS Organizations	<ul> <li>EC2</li> <li>Systems Manager</li> </ul>	Lambda 53		AWS Console Mobile App now supports four additional regions. Download the AWS Console Mobile App to your iOS or Android mobile device. Learn more Z	
		All services				Explore AWS	
		Build a solution Get started with simple wizards and automat	ted workflows.			Build Apps Faster with GraphQL AWS AppSync uses GraphQL APIs to query data from multiple data sources in a single request.	
		Launch a virtual machine With EC2 2-3 minutes	Build a web app With Elastic Beanstalk 6 minutes	Build using virtual serve With Lightsail 1-2 minutes	rs	Free Digital Training Get access to 500+ self-paced online courses	
Feedback	English (l		ද්වූවා	• © 2008 - 2021, Ап	nazon Web Services, Inc. or i	covering AWS products and services. Learn more [2] Its affiliates. All rights reserved. Privacy Policy Terms of Use Cookle prefere	nces

# Configuring SAML SSO with Amazon Managed Grafana and PingOne

Learn how to configure SAML SSO for Amazon Managed Grafana and PingOne.

### About this task

# (i) Note

Amazon Managed Grafana only supports SP-initiated SSO that is initiated from the Grafana Workspace URL.

### Configuring an Amazon Managed Grafana connection

#### Steps

- 1. Set up the Amazon Managed Grafana application in PingOne:
  - 1. Go to Applications  $\rightarrow$  Application Catalog.
  - 2. In the Application Catalog, search for Grafana.
  - 3. Expand the Amazon Managed Grafana entry and click Setup.
  - 4. Review the instructions to configure SAML with the Amazon Managed Grafana console.
  - 5. Click Continue to Next Step.
- 2. In the ACS URLfield, replace the *{namespace}* and *{region}* variables with your Grafana namespace and your AWS region.
- 3. In the Entity ID field, replace the \${namespace} and \${region} variables with your Grafana namespace and your AWS region.

4. Click Continue to Next Step.

### Mapping Amazon Managed Grafana attributes

### About this task

PingOne will automatically populate required SAML attributes.

For Amazon Managed Grafana, the required attributes are:

- SAML\_SUBJECT
- mail
- givenName

# (i) Note

You must set SAML\_SUBJECT to Name ID format: urn:oasis:names:tc:SAML:2.0:nameid-format:transient

### Steps

- 1. In the **Application Attribute** field, enter the attribute name as it appears in the application.
- 2. In the Identity Bridge Attribute or Literal Value field, choose one of the following.

### Choose from:

- Enter or select a directory attribute to map to the application attribute.
- Select **As Literal**, then enter a literal value to assign to the application attribute.
- 3. **Optional:** To create advanced attribute mappings, click **Advanced**.

3. SSO Attrib	ute Mapping						
Map the	necessary application provide	(AP) attrib	utes to attributes used by your id	entity provider (IdP).			
	Application Attribute	lo	dentity Bridge Attribute or Literal Val	lue	Re	quired	
			Email (Work)				
1	SAML_SUBJECT		As Literal				×
			Advanced				
			Email (Work)				
2	mail		As Literal				×
			Advanced				
			Display Name				
3	displayName		As Literal				×
			Advanced				

4. Click Continue to Next Step.

## **Customizing Amazon Managed Grafana boxes**

### Steps

1. To change the application icon, click Select Image and upload a local image file.

The image file must be:

- PNG, GIF, or JPG format
- 312 x 52 pixels maximum
- $^{\circ}$  2 MB maximum file size

(i) Note Images are scaled to 64 X 64 pixels for display.

- 2. To change the name of the application displayed on the dock, in the Name field, enter a new name.
- 3. To change the description of the application, in the **Description** field, enter the new description.
- 4. To change the category the application is assigned on the dock, in the **Category** list, select a category.
- 5. Click Continue to Next Step.

### Assigning Amazon Managed Grafana group access

### About this task

The Group Access tab shows every user group that you've created.

### Steps

- 1. To add a group's access to Amazon Managed Grafana, on the row for that group, click Add.
- 2. To remove a group's access, on the row for that group, click **Remove**.
- 3. After you finish assigning groups, click **Continue to Next Step**.

# **Configuring Amazon Managed Grafana SAML**

### Steps

1. In PingOne, on the **Review Setup** tab, either:

### Choose from:

- ° Click Download to download the SAML metadata file
- Copy the PingOne SAML Metadata URL.
- 2. Click Finish to add Amazon Managed Grafana to your PingOne dock.
- 3. In the AWS Console, go to the Amazon Managed Grafana console.

4. To import the SAML metadata into Amazon Managed Grafana, either:

Choose from:

- Use the PingOne SAML Metadata URL on the Amazon Managed Grafana connection summary page in PingOne.
- Upload the SAML metadata file.

aws	Services 🔻	Q Search for services, features, marketplace pro	ducts, and docs [Opti	ion+S]
=	Security Assertion Markup Language (S	AML)	Delete configuration	
	<b>Configure your IdP</b> Configure SAML support on your IdP for this workspace. Provide the ID and the URL info	ormation below to your IdP. This causes IdP metadata to be	generated.	
	Service provider identifier (Entity ID) D https://g-1e907b372d.grafana-workspace.eu-west- 1.amazonaws.com/saml/metadata	Service provider login URL D https://g-1e907b372d.grafana-workspace 1.amazonaws.com/login/saml	e.eu-west-	
	Service provider reply URL (Assertion consumer service URL) D https://g-1e907b372d.grafana-workspace.eu-west- 1.amazonaws.com/saml/acs			
	Import the metadata Once your IdP is configured, an IdP metadata is generated. Import the metadata from a	n XML file, specify a URL or copy and paste to the editor be	low.	
	Import method			
	• URL Specify a URL and we will copy the metadata.	<ul> <li>Upload or copy/paste</li> <li>Upload the XML file from your local computer or</li> </ul>	copy/paste.	
	Metadata URL			
	https://admin-api.pingone.com/latest/metadata/e814ca32-0cd9-4974			

# Assigning Amazon Managed Grafana administrators

### About this task

During authentication to Amazon Managed Grafana, you can optionally assign the Grafana Admin role to users by defining an admin role attribute and populating a PingOne SAML assertion attribute with the expected agreed-upon value.

For the example configuration, in PingOne, the **memberOf** attribute is mapped to the SAML assertion **groups** attribute. In Amazon Managed Grafana, the SAML assertion **groups** attribute is mapped to the Grafana admin role value, as shown in the following image.

Assertion mapping Info Configure SAML assertion attributes to map your IdP user information to AMG work	space users as well as assign orgs and users access to the workspace.
Assertion attribute role for admin An admin is required to set up data sources, assign user permissions, and more.	
Assertion attribute role	
groups	
Admin role values	
GrafanaAdmins@directory	
Enter comma separated values for multiple roles.	
□ I want to opt-out of assigning admins to my workspace.	
Additional settings - optional	
Assertion attribute name	Assertion attribute login
first	mail
Assertion attribute email	Login validity duration (in minutes)
mail	60
Assertion attribute organization	Assertion attribute groups
	groups
Allowed organizations	Editor role values
Eg: Engineering, Sales	GrafanaEditors@directory
Enter comma separated values for multiple roles.	Enter comma separated values for multiple roles.

### Steps

- 1. In your Amazon Managed Grafana workspace, go to SAML Configuration.
- 2. In the Assertion mapping section, in the Assertion attribute role field, enter groups.
- 3. Set the Admin role values to the PingOne group for Grafana admins.

# (i) Note

The example in step 7 uses GrafanaAdmins@directory. The @directory is appended to any PingOne group name.

- 4. Optional: Set the Assertion attribute groups to the groups and Editor role values to the PingOne group for Grafana editors.
- 5. Click Save SAML configuration.
- 6. In PingOne, go to Amazon Managed Grafana application Attribute Mapping.
- 7. Map PingOne's **memberOf** attribute to the SAML assertion **groups** attribute.

3. SSO	Attribute	Mapping		
м	ap the neo	essary application provider (AP) attrib	outes to attributes used by your id	entity provider (IdP).
1	A	pplication Attribute	dentity Bridge Attribute or Literal Va	lue
			Email (Work)	
	1	SAML_SUBJECT	As Literal	
			Advanced	
			Email (Work)	
	2	mail	As Literal	
			Advanced	
			First Name	
	3	first	As Literal	
			Advanced	
			memberOf	
	4	groups	As Literal	
			Advanced	

### Result:

Users in the PingOne **GrafanaAdmins** group are Just-In-Time provisioned during authentication as Grafana admins, and users in the PingOne **GrafanaEditors** group are Just-In-Time provisioned during authentication as Grafana editors.

# Configuring SAML SSO with AWS Client VPN and PingOne

Learn to configure SAML single sign-on (SSO) using AWS Client VPN and PingOne.

### Before you begin

Make sure you have:

- ・An Amazon Web Services (AWS) account ビ
- An Amazon VPC<sup>[]</sup> with an EC2 instance<sup>[]</sup>

### 🏠 Important

In the instance Security Group, allow ICMP traffic from the VPC CIDR range. You need this for testing.

- A private certificate imported into AWS Certificate Manager (ACM)
- PingOne user and group information
- A desktop (Windows or macOS) running the latest AWS Client VPN software

# (i) Note

You can download the software here  $\square$ .

## Create the AWS Client VPN application in PingOne

1. In the PingOne admin portal, go to **Connections**  $\rightarrow$  **Add Application**.



- 2. Click Advanced Configuration.
- 3. In the Choose Connection Type menu, next to SAML, click Configure.

		that can perform actions using Roles.	A front-end application that uses an API.	Applications that are stored and run from a device or desktop.	Web applications that are accessed within a browser.
r choice baniers spicle ficability	Your choice     No barriers     Complete f	Non-interactive service integrations     Client Credentials wRicle Assignment     Interactive admin consoles & portals	- Angular + Node js	KOS and Android apps     Dosktop apps     Push Authentication	• .NET web apps • Java apps
URATION	CONFIGURATIO	WORKER	SINGLE PAGE APP	NATIVE APP	WEB APP
ED		WORKER	SINGLE PAGE APP		WEB APP

4. On the Create App Profile page, enter an Application Name, Description, and Icon for your application. Click Next.

Create App Profile		
Personalize your application by creating a unique pr	offer. The description will help your customers identify the purpose of the application and provide important information to misguided connections.	
APPLICATION NAME		
AWS Client VPN		
DESCRIPTION		
Custom SAML Application for Client VPN		
ICON		
Max Size 1.0 MB		
JPEC, JPC, CIF, PNC		
	Cancel	Ne

5. For Configure SAML Connection, select Manually Enter and configure the following:

- For ACS URLs, enter http://127.0.0.1:35001.
- Select Sign Assertion & Response.
- Select **RSA\_SHA256** as the algorithm for **Signing the response**.
- $\circ$  For Entity ID, enter urn:amazon:webservices:clientvpn.
- For Subject nameID format, enter urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress.
- $\,\circ\,$  For Assertion Validity Duraction (in seconds), enter  $\,$  300 .
- $\,\circ\,$  For  ${\rm SLO}$  options, leave the default settings.

6. After configuring the above values, leave the default settings and click Save and Continue.

Ping/dentity.			() ·	🔊 Explo
APPLICATION NAME AWS Client VPN	Advanced Configuration	PROTOCOL SAML		
Configure SAML Connection SML is an authentication protocol that acts as a service provider (SP) to PingUne (the identity pro	wder, or Id≓).			
INTOVIDE ANY INCLADATA Import Mesidata Import From URL Manually Enter ENTER METADATA FOR YOUR APPLICATION ACS URLS MappinT220.01036001 ×				
SIGNING KEY PregOne SSO Certificate for Administrators environme Download Signing Certificate Signi Assertion Signi Response Signi Assertion & Response Signi Assertion & Response Signi Assertion & Communication Signi Assertion Signi				
		Cunto	Save and	Continue

7. Configure Attribute Mapping by adding the following PingOne Attributes:

PingOne User Attribute	Application Attribute
Username	saml_subject
Given Name	FirstName
Family Name	LastName
Group Names	memberOf

Result:

The new application is shown in the **Applications** list.

- 8. Expand the application details and on the **Policies** tab, click the **Pencil** icon to edit the **Authentication Policy**.
- 9. Expand the application details and on the **Configuration** tab, download the metadata file.

Pi	ingldentıty.		
Enviror Admir Produc	nments nistrators ~ <sup>xtion</sup>	Applications 😁	
	< Connections	Q Search Filter	
<b>.</b>	APPLICATIONS Applications	4 Applications by Application Name	
เข	IDENTITY PROVIDERS	AWS Client VPN Client ID: bedd8f40-2dd8-47d6-8af4-77f1090bd976	
٢	PING PRODUCTS	Profile         Configuration         Attribute Mappings         Policies         Access	
Ô	PingFederate		
	PingIntelligence	DOWNLOAD METADATA:	
(i	<b>Note</b> You'll upload this me	etadata file in the next step.	

# Add PingOne as your IdP in the AWS Management Console

## Important

AWS Client VPN is a separate app and requires a unique IdP definition in AWS. You cannot reuse an IdP already defined for another app, even if it's from the same vendor.

- 1. In the AWS Management Console, open the IAM console and in the Access management section, click Identity providers.
- 2. Click Add Provider.
- 3. For Provider type, select SAML.
- 4. For **Provider name**, enter a unique name.
- 5. For Metadata document, click Choose file and upload the metadata file that you downloaded from PingOne.

Identity and Access × Management (IAM)	Configure provider
Dashboard	Provider type
Access management     User groups     Users     Roles     Policies	SAML     Establish trust between your AWS account and a SAML 2.0 compabile Identity Provider such as Shibbleth or Active Directory Federation Services.     OpenID Connect Establish trust between your AWS account and Identity Provider services, such as Google or Salesforce.     Provider name
Identity providers Account settings	Enter a meaningful name to identify this provider           Ping-Identify           Maximum 128 characters. Use alphanumeric or '' characters.
Access reports     Access analyzer     Archive rules     Analyzers     Settings     Credential report     Organization activity     Service control policies (SCPs)	Metadata document         This document is issued by your IdP. <b>L</b> Choose file          File needs to be a valid UTF-8 XML document. <b>©</b> ping.xml <b>Add tags (Optional)</b> Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.
	No tags associated with the resource.  Add tag You can add up to 50 more tags
	Câncel Add provider

# **Create an AWS Client VPN endpoint**

- 1. In the Amazon VPC console, in the Virtual Private Network (VPN) section, click Client VPN Endpoints.
- 2. Click Create Client VPN Endpoint.
- 3. Enter your desired Name Tag and Description.
- 4. For Client IPv4 CIDR, enter your-IP-range/22.

# (i) Note

This is the IP range that will be allocated to your remote users.

- 5. For Server certificate ARN, select the certificate you created as a prerequisite.
- 6. For Authentication Options, select Use user-based authentication and Federated authentication.
- 7. In the **SAML provider ARN** list, select the PingOne IdP you configured earlier.

ate a new Client VPN endpoint to enable clients to access network	orks over a TLS VPN session	
Name Tag	Ping identity Endpoint	0
Description	Endpoint to authenticate remote users	0
Client IPv4 CIDR hentication Information	192.168.0.0/22	0
Client IPv4 CIDR hentication Information Server certificate ARN	192.168.0.0/22	0 • C 0
Client IPv4 CIDR hentication Information Server certificate ARN Authentication Option	192.168.0.022      Scate     Choose one or more authentication methods fr	• C 0
Client IPv4 CIDR hentication Information Server certificate ARN Authentication Options		C C C
Client IPv4 CIDR hentication Information Server certificate ARN Authentication Options		C O tom below O

8. In the Other optional parameters section, select Enable split-tunnel and leave the rest of the default values.

# (i) **Note** Enabling split-tunnel makes sure that only traffic to the VPC IP range is forwarded via the VPN.

- 9. Configure the other options according to your environment requirements.
- 10. Click Create Client VPN Endpoint to complete the setup.

# Configure the AWS Client VPN Endpoint association

- 1. In the Amazon VPC console, in the Virtual Private Network (VPN) section, click Client VPN Endpoints.
- 2. Select the VPN you created in the last step.

It should be in the Pending state.

- 3. Go to **Options** → **Associations** and click **Associate**.
- 4. In the **Associations** list, select the target VPC and subnet with which you want to associate your endpoint.
- 5. **Optional:** Repeat the previous steps to associate your Client VPN endpoint to another subnet for high availability.

### Set up SAML group-specific authorization

- 1. In the Amazon VPC console, in the Virtual Private Network (VPN) section, click Authorization.
- 2. Click Authorize Ingress.
- 3. For Destination network to enable, specify the IP address of your EC2 instance that you created as a prerequisite.
- 4. In the Grant access to section, select Allow access to users in a specific access group.
- 5. In the Access group ID field, enter the name of the group that you want to allow access to the EC2 instance.

6. Provide an optional description and click Add authorization rule.

# **Connect to the Client VPN**

- 1. In the Amazon VPC console, in the Virtual Private Network (VPN) section, click Client VPN Endpoints.
- 2. Select the VPN that you created.
  - It should be in the **Available** state.
- 3. To download the configuration profile to your desktop, click **Download Client Configuration**.
- 4. Open the AWS Client VPN desktop application.
- 5. Go to File  $\rightarrow$  Manage Profiles.
- 6. Click Add Profile, choose the configuration profile that you downloaded, and give it a Display Name of your choice.

Your profile appears in the AWS Client VPN profile list.

7. Select your profile and click Connect.

You're redirected to PingOne for authentication.

8. Sign on to PingOne as a user with access to your EC2 instance.

After successful authentication, you should be able to reach the EC2 instance in the target VPC.

### **Test your connection**

- 1. To test your connection, send an ICMP ping to the IP of the instance from your command line terminal.
- 2. In your browser, use a plugin, such as SAML-tracer, to confirm that the IdP is sending the correct details in the SAML assertion.

# Asana

# Configuring SAML SSO with Asana and PingOne

Learn how to enable Asana sign-on from the PingOne console (IdP-initiated sign-on) and direct Asana sign-on using PingOne (SP-initiated sign-on).

### Before you begin

- Link PingOne to an identity repository containing the users requiring application access.
- Populate Asana with at least one user to test access.
- You must have administrative access to PingOne and a Super Admin account for an Enterprise Organization on Asana.

### Steps

- 1. Add the Asana application to PingOne:
  - 1. Sign on to PingOne and go to **Connections**  $\rightarrow$  **Applications**.
  - 2. To add a new application, click the + icon next to the **Applications** heading.

ingldentity.		
nments pox - Phil V px	Applications 🔸	
< Connections	Q Search	Filter
APPLICATIONS Applications	3 Applications by Application Name	
IDENTITY PROVIDERS	PingOne Admin Console Client ID	
External IDPs	PingOne Application Portal	
PING PRODUCTS	Client ID: "	
PingFederate PingIntelligence	PingOne Self-Service - MyAccount Client ID: d	
	ingldentity.	Ingldentity.   Ingents   Instant   Instant   Applications   Applications   IDENTITY PROVIDERS   External IDPs   PING PRODUCTS   PingFederate   PingIntelligence   PingOne Self-Service - MyAccount Client ID: Clie

- 3. When prompted to select an application type, select **WEB APP**, then click **Configure** next to **SAML** for the chosen connection type.
- 4. Enter Asana as the application name.
- 5. Enter a suitable description.

- 6. Upload an icon if desired.
- 7. Click Next.
- 8. For Provide App Metadata, select Manually Enter.
- 9. In the ACS URLS field, enter https://app/asana.com/-/saml/consume.
- 10. Select the **Signing Key** to use and then click **Download Signing Certificate** to download the certificate as X509 PEM (.crt).
- 11. In the Entity ID field, enter https://app.asana.com.
- 12. Leave SLO Endpoint and SLO Response Endpoint blank. Asana does not support single logout (SLO).
- 13. Enter a suitable value for Assertion Validity Duration (in seconds). A value of 300 seconds is typical.
- 14. Click Save and Continue.
- 15. Because Asana expects an email address to identify a user in the SSO security assertion:

Choose from:

- If you use email address to sign on through PingOne, click Save and Close.
- If you sign on with a username, select Email Address in the PingOne User Attribute list to map that to the SAML\_SUBJECT, then click Save and Close.
- 16. Enable user access to this new application by moving the toggle to the right.
- 17. On the **Configuration** tab of the newly-created Asana application, copy and save the **Issuer ID** and **Initiate Single Sign-On URL**.

You will need these when configuring SAML on Asana.

^	CONNECTION DETAILS	
	DOWNLOAD METADATA:	Download
	ISSUER ID:	https://auth.pingone.eu/
	SINGLE LOGOUT SERVICE :	https://auth.pingone.eu
	SINGLE SIGNON SERVICE:	https://auth.pingone.eu/20202001_1202_0201_120200211_56/saml20/idp/sso
	IDP METADATA URL:	https://auth.pingone.eu/
	INITIATE SINGLE SIGN-ON URL:	https://auth.pingone.eu/ <b>Case.com/Case.com/Case.com/Case.com/Case.com/Case.com/Case.com</b> /Case.com/Ca

- 2. Add PingOne as an identity provider (IdP) to Asana:
  - 1. Sign on to Asana with a Super Admin account for your Enterprise Organization.
  - 2. Click your profile photo and select **Admin Console** in the menu.
  - 3. Go to the **Security** tab.
  - 4. Go to the **SAML authentication** tab.
  - 5. In SAML options, click Optional.



This is the recommended value when testing. You can change it later to **Required for all members**, **except guest accounts**.

- 6. Paste the Initiate Single Sign-On URL value that you saved earlier into the Sign-in page URL field.
- 7. Open the .crt file that you downloaded in a text editor and copy and paste the entire contents into the **X.509** certificate field.
- 8. Click Save configuration.
- 3. Test the PingOne IdP integration:
  - 1. Go to your PingOne Application Portal and sign on with a user account.



2. Click the Asana icon.

### Result:

You're redirected to the Asana website and signed on with SSO.

- 4. Test the PingOne service provider (SP) integration:
  - 1. Go to https://app.asana.com/ , choose the option to sign on with SSO, and enter your email address only.

#### Result:

You're redirected and presented with a PingOne sign on prompt.

2. Enter your PingOne username and password.

	Ping Sign On	
USERNAME		
PASSWORD		
	Hemember Me	
	Sign On	
	Forgot Password	

## Result:

After successful authentication, you're redirected back to Asana and signed on.

# **BambooHR**

# Configuring SAML SSO with BambooHR and PingFederate

### About this task

The following table details the required and optional attributes to be configured in the assertion attribute contract.

Attribute Name	Description	Required / Optional
<pre>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</pre>	Email address for user	Required

The following table details the references that are used within this guide which are environment specific. Replace these with the suitable value for your environment.

Reference	Description
tenant	BambooHR Tenant name

### Steps

- 1. Create the PingFederate service provider (SP) connection for BambooHR.
  - 1. Sign on to the PingFederate administrative console.
  - 2. Using the metadata from https://tenant.bamboohr.com/saml/sp\_metadata.php, create an SP connection in PingFederate:
    - Configure using Browser SSO profile SAML 2.0
    - Enable the IdP-Initiated SSO SAML profile.
    - Enable the SP initiated SSO SAML profile.
    - In Assertion Creation → Attribute Contract, set the Subject Name Format to urn:oasis:names:tc:SAML: 1.1:nameid-format:emailAddress.
    - In Assertion Creation → Attribute Contract Fulfillment, map the attribute SAML\_SUBJECT to the attribute mail.
    - In Protocol Settings → Allowable SAML Bindings, enable Redirect.
  - 3. Export the metadata for the newly-created SP connection.
  - 4. Export the signing certificate public key.

PT	PingFederate	× +			- 🗆 X
÷	→ C A Not secur	ping.localdomain:9999/pingfederate	/app#/spConnections		☆ \varTheta :
Ping	gFederaté	AUTHENTIC	ATION APPLICATIONS SECUI	rity system	Q   @   ®
	< Integration	SP Connections			
Ð	SP Connections	On this screen you can manage conne	ections to your partner SPs.		
Æ	SP Adapters		Search	Clear Narrow By V	
ŵ	Target URL Mapping	Connection Name   Connect	tion ID Virtual ID	Protocol Enabled Action	
	SP Default URLs	SambooHR-SAML Bamboo	HR-SAML	SAML 2.0 Select Action ~	
	Policy Contract Adapter Mappings	Create Connection Impor	Connection		
	Adapter-to- Adapter Mappings				

- 2. Configure the PingFederate identity provider (IdP) connection for BambooHR.
  - 1. Sign on to BambooHR as a Full Admin administrator user.
  - 2. On the **Settings** page, click **Apps**.
  - 3. On the **SAML Single Sign-On** application published by BambooHR line, click **Install**.



4. In the **SSO Login URL** field, enter the URL Location for **SingleSignOnService Location** retrieved from the PingFederate SP metadata that you downloaded from the BambooHR configuration.

### Example:

#### https://PingFederateHostname:PingFederatePort/idp/SS0.saml2

5. In a text editor, open the signing certificate that you downloaded in from PingFederate and paste the contents into the **x.509 Certificate** field.



### 6. Click Install.

### Result:

Your configuration is complete.

From this point BambooHR will redirect to the configured IdP for authentication for all new sessions. You should complete testing in a private or incognito browser session while keeping the original admin session active. This allows you to change settings or remove the configuration if the integration testing fails.

Apps Settings × +	- 0	×
← → C   bamboohr.com/sett	ings/apps 💁 🗘	•
6 COMPANY LOGO HERE	Home My Info People Hiring Reports Files 🔍 💭 🖗 🌣	
Settings		
🖉 Account	Apps Settings	
Access Levels	Installed	
Ko Employee Fields		
Approvals	SAML Single Sign-On	
🛆 Apps	Uninstall Settings Learn more	
😍 Benefits	Published by BambooHR	
Company Directory		
📷 Email Alerts	Not installed	
Employee Satisfaction	These are the apps that you can install directly from BambooHR, but there are many more available in the BambooHR	
E Hiring	Marketplace	
Holidays		
Color & Color	Google Single Sign-On	

3. Test the integration.

# Choose from: PingFederate IdP-initiated SSO

1. Go to the **SSO Application** in the PingFederate Application configuration to perform IdP-initiated SSO, such as https://PingFederateHostname:PingFederatePort/idp/startSSO.ping?PartnerSpId=BambooHR-SAML.

🕅 Sign On 🗙 🕂		- 0 ×
← → C ▲ Not secure   ping.localdomain:9031/i	idp/startSSO.ping?PartnerSpId=BambooHR-SAML	☆ 😝 :
	Sign On	
	0	
	USERNAME	
	PASSWORD	
	Sign On	
	n	
	Powered by <b>Pingtberkty</b> Copyright © 2003-2020. Ping Identity Corporation. All rights reserved.	

2. Go to the SSO Application Endpoint in the BambooHR configuration



# PingFederate SP-initiated SSO

Go to the URL for your BambooHR tenant: https://tenant.bamboohr.com



# Configuring SAML SSO with BambooHR and PingOne for Enterprise

About this task

The following table details the required and optional attributes to configure in the assertion attribute contract.

Attribute Name	Description	Required / Optional
<pre>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</pre>	Email address for user	Required

The following table details the environment-specific references used in this guide. Replace these references with the suitable value for your environment.

Reference	Description
tenant	BambooHR Tenant name

### Create a PingOne for Enterprise application for BambooHR.

- 1. Download the BambooHR metadata from <a href="https://tenant.bamboohr.com/saml/sp\_metadata.php">https://tenant.bamboohr.com/saml/sp\_metadata.php</a>.
- 2. Sign on to PingOne for Enterprise and go to Applications → Application Catalog.

3. On the SAML tab, in the Add Application list, select Search Application Catalog.

ringune	DAS	HBOARD APPLICATION	USERS SETU	PACCOUNT		⑦ ↓	Sign Off	
My Applications Appli	ation Catalog Pir	gID SDK Applications	OAuth Settings					I
My Applications								
SAML OIDC								
Applications you've added t	your account are lis	ted here. You can sear	ch by application	name, description or e	entityId			
Applications you've added t	, ,		and approximate					
Active applications are     Details displays the app	nabled for single sig	n-on (SSO).						
Active applications are Details displays the app	nabled for single sig ication details.	n-on (SSO).						
Active applications are     Details displays the app	nabled for single sig ication details.	n-on (SSO). Type Status	Er	abled				
Active applications are     Details displays the application Name Use the button below to add	your first application	n-on (SSO). Type Status	Er	abled				
Active applications are Details displays the application Name Use the button below to add Add Application -	your details.	n-on (SSO). Type Status	Er	bled		Pause All SSO	0	
Active applications are Details displays the app Application Name Use the button below to add Add Application - Search Application Cata	your first application	n-on (SSO). Type Status	Er	abled		Pause All SSO	Θ	
Active applications are Details displays the application Name Use the button below to add Add Application • Search Application Catal New SAML Application	your first application	n-on (SSO). Type Status	Er	abled		Pause All SSO	Θ	
Active applications are Details displays the app Application Name Use the button below to add Add Application - Search Application Cata New SAML Application Request Ping Identity add	your first application og	n-on (SSO). Type Status . o the application catalo	En	ibled		Pause All SSO	Ø	

- 4. Search for BambooHR.
- 5. Click the **BambooHR** row.

PingOne - Application Catalog	× +						-		×
$\leftrightarrow$ $\rightarrow$ C $($ admin.pingor	ne.com/web-portal/cas/a	pplicationcatalog?x=8C50Zg	24BnA				☆	θ	()
<b>Ping</b> One'		DASHBOARD APPLICATIONS		ACCOUNT		⊇	Sign Off		Î
My Applications	Application Catalog	PingID SDK Applications	OAuth Settings						
Application	Catalog				Applications / I	Application Catalog			
Browse for the applic	ation you want to add or se	arch for it by name. Don't see	the application you'	re looking for? Fill out ou	r Application Request F	Form.			
bamboohr		Search							
	Applica	ion Name		* Туре			ĺ		
4∗	Bamb	DOHR		SAML		•			

6. Click Setup.

7. In the **Signing Certificate** list, select the appropriate signing certificate.
|   |               |         |  |   |  |                   | <br> |   |   |
|---|---------------|---------|--|---|--|-------------------|------|---|---|
| P | PingO         | ine - A | Application Catalog × +                |   |  |                   | -    |   | × |
| ÷ | $\rightarrow$ | G       | admin.pingone.com/web-port             | al/cas/applicationcatalog?x=8C502   | Zg24BnA  |                   | ☆    | Θ | : |
|   |               |         |  | Application Name  | • Туре   |                   |      |   | î |
|   |               |         | <b>d</b> *                             | BambooHR  | SAML   |                   |      |   |   |
|   |               |         | 1. SSO Instructions                    |   |  |                   |      |   | ł |
|   |               |         | Signing Certificate                    | x       +       -       -       -         accom/web-portal/cas/applicationcatalog?x=8C502g248nA       x       * |  |                   |      |   |   |
|   |               |         | F<br>SaaS ID                           | or reference, please note the follo   | wing configuration parameters:   |                   |      |   |   |
|   |               |         | IdP ID                                 |   |  |                   |      |   |   |
|   |               |         | Initiate Single Sign-On<br>(SSO) URL @ | https://sso.connect.pingidentity  | y.com/sso/sp/initsso?saasid=   |                   |      |   |   |
|   |               |         | Issuer                                 | https://pingone.com/idp/  |  |                   |      |   |   |
|   |               |         | li<br>B                                | n the 'Configure your connection' a<br>SambooHR subdomain for the 'ACS  | application setup page to follow, you will need to replace \${c<br>S URL' field. | ompany} with your |      |   | 1 |
|   |               |         | s                                      | Sign into BambooHR and navigate   | to the following path, then follow the instructions provided in                  | the table below.  |      |   |   |
|   |               |         | Manage -> Single Sign-On               |   |  |                   |      |   |   |
|   |               |         | Label                                  | Description   |  |                   |      |   |   |
|   |               |         | 1 Enabled                              | Under Single S  | Sign-On check the "Enabled" checkbox.  |                   |      |   |   |
|   |               |         | 2 Method                               | Select 'SAML'   | from the drop down box.  |                   |      |   | - |

8. Review the steps, and make a note of the PingOne for Enterprise SaaS ID, IdP ID, Single Sign-On URL, and Issuer values.

#### 9. Click Continue to Next Step.

10. Click Select File and upload the BambooHR metadata you downloaded.

(i) Note
If the upload fails, continue with the next steps and explicitly set the parameters based on the attributes in the metadata.

- 11. Set the ACS URL to https://tenant.bamboohr.com/saml/consume.php.
- 12. Set the Entity ID to BambooHR-SAML.

Pa	PingOr	ne - Application Catalog × +			-			×
÷	<i>→</i> (	C admin.pingone.com/web-portal	/cas/application	rcatalog7x=8C50Zg248nA		☆	θ	:
		A	oplication Nam	е туре				^
		<b>م</b>	BambooHR	SAML				
		2. Connection Configuration						ł
		Assign the attribute values	for single sig	n-on (\$\$O) to the application.				
		Upload N	letadata ⊚	Select File Or use URL				
			ACS URL	https://bamboohr.com/sami/con *				
			Entity ID	BambooHR-SAML				
		Target	Resource @					
		Single Logout	Endpoint @	example.com/sio.endpoint				
		Single Logout Response	Endpoint @	example.com/sloresponse.endpoint				
		Primary Verification (	Certificate @	Choose File No file chosen				
		Secondary Verification (	Certificate @	Choose File No file chosen				
		Force Re-auth	entication @	0				

- 13. Click Continue to Next Step.
- 14. In the Attribute Mapping section, in the Identity Bridge Attribute or Literal Value column of the SAML\_SUBJECT row, select the attribute SAML\_SUBJECT.

P1 PingOne -	Application Catalog × +		- 0	×		
← → C	admin.pingone.com/web-portal/cas/applicationcatalog?x=8C50Zg24BnA					
	Application Name	• Туре				
	BambooHR	SAML				
	3. Attribute Mapping Map your identity bridge attributes to the attributes requ	lired by the application.				
	Application Attribute Description	Identity Bridge Attribute or Literal Value				
	1 SAML_SUBJECT Email	SAML_SUBJECT As Literal Advanced				
	Add new attribute * Indicates a required attribute. NEXT: PingOne App Customization - BambooHR	Cancel Back Continue to Next Step				
			_	-		

16. Update the Name, Description, and Category fields as needed.

								~
1	PingOne	e - Application Catalog X +				-	U	^
(	• > C	admin.pingone.com/web-portal/cas/applicationca	talog?x=8C50Zg24BnA			4	Θ	:
								^
		Application Name		Туре				
		<b>ъ</b> ватьооня		SAML	•			
		4. PingOne App Customization - BambooHR						ļ
		Icon @	ъ					
		Name @	Select image BambooHR					
		Description @	BambooHR is an online HR software solution that drastically reduces the time, expense and complexity of managing employee data.					
		Category @	Human Resources 👻					
		NEXT: Group Access		Cancel Back Con	tinue to Next Step			

18. Add the user groups for the application.

PI	PingO	ne - A	pplicatio	in Catalog X +		0	×
÷	$\rightarrow$	С	ii ac	dmin.pingone.com/web-portal/cas/applicationcatalog?x=8C50Zg248nA	☆	Θ	:
			Select all user groups that should have access to this application. Users that are members of the added groups will be able to SSO to this application and a see this application on their personal dock.				^
				Group1, Group2, etc Search			
				Group Name			
				Domain Administrators@directory Remov	e		
				Users@directory	e		ł
			,	Continue to Nex	t Step	•	
	02	003 -	2021 P	ing Identity Corporation. All rights reserved. Privacy   Terms	Abou	,t	

# 20. Review your settings.

6. Review Setup	
Test your connection to the application	
Icon @	<b>*</b> b
Name @	BambooHR
Description @	BambooHR is an online HR software solution that drastically reduces the time, expense and complexity of managing employee data.
Category @	Human Resources
Connection ID	
You may need to configure these connect	ction parameters as well.
saasid	
idpid	
Issuer	https://pingone.com/idp/
Signing @	Assertion
Signing Algorithm @	RSA_SHA256
Encrypt Assertion @	false

21. Copy the Single Sign-On (SSO) URL value to a temporary location.

PI	Pin	igOne -	Application Catalog × +		-	I		×
←	$\rightarrow$	C	admin.pingone.com/web-portal/cas/applicationca	talog?x=8C50Zg248nA		☆	Θ	:
			<b>a</b>					^
			Single Sign-On (SSO) Relay State ⊕	https://pingone.com/1.0/				
			Single Logout Endpoint					
			Single Logout Response Endpoint					
			Force Re-authentication @	false				
			Signing Certificate	Download				
			SAML Metadata	Download				
			SAML Metadata URL	https://admin-api.pingone.com/latest/metadata/				
			Application Attribute	Identity Bridge Description Attribute or Literal Value				
			1 SAML_SUBJECT *	Email SAML_SUBJE CT				
			* Indicates a required attribute.	Back	nish			

This is the IdP-initiated SSO URL that you can use for testing.

### 22. On the Signing Certificate line, click Download.

You use this in the BambooHR Cloud configuration.

#### 23. On the SAML Metadata line, click Download.

You use this in the BambooHR Cloud configuration.

#### 24. Click Finish.

Pi	PingOne - My Applications x +					- 0	×
$\leftarrow$	→ C admin.pingone.com/web-portal/cas/	connections#/				☆ 8	) =
	<b>Ping</b> One <sup>®</sup>	DASHBOARD APPLICATIONS		ACCOUNT	0	Sign Off	Î
	My Applications Application Catalog	PingID SDK Applications	OAuth Settings				
	My Applications						
	Applications you've added to your account a	re listed here. You can search i	by application na	me, description or entityId			
	<ul> <li>Active applications are enabled for singl</li> <li>Details displays the application details.</li> </ul>	e sign-on (SSO).					
	Application Name	Туре	Status	Enabled			
	BambooHR	SAML	Active	Yes	Remove		
	simpleSAMLphp	SAML	Active	Yes	Remove		
	> Splunik Cloud	SAML	Active	Yes	Remove		
	Add Application -				Pause All SSO	•	

# Configure the PingOne for Enterprise IdP connection for BambooHR

- 1. Sign on to BambooHR as a Full Admin administrator user.
- 2. On the **Settings** page, click **Apps**.

Apps 5	iettings X +	-	•	×
€ → I	C B bamboohr.com	vsettings/apps ov	я <b>е</b>	) : ^
6	COMPANY LOGO HERE	Home My Info People Hiring Reports Files 🔍 🖓 🖗 🕻	×	
<b>\$</b> 5	Settings			
s	Account	Apps Settings		
6	Access Levels	Installed		1
17	Employee Fields			
- I	Approvals			
4	Apps			
¢	Benefits			
B	Company Directory	You don't have any apps installed yet.		
-	Email Alerts	Enhance your BambooHR experience and connect with some of our exceptional technology partners. Some apps can be installed below.		
e	Employee Satisfaction	Ramboold Marketolace		
E	j Hiring	barnoorn manesplace		
ĩ	Holidays			
4	Loro & Color			

3. On the SAML Single Sign-On application published by BambooHR line, click Install.

🔕 Apps Settings 🛛 🗙 🕂			- 🗆 ×
← → ♂ 🕯 bamboohr.com/settin	igs/apps		∾ ± 🖰 i
COMPANY LOGO HERE	-lome My Info People H	iring Reports Files	o 🗜 🖉 🎄
	One Source. Many Benefits. Published by PlanSource	Install Learn more	
	SAML & Published by BambooHR	SAML Single Sign-On Install Learn more	
	Si Small Improvements Published by Small Improvements	Small Improvements Install Learn more	
Privacy Policy - Terms of Service - © 2008-20	21 BambooHR All rights reserved.		*bambooня-

4. In the **SSO Login URL** field, enter the URL Location for **SingleSignOnService Location** retrieved from the PingOne SP metadata that you downloaded from the BambooHR configuration.

#### Example:

```
https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=idpid
```



5. In a text editor, open the signing certificate that you downloaded in the PingOne for Enterprise SP configuration and paste the contents into the **x.509 Certificate** field.

6. Click Install.



#### Result:

Your configuration is complete.

### (i) Note

From this point BambooHR will redirect to the configured IdP for authentication for all new sessions. You should complete testing in a private or incognito browser session while keeping the original admin session active. This allows you to change settings or remove the configuration if the integration testing fails.

### Test the integration

#### Choose from:

### PingOne for Enterprise IdP Initiated SSO

Go to the **Single Sign-On (SSO) URL** in the PingOne Application configuration to perform IdP initiated SSO (https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=saasid&idpid=idpid ).

P1 https://login.pingone.com/idp/di × +		-			×
← → C  ill login.pingone.com/idp/directory/a	/sso/?returnurl=https%3A%2F%2Fsso.connect.pingidentity.com%2Fs	07	☆	θ	:
	Sign On     USERNAME     PASSWORD     Immember Me     Sign On     Proget Password				

# PingOne SP Initiated SSO

Go to the URL for your BambooHR tenant, https://tenant.bamboohr.com



# Box

# **Configuring SAML SSO with Box and PingFederate**

Learn how to configure SAML SSO with Box and PingFederate.

#### About this task

The following table details the required and optional attributes to be configured in the assertion attribute contract.

Attribute Name	Description	Required / Optional
SAML_SUBJECT	Email	Required
givenName	First Name	Optional
sn	Last Name	Optional
memberOf	Groups	Optional

### ) Note

The following configuration is untested and is provided as an example. Additional steps might be required.

#### **Create a PingFederate SP connection for Box**

- 1. Download the Box metadata from https://cloud.app.box.com/s/9y0zm1sqgvkxe8ha2qa3dfhwoivpoyy4<sup>[]</sup>.
- 2. Sign on to the PingFederate administrative console.
- 3. Using the metadata that you downloaded, create an SP connection in PingFederate:
  - 1. Configure using Browser SSO profile SAML 2.0.
  - 2. Enable the following SAML Profiles:
    - IdP-Initiated SO
    - SP-Initiated SSO
    - IdP-Initiated SLO
    - SP-Initiated SLO
  - 3. In Assertion Creation: Attribute Contract, set the Subject Name Format to urn:oasis:names:tc:SAML:1.1:nameidformat:emailAddress.

- 4. Extend the contract with the following attributes:
  - givenName
  - memberOf
  - Sn
- 5. In the Assertion Creation: Attribute Contract Fulfillment section:
  - Map the attribute **SAML\_SUBJECT** to the attribute **mail**.
  - Map the optional attribute **givenName** to the attribute for the user's first name.
  - Map the optional attribute **memberOf** to the attribute for the user's Box roles.
  - Map the optional attribute **Sn** to the attribute for the user's surname or family name.

#### 6. In Protocol Settings:

- In Assertion Consumer Service URL, delete Artifact and PAOS Bindings.
- In SLO Service URLs, delete Artifact and SOAP bindings.
- In Allowable SAML Bindings, enable Redirect and POST.
- 4. Export the metadata for the newly-created SP connection.
- 5. Export the signing certificate public key.

Pr F	PingFederate	× +						-	
<i>←</i>	→ C ▲ Not secur	e   ping.localdomain:9999/pi	ngfederate/app#/spCor	nnections				☆	<b>* 0</b> :
Ping	Federate	A	UTHENTICATION		SECURITY	SYSTEM			
	< Integration	SP Connections							
2	SP Connections	On this screen you can ma	nage connections to yo	ur partner SPs.					
Æ	SP Adapters				Search C	lear Narrow B	у ~		
ŵ	Target URL Mapping	Connection Name A	Connection ID		Virtual ID	Protocol Enable	d Action		
	SP Default URLs	🖉 box.net	box.net		E	SAML 2.0	Select Action $\vee$		
	Policy Contract Adapter Mappings	Create Connection	Import Connection						
	Adapter-to- Adapter Mappings								

# Configure the PingFederate IdP connection for Box

1. Sign on to the Box Admin Console as an administrator.



- 2. Click Enterprise Settings.
- 3. Click the **User Settings** tab.
- 4. In the Configure Single Sign On (SSO) for All Users section, click Configure.



5. Click 'I don't see my provider, or don't have a metadata file.'

#### 6. Complete the Box SSO Setup Support Form:

- 1. Review the request form and the For faster service please read section.
- 2. Complete the required fields:
  - For Who is your Identity Provider?, select Other with Metadata.
  - For What is the attribute for the user's email?, select SAML\_SUBJECT.
  - For What is the attribute for groups?, select memberOf.
  - For What is the attribute for the user's first name?, select givenName.
  - For What is the attribute for the user's last name?, select Sn.
  - Attach the metadata that you downloaded from the PingFederate configuration.
- 7. Click Submit.

Submit a request - Box Support 🗙 +	- 🗆 X
$\leftrightarrow$ $\rightarrow$ C $\cong$ support.box.com/hc/en-us/requests/new?ticket_form_id=360002612594	☆ <b>⊖</b> :
What is the attribute for the user's email?*	
SAML_SUBJECT	
Ex. "SAML_SUBJECT" "emailaddress"	
What is the attribute for groups?	
memberOf	
If using groups, include the attribute here	
What is the attribute for the user's first name?	
givenName	
Ex. "firstName", "givenname"	
What is the attribute for the user's last name?	
sn	
Ex. "lastname", "surname"	
Attachments *	
Add file or drop files here	
Submit	

8. After the Box support team completes the configuration, follow any provided instructions and test the integration.

# Configuring SAML SSO with Box and PingOne for Enterprise

Learn how to configure SAML SSO with Box and PingOne for Enterprise.

#### About this task

The following table details the required and optional attributes to be configured in the assertion attribute contract.

Attribute Name	Description	Required / Optional
SAML_SUBJECT	Email	Required
givenName	First Name	Optional
sn	Last Name	Optional
memberOf	Groups	Optional

### γ Νote

The following configuration is untested and is provided as an example. Additional steps might be required.

# Create a PingOne for Enterprise application for Box

- 1. Download the Box metadata from https://cloud.app.box.com/s/9y0zm1sqgvkxe8ha2qa3dfhwoivpoyy4<sup>[]</sup>.
- 2. Sign on to PingOne for Enterprise and click **Applications**.
- 3. On the SAML tab, click Add Application.

	+											
$\rightarrow$ C $($ admin.pingone.co	m/web-portal/cas/co	nnections#/									\$	0
PingOne <sup>®</sup>	ı	DASHBOARD	APPLICATIONS	USERS	SETUP	ACCOUNT	i i		0	Sign	1 Off	
My Applications Ap	plication Catalog	PingID SDK A	pplications	OAuth Se	ettings							
My Applications												
SAML OIDC												
-												
Applications you've adde	d to your account are	listed here. Y	/ou can search	by applic	ation nar	me, descrip	ption or er	ntityId				
<ul> <li>Active applications a</li> <li>Details displays the i</li> </ul>	re enabled for single :	sign-on (SSO)	).									
<ul> <li>Details displays the a</li> </ul>	application details.											
Application Nar	ne	Туре	Status		Enabl	ed						
Application Nat	ne	Туре	Status		Enabl	ed						
Application Nat	ne add your first applicat	Type ion.	Status		Enabl	ed						
Application Nat	ne add your first applicat	Type ion.	Status		Enabl	ed						
Application Nat Use the button below to a Add Application •	ne add your first applicat	Type ion.	Status		Enabl	ed			Pause All SSO	•		
Application Nat Use the button below to a Add Application • Search Application Ca	ne add your first applicat atalog	Type ion.	Status		Enabl	ed			Pause All SSO	•		
Application Nat Use the button below to a Add Application + Search Application Ca New SAML Applicatio	ne add your first applicat atalog n	Type ion.	Status		Enabl	ed			Pause All SSO	•		
Application Na Use the button below to a Add Application • Search Application Ca New SAML Application Request Ping Identity	ne add your first applicat atalog n add a new applicatio	Type ion.	Status		Enabl	ed			Pause All SSO	Θ		
Application National Vise the button below to a Add Application	ne add your first applicat atalog n add a new applicatio	Type Jon.	Status cation catalog		Enabl	eđ			Pause All SSO			
Application Nat Use the button below to a Add Application Search Application Ca New SAML Application Request Ping Identity	ne add your first applicat atalog n add a new applicatio	Type Ion.	Status cation catalog		Enabl	eđ			Pause All SSO	0		
Application Na Use the button below to a Add Application ~ Search Application Ca New SAML Applicatio Request Ping Identity	ne add your first applicat atalog n add a new applicatio	Type fon.	Status cation catalog		Enabl	ed			Pause All SSO	Ð		

- 4. Click Search Application Catalog and search for Box .
- 5. Click the **Box** row.

$\epsilon \rightarrow 0$	admin.pingone.com/web-portal/cas/ap	plicationcatalog?x=Suz-t0g2	21mo		Ŷ	9	:
	Showing 1 to 10 of 25			123>>>			^
	Application Name		- Type				
	AmeriGives - Sandbox		SAML				
	Athenium Manager - Sa	ndbox	SAML	►			
	Athenium Teamthink - S	andbox	SAML				
	box Box		SAML with Provisioning (API)				
	lcc Nam Descriptic	n e box e e Box n e Collaboration tools	adopted by over 100000				
		companies globally replaces FTP and o workspaces.	6 Box simplifies online file storage, connects teams in online				1
	Catego	y  Collaboration		Setup			
	Corcentric - Sandbox		SAML	•			

# 6. Click Setup.

- 7. Select the appropriate signing certificate.
- 8. Review the steps, and note the **PingOne for Enterprise SaaS ID**, **IdP ID**, **Initiate Single Sign-on (SSO) URL**, and **Issuer** values.

P1	PingOr	e - Applicati	on Catalog × +						-		×
$\leftarrow$	$\rightarrow$	C 🔒 a	dmin.pingone.com/web-port	tal/cas/applicationcat	alog?x=Suz-t0gZ1mo				☆	Θ	:
		box	Box			SAML with Provisioning (API)					•
		1.	SSO Instructions								
			Signing Certificate	PingOne Account	t Origination Certificate	e (2021) V Download					
			F	For reference, please	note the following con	figuration parameters:					1
			Saas ID								
			Initiate Single Sign-On (SSO) URL @	https://sso.connec	ct.pingidentity.com/ss	o/sp/initsso?					
			Issuer	https://pingone.co	m/idp/						
			l v r a r e	n order to allow your want to enable SSO. A node desired (SSO E authenticate using Bo equires a user to logi email, please attach th	users to Single Sign-o Accompanying this em nabled or SSO Requir x credentials however n only via SAML SSO. he PingOne IdP Metad	n to Box, you will need to contact B ail, one must provide Box with the F ed). SSO Enabled mode is where they are also able to login via SAM Users can not use their local Box o ata, which you can download follow	Box via email to inform PingOne metadata al customers can conti IL SSO. SSO Require credentials any more wing the instructions I	n them you nd the SSO nue to ed mode . In the same below.			
			Label		Description						
			1 Continue to	Next Step	Click on the "Continue Configure your conne	e to Next Step" button on this page ction" page	which will bring you t	to "2.			
			2 "Configure y	our connection"	Click on the "Continue	to Next Step" button on this page	as the values on this	page			-

2. In the Upload Metadata section, click Select File, and upload the Box metadata file that you downloaded.

3. Ensure that ACS URL is set to https://sso.services.box.net/sp/ACS.sam12 and Entity ID is set to box.net.

R	$\sim$	1
	U	2

PingOne - Application Catalog × +		-		×
$\leftrightarrow$ $\rightarrow$ C $($ admin.pingone.com/web-portal/cas/applicat	oncatalog?x=Suz-t0gZ1mo	☆	Θ	:
2. Connection Configuration				•
Assign the attribute values for single s	ign-on (SSO) to the application.			
Upload Metadata	Uploaded file:boxmetadata.xml			
	Select File Or use URL			
ACS URL	https://sso.services.box.net/sp/ACS.sa *			
Entity ID	box.net *			
Target Resource				
Single Logout Endpoint @	https://sso.services.box.net/sp/SLO.sai			
Single Logout Response Endpoint	example.com/sloresponse.endpoint			
Primary Verification Certificate	Choose File No file chosen saml20metadata.cer			
Secondary Verification Certificate @	Choose File No file chosen			
Force Re-authentication @				
Encrypt Assertion				

- 9. Click Continue to Next Step.
- 10. In the Attribute Mapping section, in the **Identity Bridge Attribute or Literal Value**column of the **SAML\_SUBJECT**row, select the attribute **SAML\_SUBJECT**.
- 11. Complete the remaining attribute mappings for **givenName**, **sn**, **memberOf**, and **title**.

P1	PingOne -	Application (	Catalog	× +				-		×
←	→ C	🗎 adm	iin.pingo	ne.com/web-portal/cas/	/applicationcatalog?x=Suz-t0gZ1mo			☆	θ	:
		3. Attr	ribute M Aap you	lapping r identity bridge attribu	ites to the attributes required by the ap	plication.				•
				Application Attribute	Description	Identity Bridge Attribute or Literal Value				
						SAML_SUBJECT				
			1	SAML_SUBJECT *	Click to Edit	As Literal				
						Advanced				- 11
					Optional: Lised for Box Auto	First Name				
			2	givenName	provisioning	As Literal				
						Advanced	_			
					Optional: Used for Box Auto-	Last Name				
			3	sn	provisioning	As Literal				
						Advanced				
						Name or Literal				
			4	memberOf	Optional: Used for Box SSO Groups	As Literal				
						Advanced	-			- 14
					Cotionals Used for subdemain	Name or Literal				
			5	ttte	Optional: Used for subdomain	As Literal				
						Rovince				
			Add ne	w attribute						
		*	Indicate	is a required attribute						-

- 12. Click Continue to Next Step.
- 13. Update the Name, Description, and Category fields as required.

PingOne - Application Catalog × +		- 🗆 ×
$\leftrightarrow$ $\rightarrow$ C $($ admin.pingone.com/web-portal/cas/applicationca	atalog?x=Suz-t0gZ1mo	☆ \varTheta :
box Box	SAML with Provisioning (API)	
4. PingOne App Customization - Box Icon @	box	
Name ⊛ Description ⊛	Select image Box * Collaboration tools adopted by over 100000 companies globally. Box simplifies online file storage, replaces FTP and connects teams in online workspaces.	
Category @	Collaboration	
NEXT: Group Access	Cancel Back Continue to Next Step	
Corcentric - Sandbox	SAML	

15. Add suitable user groups for the application.

P1 PingOr	One - Application Catalog X +	-		×
$\leftrightarrow$ $\rightarrow$	C admin.pingone.com/web-portal/cas/applicationcatalog?x=Suz-t0gZ1mo	ž	• •	1
	box Box SAML with Provisioning (API)			
	5. Group Access Select all user groups that should have access to this application. Users that are members of the added groups will be able to SSO to the see this application on their personal dock. Group1, Group2, etc Search	s application and	lliw t	
	Group Name Domain Administrators@directory Users@directory	Remove		
	NEXT: Review Setup	ontinue to Next S	Step	

17. Review the settings.

	Application Catalog	× +			_		~	
← → C	admin.pingon	ne.com/web-portal/cas/applicationca	atalog?x=Suz-t0gZ1mo		¥	2	9	-
		Box	SAML with Provisioning (API)					
	6. Review Setu	dī						
	Test your	connection to the application						
		Icon @	box					
		Name @	Box					ł
		Description @	Collaboration tools adopted by over 100000 companies globally. Box simplifies online file storage, replaces FTP and connects teams in online workspaces.					
		Category @	Collaboration					
		Connection ID						
	You may	need to configure these connec	ction parameters as well.					
		saasid						
		idpid						
		Issuer	https://pingone.com/idp/c					
		Signing @	Assertion					×
PingOne -	<ul> <li>Application Catalog</li> </ul>							
→ C	admin.pingon	× +	atalog?x=Suz-t0gZ1mo		ź	5	Α	1
→ C	admin.pingon	x + ne.com/web-portal/cas/applicationca Signing Certificate	atalog?x=Suz-t0gZ1mo		¥	*	0	
→ C	admin.pingon	× + ne.com/web-portal/cas/applicationca Signing Certificate SAML Metadata	atalog?x=Suz-t0gZ1mo Download Download		ž	~	0	
→ C	admin.pingon	x + ne.com/web-portal/cas/applicationca Signing Certificate SAML Metadata SAML Metadata URL	atalog?x=Suz-t0gZ1mo Download Download https://admin-api.pingone.com/latest/metadata/		5	47	0	
→ C	admin.pingon	x + he.com/web-portal/cas/applicationca Signing Certificate SAML Metadata SAML Metadata URL Application Attribute	atalog?x=Suz-t0gZ1mo Download Download https://admin-api.pingone.com/latest/metadata/ Description	ldentity Bridge Attribute or Literal Value	2	*	0	
→ C	admin.pingon	x +  ae.com/web-portal/cas/applicationca Signing Certificate SAML Metadata SAML Metadata URL Application Attribute SAML_SUBJECT *	atalog?x=Suz-t0gZ1mo Download Download https://admin-api.pingone.com/latest/metadata/ Description Click to Edit	Identiity Bridge Attribute or Literal Value SAML_SUBJE CT	×	*	Θ	*
→ C	admin.pingon	x + he.com/web-portal/cas/applicationca Signing Certificate SAML Metadata SAML Metadata URL Application Attribute SAML_SUBJECT * givenName	atalog?x=Suz-t0gZ1mo Download Download https://admin-api.pingone.com/latest/metadata/ Description Click to Edit Optional: Used for Box Auto-provisioning	Identity Bridge Attribute or Literal Value SAML_SUBJE CT First Name	×	4	0	
→ C	<ul> <li>admin.pingon</li> <li>1</li> <li>2</li> <li>3</li> </ul>	x + he.com/web-portal/cas/applicationca Signing Certificate SAML Metadata SAML Metadata URL Application Attribute SAML_SUBJECT * givenName sn	atalog?x=Suz-t0gZ1mo Download Download https://admin-api.pingone.com/latest/metadata/ Description Click to Edit Optional: Used for Box Auto-provisioning Optional: Used for Box Auto-provisioning	Identity Bridge Attribute or Literal Value SAML_SUBJE CT First Name Last Name	x	*	Θ	*
→ C	admin.pingon	x +  he.com/web-portal/cas/applicationca Signing Certificate SAML Metadata SAML Metadata URL Application Attribute SAML_SUBJECT * givenName sn memberOf	atalog?x=Suz-t0gZ1mo Download Download https://admin-api.pingone.com/latest/metadata/ Description Click to Edit Optional: Used for Box Auto-provisioning Optional: Used for Box Auto-provisioning Optional: Used for Box SSO Groups	Identity Bridge Attribute or Literal Value SAML_SUBJE CT First Name Last Name	X	*	8	
→ C	<ul> <li>▲ admin.pingon</li> <li>1</li> <li>2</li> <li>3</li> <li>4</li> <li>5</li> </ul>	x +  ae.com/web-portal/cas/applicationca Signing Certificate SAML Metadata SAML Metadata URL Application Attribute SAML_SUBJECT * givenName sn memberOf title	atalog?x=Suz-t0gZ1mo Download Download https://admin-api.pingone.com/latest/metadata/ Description Click to Edit Optional: Used for Box Auto-provisioning Optional: Used for Box Auto-provisioning Optional: Used for Box SSO Groups Optional: Used for subdomain	Identity Bridge Attribute or Literal Value SAML_SUBJE CT First Name Last Name	X	*	Θ	
→ C	<ul> <li>▲ admin.pingon</li> <li>1</li> <li>2</li> <li>3</li> <li>4</li> <li>5</li> </ul>	x +  ae.com/web-portal/cas/applicationca Signing Certificate SAML Metadata SAML Metadata URL Application Attribute SAML_SUBJECT * givenName sn memberOf title	atalog?x=Suz-t0gZ1mo Download Download https://admin-api.pingone.com/latest/metadata/ Click to Edit Click to Edit Optional: Used for Box Auto-provisioning Optional: Used for Box SSO Groups Optional: Used for subdomain	Identity Bridge         Attribute or         Literal Value         SAML_SUBJE         CT         First Name         Last Name	X	*	Θ	
→ C	▲ admin.pingon		atalog?x=Suz-t0gZ1mo Download Download https://admin-api.pingone.com/latest/metadata/ Click to Edit Click to Edit Optional: Used for Box Auto-provisioning Optional: Used for Box SSO Groups Optional: Used for subdomain	Identity Bridge         Attribute or         Literal Value         SAML_SUBJE         CT         First Name         Last Name	X	*	θ	
⇒ œ	<ul> <li>admin.pingon</li> <li>1</li> <li>2</li> <li>3</li> <li>4</li> <li>5</li> <li>* Indicate</li> </ul>	x +  he.com/web-portal/cas/applicationca Signing Certificate SAML Metadata SAML Metadata URL Application Attribute SAML_SUBJECT * givenName sn memberOf title es a required attribute.	atalog?x=Suz-t0gZ1mo Download Download https://admin-api.pingone.com/latest/metadata/ Description Click to Edit Optional: Used for Box Auto-provisioning Optional: Used for Box Auto-provisioning Optional: Used for Box SSO Groups Optional: Used for subdomain	Identity Bridge         Attribute or         Literal Value         SAML_SUBJE         CT         First Name         Last Name	X	*	θ	
⇒ c	▲ admin.pingon	x + he.com/web-portal/cas/applicationca Signing Certificate SAML Metadata SAML Metadata URL Application Attribute SAML_SUBJECT * givenName sn memberOf title es a required attribute.	atalog?x=Suz-t0gZ1mo Download Download https://admin-api.pingone.com/latest/metadata/ Click to Edit Click to Edit Optional: Used for Box Auto-provisioning Optional: Used for Box Auto-provisioning Optional: Used for Box SSO Groups Optional: Used for subdomain	Identity Bridge         Attribute or         Literal Value         SAML_SUBJE         CT         First Name         Last Name	X	*	θ	

18. Copy the Single Sign-On (SSO) URL value to a temporary location.

This is the IdP-initiated SSO URL that you can use for testing.

- 19. On the SAML Metadata row, click Download. You will use this for the Box configuration.
- 20. Click Finish.

#### Configure the PingOne for Enterprise IdP connection for Box

1. Sign on to the Box Admin Console as an administrator.



- 2. Click Enterprise Settings.
- 3. Click the User Settings tab.
- 4. In the Configure Single sign-on (SSO) for All Users section, click Configure.

	Powered by Box × +		-		×
$\leftarrow \   \rightarrow$	C app.box.com/master/settings/u	iser	ŕ	0	:
≡	Q Search Users Custom Setup Security	Content & Sharing Notifications User Settings Mobile Device Trust			)
וו פ	User Settings	Sav	2		
::: م ا	Configure Single Sign On (SSO) for All Users SSO can provide a simpler log in process for your end users. Learn more about setting up SSO here.	Configure SSO for Box with a third party identity provider (IdP) for added security. Obtain your IdP SSO metadata file, upload here, and then test and deploy to your enterprise. Processing can take up to 24 hours			
•	Promote Usage of Box Applications	Mobile Promotion          Show Mobile promotion for users         Box Notes Promotion         Show Box Notes promotion for users         Collections Promotion         Show Collections promotion for users			

- 5. Click I don't see my provider, or don't have a metadata file.
- 6. Complete the Box SSO Setup Support Form:
  - $\circ\,$  Review the request form and the For faster service please read section.
  - $\,\circ\,$  Complete all the required fields.
    - For Who is your Identity Provider, select Other with Metadata.
    - For What is the attribute for the user's email?, select SAML\_SUBJECT.
    - For What is the attribute for groups?, select memberOf.
    - For What is the attribute for the user's first name?, select givenName.
    - For What is the attribute for the user's last name?, select Sn.
    - Attach the metadata that you downloaded from the PingOne for Enterprise configuration.
  - Click Submit.

ubmit a request – Box Support 🗙 🕂	- 0
C support.box.com/hc/en-us/requests/new?ticket_form_id=360002612594	☆ (
What is the attribute for the user's email?*	
SAML_SUBJECT	
Ex. "SAML_SUBJECT" "emailaddress"	
What is the attribute for groups?	
memberOf	
If using groups, include the attribute here	
What is the attribute for the user's first name?	
givenName	
Ex. "firstName", "givenname"	
What is the attribute for the user's last name?	
sn	
Ex. "lastname", "surname"	
Attachments *	
Add file or drop files here	

7. After the Box support team completes the configuration, follow any provided instructions and test the integration.

# Cloudflare

# Configuring SAML SSO with Cloudflare and PingFederate

Learn how to direct Cloudflare sign on using PingFederate (SP-initiated sign-on).

#### Before you begin

- Configure PingFederate to authenticate against an identity provider (IdP) or datastore containing the users requiring application access.
- PingFederate's X.509 certificate should be exchanged to verify the signature in SAML assertions.
- An Email Attribute is required in the assertion, either the SAML Subject or another SAML attribute per the SAML configuration. The value of the Email Attribute must be a valid email address. It is used to uniquely identify the user in the organization.
- Populate Cloudflare with at least one user to test access.

#### Create a PingFederate service provider (SP) connection for Cloudflare:

- 1. Sign on to the PingFederate administrative console.
- 2. Create an SP connection for Cloudflare in PingFederate:
  - 1. Configure using Browser SSO profile SAML 2.0.
  - 2. Set Partner's Entity ID to https://team name.cloudflareaccess.com/cdn-cgi/access/callback .
  - 3. Enable the IDP-Initiated SSO and SP-Initiated SSO SAML profiles.
  - In Assertion Creation: Attribute Contract, select urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress for SAML\_SUBJECT.
  - 5. In Assertion Creation: Authentication Source Mapping: Authentication Source Mapping, map a new Adapter Instance to HTML Form.
  - 6. In Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfillment, map SAML\_SUBJECT.
  - 7. In Protocol Settings: Assertion Consumer Service URL, set Binding to POST and set Endpoint URL to /cdn-cgi/ access/callback.

#### (i) Note

This value is received and updated from Cloudflare.

8. In Protocol Settings: Allowable SAML Bindings, enable POST.

- 9. In Signature Policy, disable Always Sign Assertion and leave Sign Response As Required enabled.
- 10. In Credentials: Digital Signature Settings, select the PingFederate Signing Certificate, the Include the Certificate in the Signature *KEY INFO* Element, and the Include the Raw Key in the Signature *KEY INFO* Element check boxes.
- 3. Save the configuration.
- 4. Export the signing certificate.
- 5. Export and then open the metadata file, and copy the value of:
  - The entityID
  - The Location entry(https://your value/idp/SS0.saml2)

# Add the PingFederate IdP connection to Cloudflare

1. Sign on to the Cloudflare application and click **pingfed.com** at the top of the page.

$\leftrightarrow$ $\rightarrow$ C $\triangleq$ dash.cloudflare.com/21f8d803f37a30b63f919	187c5302e2a				☆ 😕	Lupdate
CLOUDFLARE pingfed.com			Add site	Support 🔻	English (US) 🔻	± •
	Home Members Audit Log Billing Configurations Notifications Registrar					
	Q. jsearch websites in Seshadri.addanki@proofid.com's Accour       Image: Comparison of the server Update	Create custom billing alerts. Receive an email when billable usage exceeds a certain amount. © Configure				
		Account Analytics Beta Overview of traffic to all your sites.				
		Deploy front-end applications in record time.				
		Workers Build serverless applications.				
		Registrar Transfer domains with zero mark-up on renewals.				
		Stream Upload and stream videos effortiessly.				
		Zero Trust security for everyone.				
		Web Analytics Free analytics without changing your DNS.				
		Carbon Impact Report View your carbon impact on the				

2. Go to Access  $\rightarrow$  Access App Launch  $\rightarrow$  Setup Access App Launch.

Setup Access App Launch				
When end users visit the Access App Launch page, they will be prompted to authenticate with your identity provider. Once logged in, the page will display the applications they can reach as tiles. When the user selects a tile, the browser will open the application.				
You can control which users in your team can reach this page with the policy below. The rules saved who can reach the Access App Launch page. This policy does not impact or change the permissions the applications behind Access.	I here define ; for any of			
Include				
Everyone   Everyone	$\times$			
+ Add another include rule				
+ Exclude + Require				
Cance	el Save			

#### 3. Click Save.

4. Go to Access  $\rightarrow$  Login Methods  $\rightarrow$  Add  $\rightarrow$  SAML.

← → C 🔒 dash.cloudflare.com/21f8d8	803f37a30b63f919187c5302e2a/pingfed.com/access		
CLOUDFLARE pingfed.com	Add a <b>SAML</b> identity provider		×
	Drop or select IdP metadata file to upload	Instructions 1. You would be able to integrate with any SAML 2.0 based identity provider.	^
	Provider Name Your SAML Provider Name Single Sign On URL Your SAML URL IdP Entity ID or Issuer URL Your identity provider's id Signing certificate Signing certificate SAML signing certificate Sign SAML authentication request (optional) Email attribute name (optional) SAML attribute name for email	1. You would be able to integrate with any SAML 2.0 based identity provider.     2. Here's the sample instructions for Okta, Centrify, and Active Directory.     3. Use	
	SAML attributes (optional) No attributes configured + Add an attribute SAML header attributes (optional) No headers configured + Add a header	4	× •

5. Click Drop or select IdP metadata file to upload to upload the IdP metadata file and enter the Provider Name value.

← → C ash.cloudflare.com/21f8d803f37a30b63f919187c5302e2a/pingfed.com/access		1
CLOUDFLARE pingfed.com	Add site Suppor	🔻 Eng
	3 () () () () () () () () () () () () ()	
Add a <b>SAML</b> identity provider	×	
metadata (1).x	Instructions	
	You would be able to integrate with any SAML 2.0 based identity provider.     Arrev's the sample instructions for Okta, Centrify, and Active Directory.	
Provider NameO pingfed	3.Use https://pingfed.cloudflareaccess.com/cdn-cgi/access/callback	
Single Sign On URL®	as your Assertion consumer (ACS) URL and SP Entity ID as mentioned in the documentation.	
IdP Entity ID or Issuer URL <sup>①</sup> Your identity provider's id	4. You can configure the attributes received via SAML assertion as headers for your application. Input the attribute name you intend to use and map it to the SAML attribute.	
Signing certificate D	<ol><li>Toggle the box to set it as a header. You can add additional attributes after saving them first. This step can also be skipped if you do not need to configure any headers.</li></ol>	
SAML signing certificate	6. Some identity providers allow you to upload the metadata file for Cloudflare (listed as "Service Provider Metadata file"). You can download your unique file by following the link here.	
Sign SAML authentication request (optional)	You can build policies based on groups defined in your SAML provider configuration using the group name as an attribute. To do so, configure the attribute name in the integration modal here and then select "SAML Group" as a rule option when creating the policy.	
Save		
Access Policies Control which individuals he G Suite Okt	Create Access Policy	

- 6. Click **Save** and close the **Login Method** page.
- 7. On the **Teams** dashboard, go to **Settings**  $\rightarrow$  **Authentication**.
- 8. In the Login methods section, select SAML + Pingfed.

← → C 🗎 dash.tear	s.cloudflare.com/21f8d803f37a30b63f919187c5302e2a/settings/authentication		🖈 🌲 😩 🗘 Update
<ul> <li>Cloudflare for Teams</li> <li>Home</li> <li>Gateway</li> </ul>	Back to Settings		
- Access -	Authentication		
<ul> <li>a Cogs</li> <li>Analytics ▼</li> <li>Analytics ▼</li> <li>Settings</li> </ul>	Global session timeout Set the maximum session length for all your applications.	Timeout: Same as application session timeout Edit	
	App Launcher Define who has access to the App Launcher.	Manage	
	Login methods	Add new	
	Gne-time PIN	Edit	
	🖒 SAML • pingfed	Iest   Edit	
🛓 Sethadriaddanki@pr 🔻			
-			

The Cloudflare connection configuration is now complete.

### 9. Click Test.

10. After the Cloudflare application redirects to PingFederate, enter the credentials.



# Test the PingFederate SP-initiated SSO integration

1. Go to your **Cloudflare Authentication Request URL** (for example, https://pingfed.cloudflareaccess.com/) and click **Login**.



2. Click SAML- PingFed.

<ul> <li>Sign in - Cloudflare Access x +</li> <li>← → C is pindled.cloudflareaccess.com/cdn-ca/access/login/pindled.cloudflareaccess.com/?cdn</li> </ul>	direct_url=%2F8kid=b6cc7709e9561643a4dd8705d83c8d1403b67fa523a146 <u>e488f687363a427536</u>	● - G × ☆ 🎧 Inconta (3) (Uottie - 1)
	·	
	pingfed cloudflareaccess.com	
	App Launcher Sign in with:	
	└♪ SAML · Pingfed	
	Get a login code emailed to you	
	Email example@email.com	
	Send me a code	
	Loudflare for Teams	
3. After you're redirected to PingFederate, enter your PingFederate username and password.

After successful authentication, you're redirected back to Cloudflare.

# Coupa

# Configuring SAML SSO with Coupa and PingFederate

Learn how to enable Coupa sign-on from a PingFederate URL (IdP-initiated sign-on) and direct Coupa sign-on using PingFederate (SP-initiated sign-on).

### Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users requiring application access.
- Populate Coupa with at least one user to test access.
- You must have administrative access to PingFederate and Coupa.

## Download the Coupa metadata

- 1. Sign on to your Coupa Admin organization as an administrator.
- 2. Go to https://your\_site.coupahost.com/administration/security.
- 3. Select the Sign in using SAML check box.
- 4. Click the Download and import SP metadata link.
- 5. Save the Coupa metadata.

## **Create a PingFederate SP connection for Coupa**

- 1. Sign on to the PingFederate administrative console.
- 2. Create an SP connection for Coupa in PingFederate using the Coupa metadata:
  - 1. Configure using Browser SSO profile SAML 2.0.
    - Enable the following SAML Profiles:
      - IdP-Initiated SSO
      - SP-Initiated SSO
    - In Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfillment, map SAML\_SUBJECT to the attribute containing a user's email address.
    - In Protocol Settings: Allowable SAML Bindings, enable POST.
    - In Credentials: Digital Signature Settings select the PingFederate signing certificate.
- 3. Save the configuration.

- 4. Export the signing certificate.
- 5. Export the metadata file.

## Add the PingFederate IdP Connection to Coupa

- 1. Sign on to your Coupa Admin organization as an administrator.
- 2. Go to https://your\_site.coupahost.com/administration/security.
- 3. Make sure that the Sign in using SAML check box is selected.
- 4. In the Upload IdP metadata section, click Choose File.
- 5. Select the PingFederate metadata file and import it.
- 6. In the **Certificate** field, upload the PingFederate signing certificate.
- 7. Click Save.
- 8. Click the Users tab and edit the users who will use SAML authentication.
- 9. Set Single Sign-On ID to the value users will use to sign on, for example, their email address.
- 10. Set Authentication method to SAML.
- 11. Click Save.

## Test the PingFederate IdP-initiated SSO integration

- 1. Go to the PingFederate SSO application endpoint for the Coupa SP connection.
- 2. Complete PingFederate authentication.

You're redirected to your Coupa domain.

## Test the PingFederate SP-initiated SSO integration:

- 1. Go to your Coupa URL.
- 2. After you're redirected to PingFederate, enter your PingFederate username and password.

You're redirected back to Coupa.

# Configuring SAML SSO with Coupa and PingOne for Enterprise

Learn how to enable Coupa sign-on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct Coupa sign-on using PingOne for Enterprise (SP-initiated sign-on).

#### Before you begin

- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Populate Coupa with at least one user to test access.

• You must have administrative access to PingOne for Enterprise and Coupa.

## Download the Coupa metadata

- 1. Sign on to your Coupa Admin organization as an administrator.
- 2. Go to https://your\_site.coupahost.com/administration/security.
- 3. Select the Sign in using SAML check box.
- 4. Click the Download and import SP metadata link.
- 5. Save the Coupa metadata.

## Set up the Coupa application in PingOne for Enterprise and extract the metadata

- 1. Sign on to PingOne for Enterprise for Enterprise and go to **Applications**  $\rightarrow$  **Application Catalog**.
- 2. Search for Coupa.
- 3. Expand the Coupa entry and click the **Setup** icon.

Application	Catalog			Applications / Appl	ication Catalog
Browse for the applic	ation you want to add or search f	or it by name. D	on't see the application you're looking for? Fill out ou	ur Application Request Form	ı.
Coupa		Search			
	Application Name	•	Туре		
Çicoupa	Coupa		SAML with Provisioning (API)		

4. Copy the IdP ID value.

Signing Certificate	PingOne Account Origination Certificate (2021) 🗸	Download
Fo SaaS ID	r reference, please note the following configuration particle and the followin	rameters:
IdP ID		

- 5. Click Continue to Next Step.
- 6. Click Select File and upload the Coupa metadata file.

2. Connection Configuration	
Assign the attribute values for single sign	-on (SSO) to the application.
Upload Metadata 🛛 💿	Select File Or use URL
ACS URL	https://
Entity ID	.coupahost.com

7. Edit the ACS URL to add a relay state parameter to enable IdP initiated sign-on.

https://your-environment.coupahost.com/sp/ACS.saml2?RelayState=https://your-environment.coupahost.com/ sessions/saml\_post

- 8. Click Continue to Next Step.
- 9. Ensure **SAML\_SUBJECT** is mapped to the field containing a user's email address.

3. Attribut	Attribute Mapping				
Мар у	Map your identity bridge attributes to the attributes required by the application.				
	Application Attribute	Description	Identity Bridge Attribute or Literal Value		
1	SAML_SUBJECT *	\${map to your email}	Email (Work)		
			Advanced		

- 10. Click Continue to Next Step twice.
- 11. Click **Add** for all user groups that should have access to Coupa.

5. Group Access		
Select all user groups that should have access to the see this application on their personal dock.	nis application. Users that are members of the added groups will be able to SSO to	this application and will
Group1, Group2, etc	Search	
Group Name		
Users@directory		Remove
Domain Administrators@directory		Add

#### 12. Click Continue to Next Step.

13. Download the PingOne for Enterprise SAML metadata and signing certificate.

Single Logout Response Endpoint		
Force Re-authentication @	false	
Signing Certificate	Download	
SAML Metadata	Download	

14. Click Finish.

## Add the PingOne for Enterprise IdP connection to Coupa

- 1. Sign on to your Coupa Admin organization as an administrator.
- 2. Go to https://your\_site.coupahost.com/administration/security.
- 3. Ensure the Sign in using SAML check box is selected.
- 4. In the Upload IdP metadata section, click Choose File, select the PingOne for Enterprise metadata, and import the file.
- 5. Confirm that the Login Page URL field has the IdP ID value from PingOne for Enterprise.

https://your site.coupahost.com/sp/startSSO.ping?PartnerIdpId=PingOne for Enterprise IdP ID value&TARGET= https://your site.coupahost.com/sessions/saml\_post

- 6. In the **Certificate** field, upload the PingOne for Enterprise signing certificate.
- 7. Click Save.
- 8. Click the **Users** tab and edit the users who will use SAML authentication.
- 9. Set Single Sign-On ID to the value users will use to sign on, for example, their email address.

- 10. Set Authentication method to SAML.
- 11. Click Save.

## Test the PingOne for Enterprise IdP-initiated SSO integration:

1. Go to your Ping desktop as a user with Coupa access.

## (i) Note

To find the Ping desktop URL in the Admin console, go to **Setup**  $\rightarrow$  **Dock**  $\rightarrow$  **PingOne Dock URL**.

2. Complete PingOne for Enterprise authentication.

You're redirected to your Coupa domain.

		Ping Kentity Sign On	
USER	NAME		
PASS	WORD		
		Remember Me	
		Sign On	
		Forgot Password	

## Test the PingOne for Enterprise SP-initiated SSO integration

- 1. Go to your Coupa URL.
- 2. After you're redirected to PingOne, enter your PingOne for Enterprise username and password.



You're redirected back to Coupa.

# Datadog

## Configuring SAML SSO with Datadog and PingOne

Learn how to enable SAML SSO with Datadog and PingOne

#### Before you begin

To enable SSO within Datadog, you must have an administrator account.

#### About this task

i Νote

This is a tested integration.

#### Set up the integration

- 1. Sign on to your PingOne SSO admin account and go to **Connections** → **Applications** and click the plus icon (+).
- 2. On the New Application page, click Advanced Configuration, and on the SAML line, click Configure.
- 3. On the Create App Profile page, enter the following:
  - 1. Application Name
  - 2. Optional: Description
  - 3. Optional: Icon
- 4. Click Next.
- 5. On the corresponding **Configure SAML Connection** page, click **Manually Enter** to begin configuring Datadog with PingOne.
- 6. In a new tab, sign on to your Datadog admin account. In the lower left hand corner, click on your account name and then **Configure SAML**, which will contain information for the next step.
- 7. In PingOne, enter the following information for the required fields:
  - 1. The ACS URL(s) of the application.

You can find this on the Datadog admin console under Assertion Consumer Service URL.

2. The **Entity ID** of the application. from the previous step.

You can find this on the Datadog admin console under Service Provider Entity ID.

3. Update the SUBJECT NAMEID FORMAT to urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress.

- 4. Enter the Assertion Validity Duration (in seconds), for example, 3600.
- 5. Configure the remaining options as needed.
- 6. Click Save and Continue.
- 8. On the Attribute Mapping page, enter the following attributes:
  - 1. Outgoing value: User ID = Application Attribute: saml\_subject (required).
  - 2. Outgoing value: Family Name = Application Attribute: sn
  - 3. Outgoing value: Given Name = Application Attribute: givenName
  - 4. Outgoing value: Username = Application Attribute: eduPersonPrincipalName
  - 5. Click Save and Close.

### (i) Note

You can add additional attributes to control roles. See the Datadog documentation for more information.

- 9. On the newly-created application, click the Configuration tab and click Download Metadata.
- 10. In your Datadog account, click **Choose File**, upload the IdP metadata that you downloaded in the previous step, and click **Upload File**.
- 11. After uploading the IdP metadata and configuring your IdP, click **Enable** to enable SAML and finalize the configuration.
- 12. If you're leveraging this integration for an IdP-initiated sign-on, in the **Additional Features** section of Datadog, make sure to select the **Identity Provider (IdP) Initiated Login** check box.

The set up is now complete.

#### **Create and assign identities**

Before you test the integration, you must create and assign identities in PingOne.

## ) Note

If you've already assigned identities and groups in PingOne, you can test the integration.

- 1. In PingOne, go to **Identities**  $\rightarrow$  **Groups** and click the + icon next to **Groups**.
- 2. On the Create New Group page, enter values for the following:
  - Group Name (Required)
  - **Description** (Optional)
  - Population (Optional)
- 3. Click Finish & Save.
- 4. To add identities to the group, on the **Identities** tab, go to **Users**  $\rightarrow$  + Add User.

5. On the **Add User**page, enter in all the necessary information for a user.

## 介 Important

Verify the first name, last name, USER ID, and USERNAME are correct, as these are values passed in the SAML assertion.

- 6. Click Save.
- 7. Assign the user that you created to the group that you created previously.

Locate the user you created and do the following:

- 1. Expand the section for the user.
- 2. Select the **Groups** tab.
- 3. Click **+ Add**.
- 8. In the **Available Groups** section, select the group that you created and click the + icon to add it to the user's group memberships. Click **Save**.
- 9. On the **Connections** tab, for the Datadog application:
  - Click the Access tab
  - $^\circ\,$  Click the Pencil icon to edit the configuration
- 10. Select the group that you created and add it to the Applied Groups section. Click Save.

## **Test the integration**

- 1. In the PingOne admin console, go to **Dashboard**  $\rightarrow$  **Environment Properties**.
- 2. Right-click on the Application Portal URL and open it in a private browser session.
- 3. Sign on as the test user that you created and click the Datadog tile.

You're signed on to the user's Datadog account using SSO and testing is complete.

# DocuSign

# Configuring SAML SSO using DocuSign and PingFederate

Learn how to enable DocuSign sign on from a PingFederate URL (IdP-initiated sign-on) and direct DocuSign sign on using PingFederate (SP-initiated sign-on).

#### Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users requiring application access.
- Make sure DocuSign has a valid domain, an organisation created, and is populated with at least one user to test access.
- You must have administrative access to PingFederate and DocuSign.

#### Create a PingFederate SP Connection for DocuSign

- 1. Sign on to PingFederate administration console.
- 2. Create an SP connection for DocuSign in PingFederate:
  - Configure using Browser SSO profile SAML 2.0.
  - Set Partner's Entity ID to Placeholder .

You will update this value later.

- Enable the following SAML Profiles:
  - IdP-Initiated SSO
  - SP-Initiated SSO
- In Assertion Creation: Attribute Contract, extend the contract to add attributes named SAML\_NAME\_FORMAT, surna me, givenname and emailaddress.
- In Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfillment, map SAML\_SUBJECT, surname, givenname and emailaddress and map SAML\_NAME\_FORMAT to urn:oasis:names:tc:SAML: 2.0:nameid-format:persistent.
- In Protocol Settings: Assertion Consumer Service URL, set binding to POST, and set Endpoint URL to http://placeholder.

You will update the placeholder value later.

- In Protocol Settings: Allowable SAML Bindings, enable POST.
- In Credentials: Digital Signature Settings, select the PingFederate signing certificate.

- 3. Save the configuration.
- 4. Export the signing certificate.
- 5. Export and then open the metadata file, and copy the value of these properties:
  - entityID
  - Location entry (https://your value/idp/SS0.saml2)

## Add the PingFederate connection to DocuSign

- 1. Sign on to your DocuSign domain as an administrator.
- 2. In the left navigation pane, select Identity Providers, and then click Add Identity Provider.

III DocuSign Ad	min
SWITCH TO	Identity Providers Allow users to sign into DocuSign using their corporate credentials. Enable single sign-on for your organization by adding your identity provider below.
Admin Home Overview Accounts	The default account and permission profile are used for basic just-in-time provisioning of new users.
Connected Apps Audit Logs Bulk Actions	Default Account ID EDIT
USERS Usera	Default Permission Profile DS Viewer
Administrators	ADD IDENTITY PROVIDER
Domains	Name ^ Certificate Status

3. Configure the following fields.

Field	Value
Name	A name for the identity provider.
Identity Provider Issuer	Enter the <b>Issue</b> value from PingID.
Identity Provider Login URL	<pre>https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=PingOn e IdP ID value</pre>
Send AuthN Request by	Click <b>POST</b> .
Select Send Logout Request by	Click <b>POST</b> .

Name *	
Identity Provider Issu	er *
Identity Provider Logi	in URL *
Identity Provider Logo	out URL
Identity Provider Met:	adata URL
Sign AuthN reque	st
Sign logout reque	st
Enable Third-Party	y Login
Send AuthN request by	у.
GET	
POST	
	ur.
Send logout request by	y.
Send logout request by	y.

4. In the **Custom Attribute Mapping** section, click **Add New Mapping**, and then:

- In the Field list, select surname, then enter surname in the Attribute field.
- In the Field list, select givenname, then enter givenname in the Attribute field.
- In the Field list, select emailaddress, then enter emailaddress in the Attribute field.
- 5. Click Save.

#### 6. Click Add New Certificate.

Name A	Certificate Status
PinsOne	A No Valid Certificates
ragoire	Add New Certificate

7. Click Add Certificate.

Identity	Provider	Certificates		
ADD CERTIFICATE				
Certificate Issuer 🔺				
SAVE	CANCEL			

- 8. Select the signing certificate that downloaded from PingFederate. Click **Save**.
- 9. In the Actions list for the identity provider that you created, select Endpoints.

Identity Providers		
Allow users to sign into DocuSign using their corporate credentials. Enable single sign-on for your organization by adding your identit	y provider below.	
The default account and permission profile are used for basic just-in-time provisioning of new users.		
Default Account		
Defeult Account ID EDIT		
Default Permission Profile DS Viewer		
ADD IDENTITY PROVIDER		
Name -	Certificate Status	
PingOne	🤣 Valid	ACTIONS *
		Edit
		Endpoints
		Looie

10. Copy the Service Provider Issuer URL and Service Provider Assertion Consumer Service URL values.

View SAML 2.0 Endpoints
Service Provider Issuer URL
Service Provider Assertion Consumer Service URL
Service Provider Metadata URL
Service Provider Login URL
CLOSE

The DocuSign connection configuration is complete.

## (i) Note

After testing, you can set the domain to require IP authentication to remove the DocuSign sign-on screen.

## Update the EntityID and ACS URL values in PingFederate

- 1. Sign on to the PingFederate administrative console.
- 2. Edit the SP connection for DocuSign.
- 3. Set Partner's Entity ID to the DocuSign Service Provider Issuer URL value.
- 4. Set Assertion Consumer Service URL Endpoint URL to the DocuSign Service Provider Assertion Consumer Service URL value.
- 5. Save the changes.

## Test the PingFederate IdP-initiated SSO integration

- 1. Go to the PingFederate SSO application endpoint for the DocuSign SP connection.
- 2. Complete PingFederate authentication.

You're redirected to your DocuSign domain.

DocuSign eSignature	Home	Manage	Reports				
				Lust 6 Months			
	Point Count Foreco	signed by: dr. Your, Signats 0489203487-	ue.	0 Action Required	0 Waiting for Others	0 Expiring Soon	0 Completed

## Test the PingFederate SP-initiated SSO integration

- 1. Go to https://account.docusign.com  $\square$ .
- 2. Enter your email address.
- 3. Click Use Company Login.
- 4. After you're redirected to PingFederate, enter your PingFederate username and password.

After successful authentication, you're redirected back to DocuSign.

DocuSign eSignature	Home	Manage	Reports					
				Lood & Marches				
	Creat	signed by: de Your Signate	AL.	0	0	0	0	
	- F8160	0482034F7		Action Required	Walting for Others	Expiring Soon	Completed	

# Configuring SAML SSO with DocuSign and PingOne for Enterprise

Learn how to enable DocuSign sign on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct DocuSign sign on using PingOne for Enterprise (SP initiated sign on).

#### Before you begin

- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Make sure DocuSign has a valid domain, an organization created, and is populated with at least one user to test access.
- You must have administrative access to PingOne for Enterprise and DocuSign.

## Copy PingOne values for the Supplied DocuSign Application

1. Sign on to PingOne for Enterprise, go to **Applications**  $\rightarrow$  **Application Catalog**, and search for DocuSign.

Application	n Catalog		👚 / Applic	ations / Application Catalog
Browse for the app	lication you want to add or se	arch for it by name. Don't see the applic	cation you're looking for? Fill out our Application f	Request Form.
DocuSign		Search		
	Application Na	me	^ Туре	
Docufige	DocuSign 2.	) - Demo	SAML	•
Doculige	DocuSign 2.	) - Production	SAML	▶

- 2. Expand the **DocuSign 2.0 Production** entry and click the **Setup** icon.
- 3. Copy the **Issuer** and **IdP ID** values.
- 4. Download the **Signing Certificate**.

1. SSO Instructions	
Signing Certificate	PingOne Account Origination Certificate (2021) V
F	or reference, please note the following configuration parameters:
SaaS ID	
IdP ID	
Initiate Single Sign-On (SSO) URL @	E TELETIONE E E E PARA VERA PARA -
Issuer	

## Add the PingOne for Enterprise IdP Connection to DocuSign

- 1. Sign on to your DocuSign Admin organization as an administrator.
- 2. In the left navigation pane, select **Identity Providers**, and then click **Add Identity Provider**.

III DocuSign Ad	lmin
SWITCH TO	Identity Providers Allow users to sign into DocuSign using their corporate credentials. Enable single sign-on for your organization by adding your identity provider below.
Admin Home Overview Accounts Connected Acos	The default account and permission profile are used for basic just-In-time provisioning of new users.  Default Account
Audit Logs Bulk Actions	Default Account ID EDIT
USERS	DS Viewer
Administrators	ADD IDENTITY PROVIDER
ACCESS MANAGEMENT	
Domains	Name   Certificate Status
Identity Providers	

## 3. Configure the following fields

Field	Value
Name	A name for the identity provider
Identity Provider Issuer	The <b>Issue</b> value from PingID
Identity Provider Login URL	<pre>https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=PingOn e for Enterprise IdP ID value</pre>
Send AuthN Request by	POST
Select Send Logout Request by	POST

Name *		
Identity Provide	r Issuer *	
Identity Provide	r Login URL *	
Identity Provide	r Logout URL	
Identity Provide	r Metadata URL	
Sign AuthN	request	
	request	
Sign logout		
Enable Third	d-Party Login	
Sign logout	d-Party Login uest by:	
Sign logout	d-Party Login uest by:	
Sign logout Enable Thirr Send AuthN requ GET POST	d-Party Login west by:	
Sign logout Enable Thirr Send AuthN requ GET POST Send logout requ	d-Party Login uest by:	
Send AuthN required of the send logout required of the send l	d-Party Login uest by: uest by:	

4. In the **Custom Attribute Mapping** section, click **Add New Mapping**, and then:

- In the Field list, select surname, then enter surname in the Attribute field.
- In the Field list, select givenname, then enter givenname in the Attribute field.
- In the Field list, select emailaddress, then enter emailaddress in the Attribute field.
- 5. Click Save.

#### 6. Click Add New Certificate.

Name -	Certificate Status
PinnOne	🛕 No Valid Certificates
ragono	Add New Certificate

7. Click Add Certificate.

Identity	Provider	Certificates
ADD CEF	RTIFICATE	
Certific	ate Issuer 🔺	
SAVE	CANCEL	

8. Select the signing certificate that you downloaded from PingOne for Enterprise. Click Save.

9. In the Actions list for the IdP that you created, select Endpoints.

Identity Providers		
Allow users to sign into DocuSign using their corporate credentials.	ble single sign-on for your organization by adding your identity provider below.	
The default account and permission profile are used for basic just-in	e provisioning of new users.	
Default Account		
Defeuit Account ID EDIT		
Default Permission Profile DS Viewer		
ADD IDENTITY PROVIDER		
Name -	Certificate Status	
PingOne	🧭 Valid	ACTIONS *
		Edit
		Endpoints Delete

10. Copy the Service Provider Issuer URL and Service Provider Assertion Consumer Service URL values.

View SAML 2.0 Endpoints	
Service Provider Issuer URL	1
Service Provider Assertion Consumer Service URL	1
Service Provider Metadata URL	
Service Provider Login URL	
CLOSE	

The DocuSign connection configuration is complete.

## (i) Note

After testing, you can set the domain to require IP authentication to remove the DocuSign sign-on screen.

## Complete the DocuSign setup in PingOne for Enterprise

1. Continue editing the DocuSign entry in PingOne for Enterprise.

## (i) Note

If the session has timed out, complete the initial steps to the point of clicking Setup.

- 2. Click Continue to Next Step.
- 3. Set the ACS URL to the DocuSign Service Provider Assertion Consumer Service URL value.
- 4. Set the Entity ID to the DocuSign Service Provider Issuer URL value.

2. Connection Configuration	
Assist the attribute values for single single	and (SSO) to the explication
Assign the attribute values for single sig	n-on (SSO) to the application.
Upload Metadata	Select File Or use URL
400.00	[
ACS URL	https://account.docusign.com/organizal
	Replace the parameter(s) '\${customer-organization-ID-goes-here}' above with your configuration information.
Entity ID	https://account.docusion.com/organizat
Enary ID	Reps.naccount.docusign.comorganiza
	reprace the parameter(s) s(customer-organization-iD-goes-here) above with your configuration information.

## (i) Note

Do not just update the organization ID.

## 5. Click Continue to Next Step.

6. Map the required attributes to the corresponding attribute names in your environment.

# (i) Note

The corresponding attribute names might not be an exact match.

#### 3. Attribute Mapping

Map your identity bridge attributes to the attributes required by the application.

	Application Attribute	Description	Identity Bridge Attribute or Literal Value
	SAME SUBJECT	Man your username attribute (For	SAML_SUBJECT
1	*	example 'mail' in AD)	As Literal
			Advanced
		Map your email attribute /For	Email (Work)
2	emailaddress *	example 'mail' in AD)	LAs Literal
			Advanced
		Man your first name attribute (For	First Name
3	givenname *	example 'givenName' in AD)	As Literal
			Advanced
		Man your last name attribute (For	Last Name
4	surname *	example 'sn' in AD)	As Literal
			Advanced
			Name or Literal
5	accountid	Map your account id attribute	As Literal
			Advanced
		Man your parmission profile id	Name or Literal
6	permissionprofileid	attribute	As Literal
			Advanced

7. On the SAML\_SUBJECT line, click Advanced, and change the name format you're sending to DocuSign to urn:oasis:names :tc:SAML:2.0:nameid-format:persistent.

#### 8. Click Continue to Next Step twice.

9. Click **Add** for all user groups that should have access to DocuSign.

5. Group Access	
Select all user groups that should have access to this application. Users that are members of the added	groups will be able to SSO to this application and wi
see uiis appirtation on their personal dock.	
Group1, Group2, etc Search	
Group Name	
Users@directory	Remove
Domain Administrators@directory	Add

#### 10. Click Continue to Next Step.

11. Click Finish.

PingOne for Enterprise configuration is complete.

## Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to your Ping desktop as a user with DocuSign access.

## (i) Note

To find the Ping desktop URL in the Admin console, go to Setup  $\rightarrow$  Dock  $\rightarrow$  PingOne Dock URL.

2. Complete the PingOne for Enterprise authentication.

You're redirected to your DocuSign domain.

DocuSign eSignature	Home	Manage	Reports					
				Last 6 Months				
	Forest	signed by: ate Your Signat 2048/203417-		O Action flequired	0 Waiting for Others	O Expiring Soon	O Completed	

## Test the PingOne for Enterprise SP-initiated SSO integration

- 1. Go to https://account.docusign.com  $\square$ .
- 2. Enter your email address.
- 3. Click Use Company Login.
- 4. When you're redirected to PingOne for Enterprise, enter your PingOne username and password.

	Ping Keetuty	
USERNAME		
PASSWORD		
	Hemember Me	
	Sign On	
	Forgot Password	

After successful authentication, you're redirected back to DocuSign.

DocuSign eSignature	Home	Manage	Reports					
		-		Last 6 Months				
		ate Your Signet	RAL.	0	0	0	0	
	- F010.			Action Required	Waiting for Others	Expiring Soon	Completed	

# Dropbox

# **Configuring SAML SSO with Dropbox and PingFederate**

Learn how to configure SAML SSO with Dropbox and PingFederate.

## **Create a PingFederate SP connection for Dropbox**

- 1. Sign on to the PingFederate administrative console.
- 2. Create an SP connection in Ping Federate:
  - 1. Set Partner's Entity ID to Dropbox.
  - 2. Configure using Browser SSO profile SAML 2.0.
  - 3. Enable the following SAML Profiles:
    - IDP-Initiated SSO
    - SP-Initiated SSO
    - IDP-Initiated SLO
    - SP-Initiated SLO
  - 4. In Assertion Creation: Attribute Contract, set the Subject Name Format to urn:oasis:names:tc:SAML: 1.1:nameid-format:emailAddress.
  - 5. In Assertion Creation: Attribute Contract Fulfilment, map attribute SAML\_SUBJECT to the attribute mail.
  - 6. In Protocol Settings, set Assertion Consumer Service URL: to https://www.dropbox.com/saml\_login and in Allowable SAML Bindings, enable Redirect.
- 3. Export the metadata for the newly-created SP connection.
- 4. Export the signing certificate public key.

Pr	PingFederate	× +							-		×
~	→ C ▲ Not secure	e   ping.localdomain:9999/pi	ngfederate/app#/spCor	nnections					ģ	θ	:
Pin	<b>g</b> Federate	A	JTHENTICATION	APPLICATIONS	SECURITY	r sys	TEM				٩
Pin ব্ য	gFederate < Integration SP Connections SP Adapters Target URL Mapping SP Default URLs Policy Contract Adapter Mappings Adapter-to- Adapter	SP Connections On this screen you can mai Connection Name   Connection Name Create Connection	ATHENTICATION age connections to yo Connection ID Dropbox Import Connection	APPLICATIONS ur partner SPs.	Search Virtual ID	Clear N Protocol SAML 2:0	iarrow By	<ul> <li>Action</li> <li>Select Action &gt;</li> </ul>	α		
	Mappings										

# Configure the PingFederate IdP connection for Dropbox

1. Sign on to the Dropbox Admin Console as an administrator.



### 2. Click Settings.

3. Click the Single sign-on section.



4. For Single sign-on, select Required.



5. In the **Identity provider sign-in URL** field, enter the **URL Location for SingleSignOnService Location** value that you retrieved from the PingFederate SP metadata that you downloaded.

😻 Settings - Dropbox 🛛 🗙	+			-		×
$\leftrightarrow$ $\rightarrow$ C $($ dropbox.com/te	am/admin/settings/sso				ф <b>Ө</b>	:
	O Your trial will end in 30 days. To keep using Dropbox Business, add billing info					-
Admin console	Settings > Single sign-on	ũ	0	 Д		
Insights Members	Identity provider sign-in URL Supplied by your identity provider. Verifies members when they enter their work credentials.					
Activity Content	Identity provider sign-out URL (optional)					
Groups Billing	be redirected to this page after they log out.					
Settings Help	X.509 certificate A.pem file security certificate supplied by your identity provider.					
	SSO sign-in URL This customized link lets members go directly to their Dropbox account online once they've signed in to your identity provider.					
	Click Save when you're done making changes. Undo Save			• Pri	ivacy	Ŧ

For example, https://PingFederate-Hostname:PingFederate-Port/idp/SSO.sam12.

- 6. Upload the PingFederate signing certificate that you downloaded.
- 7. Click Save.

## Test the PingFederate IdP-initiated SSO integration

Go to the SSO Application Endpoint value displayed in the PingFederate application configuration for the Dropbox configuration.

For example: https://PingFederate-Hostname:PingFederate-Port/idp/startSS0.ping?PartnerSpId=Dropbox





## Test the PingFederate SP-initiated SSO integration

- 1. Go to https://www.dropbox.com/login<sup>[]</sup>.
- 2. Enter your email address.

Dropbox will automatically detect that single sign-on is enabled based on the email used.

3. Click Continue.

You're redirected to PingFederate for authentication.





# Configuring SAML SSO with Dropbox and PingOne for Enterprise

Learn how to configure SAML SSO with Dropbox and PingOne for Enterprise.

## Create a PingOne for Enterprise application for Dropbox

- 1. Sign on to PingOne for Enterprise and click **Applications**.
- 2. On the SAML tab, click Add Application.

	DASHBOARD APPLICATIONS	USERS SETUP ACCOUNT	?	Sign Off
My Applications Application	Catalog PingID SDK Applications	OAuth Settings		
My Applications				
SAML OIDC				
Applications you've added to your	r account are listed here. You can search	by application name, description or	entityId	
<ul> <li>Active applications are enable</li> <li>Details displays the application</li> </ul>	ed for single sign-on (SSO). on details.			
Application Name	Type Status	Enabled		
Application Name Use the button below to add your	Type Status	Enabled		
Application Name Use the button below to add your	Type Status first application.	Enabled		
Application Name Use the button below to add your Add Application -	Type Status	Enabled	Pause All SSO	Ø
Application Name Use the button below to add your Add Application  Search Application Catalog	Type Status first application.	Enabled	Pause All SSO	Ø
Application Name Use the button below to add your Add Application  Search Application Catalog New SAML Application	Type Status	Enabled	Pause All SSO	Đ
Application Name Use the button below to add your Add Application ~ Search Application Catalog New SAML Application Request Ping Identity add a m	Type Status first application.	Enabled	Pause All SSO	e

- 3. Click Search Application Catalog and search for  $\ensuremath{\,{\rm Dropbox}}$  .
- 4. Click the **Dropbox** row.


#### 5. Click Setup.

- 6. Select the appropriate signing certificate.
- 7. Review the steps, and note the **PingOne for Enterprise SaaS ID**, **IdP ID**, **Initiate Single Sign-on (SSO) URL**, and **Issuer** values.

P	PingOne - A	Application Catalog × +				-		×
←	$\rightarrow$ G	admin.pingone.com/web-port	al/cas/applicatior	acatalog		☆	0	:
	1	Application	Name	<b>*</b> Туре				^
		Dropbox		SAML with Provisioning (API)				
		1. SSO Instructions						ł
		Signing Certificate	PingOne Acco	ount Origination Certificate (2021) V Download				
		F SaaS ID	or reference, ple	ase note the following configuration parameters:				
		IdP ID						
		Initiate Single Sign-On (SSO) URL @	https://sso.com	nect.pingidentity.com/sso/sp/initsso?saasid=				
		Issuer	https://pingone	.com/idp				
		T ",	o enable SSO at Authentication." S	Dropbox, login as a Dropbox administrator, select "Admin Console" followed select the checkbox for "Enable single sign-on" and follow the configuration s	l by steps below.			1
		Admin Console > Settings	> Single sign-on					
				Description				
		Laber						
		1 Select single	-sign on option	Select Optional to allow users to log in with SAML or their Dropbox Usern Password. To force SSO authentication select Required.	ame and			
				Enter the following URL, noting to amend \${Enter the value after 'idpid=' fi Single Sign-On (SSO) URL above} with the information from the 'idpid' pa	rom Initiate rameter in the			

- 8. Click Continue to Next Step.
- 9. Ensure ACS URLis set to https://www.dropbox.com/saml\_login and Entity ID is set to Dropbox.

P1 PingOne -	Application Catalog × +		-		×
$\leftrightarrow \rightarrow c$	admin.pingone.com/web-portal/cas/applicatio	ncatalog	\$	θ	:
	Application Name	* Type			^
	Dropbox	SAML with Provisioning (API)			
	2. Connection Configuration				
	Assign the attribute values for single sig	n-on (SSO) to the application.			
	Upload Metadata 🛛 😡	Select File Or use URL			
	ACS URL	https://www.dropbox.com/sami_login			
	Entity ID	Dropbox			
	Target Resource @				
	Single Logout Endpoint @	example.com/slo.endpoint			
	Single Logout Response Endpoint @	example.com/sloresponse.endpoint			
	Primary Verification Certificate @	Choose File No file chosen			
	Secondary Verification Certificate @	Choose File No file chosen			
	Force Re-authentication @				Ŧ

### 10. Click Continue to Next Step.

11. In the Attribute Mapping section, in the Identity Bridge Attribute or Literal Value column of the SAML\_SUBJECT row, select the attribute SAML\_SUBJECT.

_													
P	Ping	jOne -	Application	Catalog	× +						-		×
6	$\rightarrow$	C	adı adı	min.pingo	ne.com/web-portal/cas/	/applicationcatalog					☆	Θ	:
			C STOP	e vn		oourun							
					Application Name	* Туре							
			₽		Dropbox	SAML with Provis	ioning (API)						
			3. A1	ttribute M Map you	lapping r identity bridge attribu	utes to the attributes required by the appl	lication.	n Alleikuda ast Saval					l
					Application Attribute	Description	Value	e Attribute or Literal					
				1	SAML_SUBJECT *	Map this value to an attribute that matches the username defined at Dropbox. Select Advanced and ensure that "NameldFormat to send to SP is set to: urn:oasis:names.tc:SAML:1.1:nameld- format:emailAddress. Note: Dropbox names are case sensitive.	SAML_SUE As Literal Advanced	BJECT					
			N	Add ne * Indicate	w attribute is a required attribute. One App Customization - D	ropbox		Cancel Back	Continue to Next \$	Step			

## 12. Click Continue to Next Step.

13. Update the Name, Description, and Category fields as required.

P1 PingOne -	Application Catalog × +		- 0	×
← → C	admin.pingone.com/web-portal/cas/application	catalog	\$	9 :
	Dishoon	Sources -		
	Application Name	* Туре		
	😌 Dropbox	SAML with Provisioning (API)		
	4. PingOne App Customization - Dropbox			1
	lcon 6	Select image		
	Name @	Dropbox		
		•		
	Description @	Dropbox is a free service that lets you bring your photos, docs, and videos anywhere and share them easily. Never email yourself a file again.		
	Category @	Information Systems		1
	NEXT: Group Access	Cancel Back Continue to Next Step		

## 14. Click Continue to Next Step.

- 15. Add suitable user groups for the application.
- 16. Click Continue to Next Step.

P	Ping	One - A	pplication	Catalog X +		-		×
÷	$\rightarrow$	G	🗎 adr	in.pingone.com/web-portal/cas/applicationcatalog		☆	Θ	:
				Application Name	* Туре			
			₽	Dropbox	SAML with Provisioning (API)			
			5. Gr	oup Access select all user groups that should have access to this applicat ee this application on their personal dock.	ion. Users that are members of the added groups will be able to SSO to this applicati	on and v	лШ	
				Group1, Group2, etc Search				
				Group Name				
				Domain Administrators@directory	Ren	nove		
				Users@directory	Ren	nove		
			N	XT: Review Setup	Continue to	Next Ste	р	Ŧ

17. Review the settings.

P1 PingOne -	Application Catalog × +		-			×
← → C	admin.pingone.com/web-portal/cas/applicationca	atalog	ź	â	θ	:
	Application Name	* Туре				
	Dropbox	SAML with Provisioning (API)				
						ł
	6. Review Setup					
	Test your connection to the application					
	Icon @					
		<b>₩</b>				l
	Name @	Dropbox				
	Description @	Dropbox is a free service that lets you bring your photos, docs, and videos anywhere and share them easily. Never email yourself a file again.				
	Category @	Information Systems				
	Connection ID					
	You may need to configure these connect	ction parameters as well.				
	saasid					
	idpid					
	Issuer					-
P1 PingOne -	Application Catalog × +		-		1	×
← → C	admin.pingone.com/web-portal/cas/applicationca	atalog	ž	\$	0	:
	Single Sign-On (SSO) Relay State @	https://pingone.com/1.0/				
	Single Logout Endpoint					
	Single Logout Response Endpoint					
	Force Re-authentication @	false				
	Signing Certificate	Download				
	SAML Metadata	Download	_			
	SAML Metadata URL	https://admin-api.pingone.com/latest/metadata/				
	Application Attribute	Identity Bridge       Description     Attribute or       Literal Value				
	1 SAML_SUBJECT *	Map this value to an attribute that matches the username defined at       Image: Compose of the second				1
	* Indicates a required attribute.					
		Back Finist	1			

18. Copy the Single Sign-On (SSO) URL value to a temporary location.

This is the IdP-initiated SSO URL that you can use for testing.

- 19. On the Signing Certificate row, click Download You will use this for the Dropbox configuration.
- 20. On the **SAML Metadata** row, click **Download**. You will use this for the Dropbox configuration.
- 21. Click Finish.

### Configure a PingOne for Enterprise IdP connection for Dropbox

1. Sign on to the Dropbox Admin Console as an administrator.

😻 Home - Dropbox 🛛 🗙	+		- 🗆 X
$\leftrightarrow$ $\rightarrow$ $C$ $\triangleq$ dropbox.com/h			☆ 🖰 :
	O Your trial will end in 30 days. To keep using Dropbox Busin	ness, add billing info	
•	Home	Q Search	0 III 4
Home	Suggested from your activity 🕡	Hide	
All files			Create new file ~
Shared	PDF		• Upload files
File requests	Get Started w		Dpload folder
Deleted files	Dropbox.pdf		🗅 New folder
Deleted files	-		New shared folder
	Recent	Hide	
Admin console	Get Started with Dropbox Paper.url Added 19 hours ago		
	Get Started with Dropbox.pdf Added 19 hours ago		
	Starred	Hide	
	When you star items, they'll show up here for easy access. Le	earn more	
			••• Privacy

### 2. Click Settings.

3. Click the Single sign-on section.



4. For Single sign-on, select Required.



5. In the **Identity provider sign-in URL** field, enter the **URL Location for SingleSignOnService Location** value that you retrieved from the PingOne for Enterprise SP metadata that you downloaded.

For example, https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=idpid

😻 Settings - Dropbox 🛛 🗙 🚽	•				-		×
← → C 🔒 dropbox.com/team/a	admin/settings/sso					☆ <b>8</b>	:
	O Your trial will end in 30 days. To keep using D	ropbox Business, add billing info					•
Admin console	Settings > Single sign-on		C	0	 Д		
Insights	Identity provider sign-in LIRI						
Members	Supplied by your identity provider. Verifies	Sign-in URL: https://sso.connect.pi	1				
Activity	members when they enter their work credentials.						
Content							
Groups	Identity provider sign-out URL (optional) Supplied by your identity provider. Members will	Add sign-out URL					
Billing	be redirected to this page after they log out.	<u></u>					
Settings							
Help	X.509 certificate A .pem file security certificate supplied by your identity provider.	Certificate: pingone-signing.crt					
	SSO sign-in URL This customized link lets members go directly to their Dropbox account online once they've signed in to your identity provider.	<u>Copy link</u>					
	Click Save when you're done making changes.	Undo			 • Pri	vacy	-

- 6. Upload the PingOne for Enterprise signing certificate that you downloaded.
- 7. Click Save.

## Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to the Single Sign-On (SSO) URL in the PingOne for Enterprise Application configuration to perform IdP-initiated SSO.

https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=saasid&idpid=idpid



## Test the PingOne for Enterprise SP-initiated SSO integration configuration

- 1. Go to https://www.dropbox.com/login<sup>[]</sup>.
- 2. Enter your email address.

Dropbox automatically detects that single sign-on is enabled based on the email used.

3. Click Continue.

You're redirected to PingOne for Enterprise for authentication.

😲 Login - Dropbox 🛛 🗙 🕂		- o x
← → C 🔒 dropbox.com/login		🕶 🗞 ☆ 😞 Incognito 🗄
Try Dropbox Business		Download the app
	Sign in	or create an account
	<b>G</b> Sign in	with Google
A CONC	🔹 Sign in	with Apple
		or
ST.	Single s	ign-on enabled
	Remember me	
e l'	Co	ntinue
	or Log in with i	Dropbox credentials



# Egnyte

# Configuring SAML SSO with Egnyte and PingFederate

Learn how to enable Egnyte sign-on from a PingFederate URL (IdP-initiated sign-on) and direct Egnyte sign-on using PingFederate (SP-initiated sign-on).

### Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users requiring application access.
- Populate Egnyte with at least one user to test access.
- You must have administrative access to PingFederate and Egnyte.

### Create an SP connection for Egnyte

- 1. Sign on to the PingFederate administrative console.
- 2. Create an SP connection for Egnyte in PingFederate.
  - 1. Configure using Browser SSO profile SAML 2.0.
  - 2. Set Partner's Entity ID to https://saml-auth.egnyte.com.
  - 3. Enable the following SAML Profiles:
    - IdP-Initiated SSO
    - SP-Initiated SSO
  - 4. In Assertion Creation → Authentication Source Mapping → Attribute Contract Fulfillment, map the SAML\_SUBJECT to the attribute containing the user's email address.
  - 5. In Protocol Settings → Assertion Consumer Service URL, set Binding to POST and set Endpoint URL to https:// your-Egnyte-domain.egnyte.com/samlconsumer/PingFederate.
  - 6. In Protocol Settings → Allowable SAML Bindings, enable POST.
  - 7. In Credentials → Digital Signature Settings, select the PingFederate Signing Certificate.
- 3. Save the configuration.
- 4. Export the signing certificate.
- 5. Export and then open the metadata file and copy the value of the entityID and the Location entry (https://your-value/ idp/SS0.saml2).

### Add the PingFederate connection to Egnyte

- 1. Sign on to your Egnyte Admin organization as an administrator.
- 2. Click the menu icon and then click Settings.



3. Click the Security and Authentication tab.



- 4. In the Single sign-on authentication list, select SAML 2.0.
- 5. In the Identity provider list, select Ping Identity.
- 6. Set the following values:

Field	Value
Identity provider login URL	The Location value from the metadata that you exported.
Identity provider entity ID	The entityID value from the metadata that you exported.
Identity provider certificate	In a text editor, open the signing certificate that you downloaded in a text editor. Copy and paste the contents.
Default user mapping	Email address

7. Click Save.

### 8. Go to Settings $\rightarrow$ Users and Groups.

9. Select the appropriate users and set their **AuthType** to **SSO**.

### Test the PingFederate IdP-initiated SSO integration

- 1. Go to the PingFederate SSO Application Endpoint for the Egnyte SP connection.
- 2. Complete the PingFederate authentication.

You're redirected to your Egnyte domain.

### **Test the PingFederate SP-Initiated SSO integration**

- 1. Go to https://your-Egnyte-domain.Egnyte.com.
- 2. Select the PingFederate sign-on option.
- 3. After you're redirected to PingFederate, enter your PingFederate username and password.

You're redirected back to Egnyte.

# Configuring SAML SSO with Egnyte and PingOne for Enterprise

Learn how to enable Egnyte sign-on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct Egnyte sign-on using PingOne for Enterprise (SP-initiated sign-on).

#### Before you begin

- · Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Populate Egnyte with at least one user to test access.
- You must have administrative access to PingOne for Enterprise and Egnyte.

### Update the supplied Egnyte application in PingOne for Enterprise

- 1. Sign on to PingOne for Enterprise and go to Applications → Application Catalog.
- 2. Search for Egnyte.

Application	n Catalog		Applications / Application Catalog
Browse for the app	olication you want to add or search :	r it by name. Don't see the application ;	rou're looking for? Fill out our Application Request Form.
egnyte		Search	
	Application Name	* Туре	
*	Egnyte	SAML with Provisio	ning (API)

- 3. Expand the Egnyte entry and click the Setup icon.
- 4. Copy the Issuer and IdP ID values.

5. Download the signing certificate.



- 6. Click Continue to Next Step.
- 7. Set ACS URL to https://Your-Egnyte-domain.egnyte.com/samlconsumer/PingIdentity.
- 8. Click Continue to Next Step twice.
- 9. In the Attribute Mapping section, map SAML\_SUBJECT to the attribute containing the user's email address.
- 10. Click Continue to Next Step twice.
- 11. Click **Add** for all user groups that should have access to Egnyte.

ee this application on their personal do	ж.	
Group1, Group2, etc	Search	
Group Name		
Users@directory		Remov
Domain Administrators@directory		Add

- 12. Click Continue to Next Step.
- 13. Click Finish.

# Add the PingOne for Enterprise IdP connection to Egnyte

1. Sign on to your Egnyte Admin organization as an administrator.

2. Click the menu icon and then click **Settings.** 



3. Click the Security and Authentication tab.



4. In the Single sign-on authentication list, select SAML 2.0.

#### 5. In the Identity provider list, select Ping Identity.

6. Set the following values:

Field	Value
Identity provider login URL	<pre>https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=IdP- ID-value</pre>
Identity provider entity ID	The <b>Issuer</b> value from above.
Identity provider certificate	In a text editor, open the signing certificate that you downloaded. Copy and paste the contents.
Default user mapping	Email address

- 7. Click Save.
- 8. Go to Settings  $\rightarrow$  Users and Groups.
- 9. Select the appropriate users and set their **AuthType** to **SSO**.

### Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to our Ping desktop as a user with Egnyte access.

# (i) Note

To find the Ping desktop URL in the Admin console, go to **Setup**  $\rightarrow$  **Dock**  $\rightarrow$  **Dock URL**.

2. Complete the PingOne for Enterprise authentication.

You're redirected to your Egnyte domain.

	Ping Keetity Sign On	
USERNAME		
PASSWORD		
	Remember Me	
	Sign On	
	Forgot Password	

## Test the PingOne for Enterprise SP-initiated SSO integration

- 1. Go to https://Your-Egnyte-domain.Egnyte.com.
- 2. Select the PingOne for Enterprise sign-on option.
- 3. After you're redirected to PingOne for Enterprise, enter your PingOne for Enterprise username and password.

	Ping Keetity Sign On	
USERNAME		
PASSWORD		
	Remember Me	
	Sign On	
	Forgot Password	

You're redirected back to Egnyte.

# **Evernote**

# **Configuring SAML SSO with Evernote and PingFederate**

Learn how to enable Evernote sign on from a PingFederate URL (IdP-initiated sign-on) and direct Evernote sign on using PingFederate (SP-initiated sign-on).

### Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users requiring application access.
- Populate Evernote with at least one user to test access.
- You must have administrative access to PingFederate and Evernote.

### **Create a PingFederate SP connection for Evernote**

- 1. Sign on to the PingFederate administrative console.
- 2. Create an SP connection for Evernote in PingFederate:
  - 1. Configure using Browser SSO profile SAML 2.0.
  - 2. Set Partner's Entity ID to https://www.evernote.com/sam12.
  - 3. Enable the following SAML Profiles:
    - IdP-Initiated SSO
    - SP-Initiated SSO
  - 4. In Assertion Creation → Authentication Source Mapping → Attribute Contract Fulfillment, map SAML\_SUBJECT.
  - 5. In Protocol Settings → Assertion Consumer Service URL, set Binding to POST and set Endpoint URL to https:// www.evernote.com/SamlConsumer.action.
  - 6. In Protocol Settings → Allowable SAML Bindings, enable POST.
  - 7. In Credentials → Digital Signature Settings, select the PingFederate Signing Certificate.
- 3. Save the configuration.
- 4. Export the signing certificate.
- 5. Export the metadata, open the metadata file in a text editor, and copy the value of the Location entry (https://your-value/idp/SS0.saml2).

### Add the PingFederate connection to Evernote

- 1. Sign on to your Evernote Admin organization as an administrator and go to the Evernote Business Admin Console.
- 2. Go to Security  $\rightarrow$  Single Sign-On.
- Set SAML HTTP Request URL to the Location value from the metadata file that you downloaded previously (https:// your-value/idp/SS0.saml2).
- 4. In a text editor, open your PingFederate signing certificate file, copy the contents, and paste your signing certificate contents into the **X.509 Certificate** field.
- 5. Click Save & Enable.

### Test the PingFederate IdP-initiated SSO integration

- 1. Go to the PingFederate SSO Application Endpoint for the Evernote SP connection.
- 2. Complete the PingFederate authentication.

You're redirected to your Evernote domain.

### **Test the PingFederate SP-initiated SSO integration**

- 1. Go to your Evernote URL.
- 2. Select the PingFederate sign-on option.
- 3. After you're redirected to PingFederate, enter your PingFederate username and password.

You're redirected back to Evernote.

# Configuring SAML SSO with Evernote and PingOne for Enterprise

Learn how to enable Evernote sign on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct Evernote sign on using PingOne for Enterprise (SP-initiated sign-on).

#### Before you begin

- · Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Populate Evernote with at least one user to test access.
- You must have administrative access to PingOne for Enterprise and Evernote.

### Update the Evernote application in PingOne for Enterprise

- 1. Sign on to PingOne for Enterprise and go to Applications  $\rightarrow$  Application Catalog.
- 2. Search for Evernote.

Application Catalog	/ Applications /	ation Catalog
Browse for the application you want to add or search f	or it by name. Don't see the application you're looking for? Fill out our Application Request Form.	
Evernote	Search	

Арр	lication Name *	Туре	
Ev	remote	SAML with Provisioning (API)	▶

- 3. Expand the Evernote entry and click the **Setup** icon.
- 4. Copy the IdP ID value.

You will need this wherever you see <code>IdP-ID-value</code> in the next procedure.

5. Download the signing certificate.

1. SSO Instructions	
Signing Certificate	PingOne Account Origination Certificate (2021) V
For	reference, please note the following configuration parameters:
SaaS ID	
IdP ID	
Initiate Single Sign-On (SSO) URL o	
Issuer	

- 6. Click Continue to Next Step twice.
- 7. In the Attribute Mapping section, map SAML\_SUBJECT to the attribute containing the user's email address.

Attribute	Mapping			
Map yo	our identity bridge attrib	utes to the attributes required by the app	lication.	
	Application Attribute	Description	Identity Bridge Attribute or Literal Value	
1	SAML_SUBJECT *	must contain the user's email address, which must match the Evernote user's business email address. Assertions must contain a NameID with a Format of urn:oasis:names:tc:SAML:1.1:nameid- format:emailAddress	Email (Work) As Literal Advanced	

- 8. Click Advanced.
- 9. In the Name ID format to send to SP field, enter urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress.



- 10. Click Save, then click Continue to Next Step twice.
- 11. Click **Add** for all user groups that should have access to Evernote.

5. G	iroup Access	
	Select all user groups that should have access to this application. Users that are members of the added groups will be able to SSO to see this application on their personal dock.	this application and will
	Group1, Group2, etc Search	
	Group Name	
	Users@directory	Remove
	Domain Administrators@directory	Add

- 12. Click Continue to Next Step.
- 13. Click Finish.

# Add the PingOne for Enterprise IdP connection to Evernote

- 1. Sign on to your Evernote Admin organization as an administrator and go to the Evernote Business Admin Console.
- 2. Go to Security  $\rightarrow$  Single Sign-On.
- 3. Set SAML HTTP Request URL to https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=IdP-ID-value.
- 4. In a text editor, open your PingOne for Enterprise signing certificate.
- 5. Copy and paste your signing certificate contents into the X.509 Certificate field.
- 6. Click Save & Enable.

### Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to your Ping desktop as a user with Evernote access.

# (i) Note

To find the Ping desktop URL in the Admin console, go to Setup  $\rightarrow$  Dock  $\rightarrow$  Dock URL.

2. Complete the PingOne for Enterprise authentication.

	<b>Ping</b> Keetaty	
USERNAME		
PASSWORD		
	Hemember Me	
	Sign On	
	Forgot Password	

You're redirected to your Evernote domain.

# Test the PingOne for Enterprise SP-initiated SSO integration

- 1. Go to your Evernote URL.
- 2. Select the PingOne for Enterprise sign on option.
- 3. After you're redirected to PingOne for Enterprise, enter your PingOne for Enterprise username and password.

	Ping Sign On	
USERNAME		
PASSWORD		
	Hemember Me	
	Sign On	
	Forgot Password	

You're redirected back to Evernote.

# **Freshworks**

# Configuring SAML SSO with Freshworks and PingOne

Learn how to configure SAML single sign-on (SSO) with Freshworks and PingOne.

### Before you begin

You must have a Business level or higher plan in Freshworks. Learn more at https://support.freshworks.com/support/solutions/articles/237923<sup>[2]</sup>.

# **Configure SSO in Freshworks**

1. Sign on to your Freshworks Admin account homepage and go to the **Security** tab.

1	Neo Admin Center
$\odot$	
ß	
	Upload Organization logo
D D	Security Organization URL
मुद्य	ORGANIZATION-ADMIN Edit Profile Edit Organization Information
53	
	My Accounts All the accounts in this organization that you have access to. Click to open.  Ping Identity newaccount162991freshdesk.com
	Explore Freshworks Products
	Our products help your teams deliver the best customer experiences
	6 6 6 6 6 6 6 6 6
	Freshdesk Freshsales Freshsales Freshsales Freshmarketer Freshdesk Freshdesk Freshservice Freshteam Freshping Freshstatus Omnichannel Support Desk Suite Contact Messaging Center

2. On the Security Settings page, in the Default Login Methods section, click the right arrow.

ow your agents, admins, and employees are authenticated into their accounts. Also, co	nfigure other security settings here.			
gning in to Freshworks nfigure the different methods through which your users can sign in to their Freshworks	account.			
Default Login Methods Configure default login methods to be applied to all accounts in the organization.	⊘ Freshworks Login	⊘ Google Login	🛞 SSO Login	>
Custom Policies Configure custom policies for one or more of your accounts. For these accounts, default login methods will not apply.	None			>

3. On the corresponding Login Methods page, click the SSO Login toggle.

ult Login Method © Help default login methods to be applied to all accounts in the organization. At least one login method needs to be enabled.		
Accounts and Porta	als nization, except for which custom policy is created, will have default login methods enabled. Show Accounts	
Login Methods		
Freshworks Logi Users can use their	in remail ID and password to create and log into their Freshworks account.	
Password Policy Low	2FA Policy Not mandated	
G Google Login Users can login into	o their Freshworks account via their Google credentials.	
SSO Login Configure SAML/ Or	Auth/OIDC/JWT SSO with the identity provider of your choice.	

The **Configure SSO** panel opens.

4. On the Configure SSO panel, in the IdP of your choice section, click SAML.

X

OneLogin usi	ng SAML		
Use OneLogin a	and enable SAML SSO fo	or your users	
Okta using SA	AML		
Use Okta and e	nable SAML SSO for you	ur users	
Azure AD usir	ng SAML		
Use Azure AD a	and enable SAML SSO fo	or your users	
ADFS using S	SAML		
Use ADFS and e	enable SAML SSO for yo	our users	
Shibboleth us	sing SAML		
Use Shibboleth	and enable SAML SSO	for your users	
IdP of your ch	hoice		
Choose the IdP proceed to conf	of your choice and any figure the SSO settings.	of the following logi	n protocols to

5. On the Set up SSO with SAML page, in the Map information in IdP section, make a note of the Assertion Consumer Services (ACS) URL and Service Provider (SP) Entity ID values. You will need them later.

Click Download Metadata.



### **Configure SSO in PingOne**

- 1. In PingOne, go to **Connections**  $\rightarrow$  **Applications**.
- 2. Click the + icon next to **Applications**.



# Important

You will use the settings displayed in Step 5 of the previous procedure to begin configuring Freshworks within PingOne.

- 3. On the **New Application** page, click **Advanced Configuration**.
- 4. In the **Choose Connection Type** list, on the **SAML** line, click **Configure**.

LECT AN APPLICATION TYPE				1
Web applications that are accessed within a browser.	Applications that are stored and run from a device or desktop.	A front-end application that uses an API.	Management API integrations that can perform actions using Roles.	Apps configured by advanced users fir the ground up.
• .NET web apps • Java apps WEB APP	- IOS and Android apps - Deaktop apps - Push Authentication NATIVE APP	Angular     Node.js SINGLE PAGE APP	Non-interactive service integrations     Client Credentials w/Role Assignment     Interactive admin consoles & portals     WORKER	Your choice     No barriers     Complete flexibility  ADVANCED CONFIGURATION
	CHOOSE CO	INNECTION TYPE		
	SAML Apps the	t utilize an Identity Provider (IDP) to authenticate users a	nd provides Service Providers an Authentication Assertion	Configure
	OIDC	Universal Login and redirect users to the login page		Configure

- 5. In **Create App Profile**, enter the values for:
  - Application Name (Required)
  - Description (Optional)
  - Icon (Optional)

Per	sonalize your application by creating a unique profile. The descriptio
	APPLICATION NAME
	Freshworks
	DESCRIPTION
	Freshworks SSO Integration
	ICON
	freshworks
	Remove Image

6. On the Configure SAML Connection page, in the Provide App Metadata section, click Import Metadata.

Upload the metadata downloaded previously and click Import.

Configure SAML Connection	
SAML is an authentication protocol that acts as a service provider (SP) to PingOne (the identity provide	r, or IdP).
PROVIDE APP METADATA	
Import Metadata Import From URL Manually Enter	
Choose File	

After import, all necessary fields are populated automatically, except for the Assertion Validity Duration.

- 7. In the **Assertion Validity Duration** field, enter a valid duration value (in seconds), such as 3600.
- 8. In the Signing Key section, select Download Signing Certificate and download in the X509 PEM (.crt) format.

Make sure that Sign Assertion & Response is selected, then click Save and Continue.

Tingone 500 certificate f	or Administrators en	vironme Y
Download Signing Certific	ate	_
Select format	Sign Response	Sign Assertion & Response
GN X509 PEM (.crt)		

- 9. On the **Attribute Mapping** page, enter the values for the following attributes:
  - Email Address = saml\_subject
  - givenName
  - LastName
  - mobile
  - phone

PPLICATION ATTRIBUTE		OUTGOING VALUE			
saml_subject	←	Email Address	~	<ul> <li>Required</li> </ul>	
			Advanced Expression		
GivenName	←	Given Name	~	Required	
			Advanced Expression		
Lastname	←	Family Name	~	Required	
			Advanced Expression		
mobile	←	Mobile Phone	~	Required	
			Advanced Expression		
phone	←	Primary Phone	~	Required	
		\$7	Advanced Expression		

- 10. Click **Save and Close** to finalize the creation of the application.
- 11. After you create the application, click the toggle next to the application to enable it.

freshworks Client ID:		<b>(</b> ) : ×
Profile Configurati	ion Attribute Mappings Policies Access	
		1
APP TYPE:	Advanced Configuration (SAML)	
DESCRIPTION:	Freshworks SSO Integration	
CLIENT ID:		
HOME PAGE URL:	No Home Page Configured	
SIGNON URL:	Default Signon Page	

- 12. Select **Configuration** and copy the following values for later use.
  - Issuer ID
  - Single Logout Service (Optional)
  - Single SignOn Service

works Client ID:		$\bigcirc$ : >
rofile Configuration Att	Attribute Mappings Policies Access	
		/
CONNECTION DETAILS		
DOWNLOAD METADATA :	Download	
ISSUER ID :	https://auth.pingone.com/f	
ISSUER ID : SINGLE LOGOUT SERVICE :	https://auth.pingone.com/f https://auth.pingone.com/f	
ISSUER ID : SINGLE LOGOUT SERVICE : SINGLE SIGNON SERVICE :	https://auth.pingone.com/f https://auth.pingone.com/f https://auth.pingone.com/f	
ISSUER ID : SINGLE LOGOUT SERVICE : SINGLE SIGNON SERVICE : IDP METADATA URL :	https://auth.pingone.com/f https://auth.pingone.com/f https://auth.pingone.com/f https://auth.pingone.com/f https://auth.pingone.com/f	

### Integrate SAML SSO with Freshworks and PingOne

1. In Freshworks, go to **Set up SSO with SAML** and paste the information from the previous step into the below locations:

- Entity ID provided by the IdP = the Issuer ID value from PingOne
- SAML SSO URL = the Single SignOn Service value from PingOne
- Logout URL = the Single Logout Service value from PingOne (Optional)

Get the following information from your Identity Provide to the relevant fields below	er and map them
Entity ID provided by the IdP*	
https://auth.pingone.com/fd65de53-8841-4006-b	907-8f4f87b6
SAML SSO URL*	
https://auth.pingone.com/fd65de53-8841-4006-b	907-8f4f87b6
Signing Options*	
Only Signed Response	~
Logout URL	
https://auth.pingone.com/fd65de53-8841-4006-t	907-8f4f87b6

2. Upload the X509 certificate that you downloaded previously. Open the downloaded file with a text editor and copy and paste the certificate into the **Security certificate** field, then select **Configure SSO**.

# (i) Note

You must include the **BEGIN CERTIFICATE** and **END CERTIFICATE** text as part of the certificate upload.

oQ8/RFUnyUm8EjiOQWFGif1oB 5MCS3CspsI+77QsIR	WBDCSd1T1HFXWF	/21iv1TG
3vD4kJgPkbcsv0rrrb2		
END CERTIFICATE	UB6LamP90FCddF	1
	(	and and and and

3. Sign out of your Freshworks account, then click the **Sign in with SSO** to sign on.
You're proxied into your account, finalizing the configuration.

- 100 10	
Email	
Password	
Keep me logged in	Forgot Password?
	anna an
Siç	in in
c	)R
G Sign in v	vith Google
Sign in	with SSO

## Create and assign identities in PingOne

Before you can test the integration, create and assign identities in PingOne. If you've already assigned identities and groups in PingOne, move on to Test the integration.

1. In PingOne, go to **Identities**  $\rightarrow$  **Groups** and click the + icon next to **Groups**.

P	ingldentity.	
Enviro Admir Produc	nments nistrators ~ vtion	
۲	< Identities	Q Search Groups
::	Users	Name
*	Groups	Apps Administrators Population
L.	Populations	
0	Attributes	Admin
	Roles	
@ 		
Ø		

- 2. On the **Create New Group** page, enter values for the following:
  - Group Name (Required)
  - Description (Optional)
  - Population (Optional)
- 3. Click Finish & Save.

Groups 🚭 Administrators can manage their groups including creating groups, updating group membership manually or dynamically and more. Learn Q. Search Groups	X Create New Group Groups provide application access for users.
Name Apps Administrators Population	Enter Profile Data Group Name
👥 Admin	Description
	Population Administrators Population Finish & Save

4. To add identities to the group, on the **Identities** tab, go to **Users**  $\rightarrow$  + Add User.

Pi	ngidentity.			⑦ • ⑤ Explore • Le Ryan Schafer
Environi Admini: Producti	ments strators ~	Users		
⊕	< Identities	Q Search or SCIM Query	Filters 🗸	+ Add User
	Users		Example SCIM Queries	
*	Groups	4 users by Family Name ~		
8	Populations			
1	Attributes			
C	Roles			
•		Test, Adam adamtest		
•				
		Test, Joe joetest		

5. On the **Add User** page, enter all the necessary information for a user.

## i) Important

Verify that the first name, last name, and email address are correct, as these are values passed in the SAML assertion.

#### 6. Click Save.

7. Assign the user that you created to the group that you created previously.

Locate the user you created and do the following:

- 1. Expand the section for the user.
- 2. Select the **Groups** tab.
- 3. Click + Add.

est, Adam amtest								Reset Password	•
Profile Group Meml	Roles	Authentication	Groups	Consent	API	Sync Status	Credentials		
Apps									

8. In the Available Groups section, select the group that you created and click the + icon to add it to the user's group memberships. Click Save.

< Back to Users Adam Test		
Profile Roles Authentication Groups		
① Groups define a collection of users using membership or by dynamic filtering criteria. Groups can be used to assign application access to	to users.	
Q Search Available Groups		
AVAILABLE GROUPS	GROUP MEMBERSHIPS	
ii Admin	+ Apps Administrators Population	Э

- 9. On the **Connections** tab for the Freshworks application do the following:
  - 1. Click the **Access** tab.
  - 2. Click the **Pencil** icon to edit the configuration.

Profile         Configuration         Attribute Mappings         Policies         Access           GROUP MEMBERSHIP POLICY         No Restrictions         Volume         Volume	ionia.	Freshwo Client ID: c	rks 814a0bb-5932-420a-9c	e0-c400e06706e0				Avg daily sign-ons:
GROUP MEMBERSHIP POLICY No Restrictions		Profile	Configuration	Attribute Mappings	Policies	Access		
	GF	OUP MI	MBERSHIP POLICY Restrictions					

10. Select the group that you created and add it to the **Applied Groups** section. Click **Save**.

< To Application	n List shworks ID: c							
Profile	Configuration	Attribute Mappings	Policies	Access				
Admin Only A Must hav Group Membe	Admin Only Access Must have admin role Group Membership Policy							
Groups can be The following s	added to control user elections determine g	access to the application. A roups that have access to t	All users have an he application.	ccess when no g	are listed.			
Q Search G	roups							
ALL GROUPS						APPLIED GROUPS		
ii Admin					(+)		Add access control for groups by dragging them here	
H Apps Adminis	trators Population				(+)	]		

## Test the integration

You're now ready to test the integration.

- 1. In the PingOne admin console, go to **Dashboard**  $\rightarrow$  **Environment Properties**.
- 2. Right-click on the **Application Portal URL** and open it in a private browser session.



3. Sign on as the test user that you created and click the Freshworks tile.

You're signed on to the user's Freshworks account using SSO and testing is complete.

			in deriver (
ALL APPLICATIONS			
Aha! 🔛 restructs Control Cont	PagerDuty	र quickbase	<b>√</b> wrike
Aha Labs Datadog Freshworks Heap Litmos Outsystems Test	PagerDuty	QuickBase	Wrike

# GitHub

## Configuring SAML SSO with GitHub Cloud and PingFederate

Learn how to enable GitHub sign-on from a PingFederate URL (IdP-initiated sign-on) and direct GitHub sign on using PingFederate (SP-initiated sign-on).

## Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users requiring application access.
- Populate GitHub with at least one user to test access.
- You must have administrative access to PingFederate and GitHub.

## **Create a PingFederate SP connection for GitHub**

- 1. Sign on to the PingFederate administrative console.
- 2. Create an SP connection for GitHub in Ping Federate UI:
  - 1. Configure using Browser SSO profile SAML 2.0.
  - 2. Set Partner's Entity ID to https://github.com/orgs/your-tenant.
  - 3. Enable the following SAML Profiles:
    - IdP-Initiated SSO
    - SP-Initiated SSO
  - 4. In Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfillment, map SAML\_SUBJECT to an attribute containing the user's email address.
  - 5. In Protocol Settings: Assertion Consumer Service URL, set Binding to POST and set Endpoint URL to https://github.com/orgs/your-tenant/saml/consume.
  - 6. In Protocol Settings: Allowable SAML Bindings, enable POST.
  - 7. In Credentials: Digital Signature Settings, select the PingFederate Signing Certificate.
- 3. Save the configuration.
- 4. Export the signing certificate.
- 5. Export and then open the metadata file.

Copy the value of the entityID and the Location entry ( https://your-value/idp/SS0.saml2 ).

## Add the PingFederate IdP connection to GitHub

- 1. Sign on to GitHub as an administrator.
- 2. Select your GitHub organization.
- 3. Click Organization settings, then click Security.
- 4. Under SAML single sign-on, select Enable SAML authentication.

í	Note
	The assertion consumer service URL displayed on this screen should match the value that you entered into the
	PingFederate <b>Endpoint URL</b> field.

Enable Identit	s SAME authentication SAML authentication for your organization through an identity provider like Azure, Okta, Onelogin, Ping y or your custom SAML 2.0 provider.
0	Save your recovery codes in a safe place. If your IdP is unavailable you can use a recovery code to skip single sign-on and access the SAML SSO Org organization.
S	The SAML SSO Org organization single sign-on URL is https://github.com/orgs/same sign-on URL is https://github.com/orgs/same sign-on URL is https://github.com/orgs/same sign-on urg/same
S	The assertion consumer service URL is https://github.com/orgs/s/saml/consume. Configure your identity provider to send authenticated users to this URL.
Sign o	
Memb	ers will be forwarded here when signing in to your organization
Issuer	
http:	s://example.com
Typica Public	Ily a unique URL generated by your SAML Identity Provider
	certificate

5. Set the following values.

Field	Value
Sign on URL	The PingFederate Location value ( https://your-value/idp/SSO.saml2 )
Issuer	The PingFederate entityID value.

Field	Value
Public certificate	Paste in the contents of the PingFederate signing certificate.

6. Click Save.

## Test the PingFederate IdP-initiated SSO integration

- 1. Go to the PingFederate SSO Application Endpoint for the GitHub SP connection.
- 2. Complete the PingFederate authentication.

You're redirected to your GitHub domain.

## Test the PingFederate SP-initiated SSO integration

- 1. Go to https://github.com/orgs/your-tenant/sso
- 2. After you're redirected to PingFederate, enter your PingFederate username and password.

You're redirected back to GitHub.

## Configuring SAML SSO with GitHub Cloud and PingOne for Enterprise

Learn how to enable GitHub sign-on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct GitHub sign-on using PingOne for Enterprise (SP-initiated sign-on).

## Before you begin

- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Populate GitHub with at least one user to test access.
- You must have administrative access to PingOne for Enterprise and GitHub.

## Set up the supplied GitHub application in PingOne for Enterprise

- 1. Sign on to PingOne for Enterprise for and go to **Applications**  $\rightarrow$  **Application Catalog**.
- 2. Search for GitHub.
- 3. Expand the GitHub entry and click the **Setup** icon.

Application	Catalog		Applications / Application Catalog
Browse for the applic	ation you want to add or search fo	or it by name. Don't see the application you're	looking for? Fill out our Application Request Form.
github		Search	
	Application Name	^ Туре	
<b>O</b>	GitHub.com	SAML with Provisioning	(API)

#### 4. Copy the Issuer and IdP ID values.

5. Download the signing certificate.

1. SSO Instructions	
Signing Certificate	PingOne Account Origination Certificate (2021) V
Fo	r reference, please note the following configuration parameters:
SaaS ID	
IdP ID	
Initiate Single Sign-On (SSO) URL @	n i i in i in i in i na sa waata waa
Issuer	

## 6. Click Continue to Next Step.

7. Set ACS URL to https://github.com/orgs/your-tenant/saml/consume.

Set Entity ID to https://github.com/orgs/your-tenant.

- 8. Click Continue to Next Step.
- 9. Ensure that **SAML\_SUBJECT** is mapped to the field containing a user's email address.
- 10. Click Continue to Next Step twice.
- 11. Click **Add** for all user groups that should have access to GitHub.

5. Group Access		
Select all user groups that should have access to the see this application on their personal dock.	is application. Users that are members of the added groups will be at	ble to SSO to this application and will
Group1, Group2, etc	Search	
Group Name		
Users@directory		Remove
Domain Administrators@directory		Add

#### 12. Click Continue to Next Step.

13. Click Finish.

## Add the PingOne for Enterprise IdP connection to GitHub

- 1. Sign on to GitHub as an administrator.
- 2. Select your GitHub organization.
- 3. Click Organization settings, then click Security.
- 4. Under SAML single sign-on, select Enable SAML authentication.

PingOne fo	r Enterprise ACS URL field.
0	Enable SAML authentication Enable SAML authentication for your organization through an identity provider like Azure, Okta, Onelogin, Ping Identity or your custom SAML 2.0 provider.
	Save your recovery codes in a safe place. If your IdP is unavailable you can use a recovery code to skip single sign-on and access the SAML SSO Org organization.
	The SAML SSO Org organization single sign-on URL is https://github.com/orgs/summerses.//sso.
	The assertion consumer service URL is https://github.com/orgs/s/saml/consume. Configure your identity provider to send authenticated users to this URL.
	Sign on URL
	https://yourapp.example.com/apps/appld
	Members will be forwarded here when signing in to your organization
	Issuer
	https://example.com
	Public contificate
	Paste your x509 certificate here

5. Set the following values.

Field	Value
Sign on URL	https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid= <sup>[]</sup> PingOne-IdP-ID-value
lssuer	PingOne for Enterprise <b>Issuer</b> value
Public certificate	Paste in the contents of the PingOne for Enterprise signing certificate.

6. Click Save.

## Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to your Ping desktop as a user with GitHub access.

## (i) Note

To find the Ping desktop URL in the Admin console, go to **Setup**  $\rightarrow$  **PingOne Dock**.

2. Complete the PingOne for Enterprise authentication.

You're redirected to your GitHub domain.

	Ping Sign On	
USERNAME		
PASSWORD		
	Remember Me	
	Sign On	
	Forgot Password	

## Test the PingOne for Enterprise SP-initiated SSO integration

- 1. Go to https://github.com/orgs/your-tenant/sso.
- 2. After you're redirected to PingOne for Enterprise, enter your PingOne for Enterprise username and password.

	Ping Keetity Sign On	
USERNAME		
PASSWORD		
	Remember Me	
	Sign On	
	Forgot Password	

You're redirected back to GitHub.

## Configuring SAML SSO with GitHub Enterprise Server and PingFederate

Learn how to enable GitHub sign-on from a PingFederate URL (IdP-initiated sign-on) and direct GitHub sign-on using PingFederate (SP-initiated sign-on).

## Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users requiring application access.
- Populate GitHub with at least one user to test access.
- You must have administrative access to PingFederate and GitHub.

## Download the GitHub metadata

- 1. Go to where your GitHub server publishes its metadata ( https://GitHub-hostname/saml/metadata ).
- 2. Save the metadata as an XML file.

## **Create a PingFederate SP connection for GitHub**

- 1. Sign on to the PingFederate administrative console.
- 2. Create an SP connection for GitHub in PingFederate using the GitHub metadata file:
  - 1. Configure using Browser SSO profile SAML 2.0.
  - 2. Enable the following SAML Profiles:
    - IdP-Initiated SSO
    - SP-Initiated SSO
  - 3. In **Assertion Creation: Attribute Contract**, if you want to have these values populated in GitHub, extend the contract to add attributes called **username** and **full\_name**.
  - 4. In Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfillment, map SAML\_SUBJECT to an attribute containing the user's email address.

If added, map username and full\_name to appropriate attributes.

- 5. In Protocol Settings: Allowable SAML Bindings, enable POST.
- 6. In Credentials: Digital Signature Settings, select the PingFederate Signing Certificate.
- 3. Save the configuration.
- 4. Export the signing certificate.
- 5. Export and then open the metadata file.

Copy the value of the entityID and the Location entry ( https://your-value/idp/SSO.saml2 ).

## Add the PingFederate IdP Connection to GitHub

- 1. Sign on to GitHub Enterprise Server as an administrator.
- 2. Click the **Rocket** icon.
- 3. Click Management Console.

🖋 Site admin	
License info & search	
Management console	
Audit log	-

#### 4. Click Authentication.



5. Click SAML and select the idP initiated SSO (disables AuthnRequest) check box.



6. In the Single sign-on URL field, enter the PingFederate Location value ( https://your-value/idp/SSO.saml2 ).



7. In the Issuer field, enter the PingFederate entityID value.



- 8. Click Choose File for the Verification Certificate and upload the PingFederate signing certificate that you downloaded
- 9. Click Save Settings.

## Test the PingFederate IdP-initiated SSO integration

- 1. Go to the PingFederate SSO Application Endpoint for the GitHub SP connection.
- 2. Complete the PingFederate authentication.

You're redirected to your GitHub domain.

## Test the PingFederate SP-initiated SSO integration

- 1. Go to your GitHub server.
- 2. After you're redirected to PingFederate, enter your PingFederate username and password.

You're redirected back to GitHub.

## Configuring SAML SSO with GitHub Enterprise Server and PingOne for Enterprise

Learn how to enable GitHub sign on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct GitHub sign on using PingOne for Enterprise (SP-initiated sign-on).

## Before you begin

- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Populate GitHub with at least one user to test access.
- You must have administrative access to PingOne for Enterprise and GitHub.

## Download the GitHub metadata

- 1. Go to where your GitHub server publishes its metadata ( https://GitHub-hostname/saml/metadata ).
- 2. Save the metadata as an XML file.

## Set up the GitHub application in PingOne for Enterprise

- 1. Sign on to PingOne for Enterprise for Enterprise and go to **Applications**  $\rightarrow$  **Application Catalog**.
- 2. On the SAML tab, click Add Application.

<b>g</b> One'		DASHBOARD		USERS	SETUP	ACCOUNT	?	Sign Of
My Applications	Application Catalog	Pingid SDK A	pplications	OAuth Se	ettings			
My Applicati	ions							
SAML OIDC								
								_
Applications you've • Active applicat	e added to your account a	are listed here. Y le sign-on (SSO)	'ou can search ).	by applic	ation nar	me, description or er	tityld	
<ul> <li>Details displays</li> </ul>	s the application details.		<i>.</i>					
Applicatio	on Name	Туре	Status		Enabl	ed		
Add Application							Pause All SSO	
								,
Search Applicat	tion Catalog							1
Search Applicat	tion Catalog dication							

- 3. Enter **GitHub** as the application name.
- 4. Enter a suitable description.
- 5. Select **Collaboration** as the category.
- 6. Click Continue to Next Step.

7. In the **Upload Metadata** row, click **Select File** and upload the metadata file that you saved from GitHub.

2. Application Configuration						
I have the SAML configuration				I have the S	SSO URL	
You will need to download this SAML metadat	ta to config	jure the	e applicati	on:		
Signing Certificate	PingOne	Accou	nt Origina	tion Certifica	ate (2021) 🗸	]
SAML Metadata	Download					
Provide SAML details about the application ye	ou are conr	necting	to:			
Protocol Version	SAML v	2.0		v 1.1		
Upload Metadata 🛛 💿	Select Fi	ile	)r use UR	IL		
Assertion Consumer Service (ACS)	https://sso	o.exam	ple.com/a	a/sso.saml2	*	
Entity ID @	example.c	com/a			*	

The following values should now be populated:

- ACS URL: https://github.com/orgs/your-tenant/saml/consume
- o Entity ID: https://github.com/orgs/your-tenant
- 8. Click Continue to Next Step.
- 9. Click Add new attribute and map SAML\_SUBJECT to the attribute containing the user's email address.
  - 3. SSO Attribute Mapping

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

Application Att	tribute Identity Bridge Attribute or Literal Value	Required
Add new attribute		

#### 3. SSO Attribute Mapping

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

Application Attribute	dentity Bridge Attribute or Literal Value	Required	l i
	Email (Work)		
1 SAML_SUBJECT	As Literal		×
	Advanced		

10. Optional: Add the username and full\_name attributes, then map these to appropriate attributes.

This populates these values in GitHub when a new user signs on.

#### 11. Click Continue to Next Step.

12. Click **Add** for all user groups that should have access to GitHub.

#### 5. Group Access

Select all user groups that should have access to this application. Users that are members of the added groups will be able to SSO to this application and will see this application on their personal dock.

Group1, Group2, etc	Search	
Group Name		
Users@directory		Remove
Domain Administrators@directory		Add

#### 13. Click Continue to Next Step.

14. Copy the Issuer and idpid values.



16. Click Finish.

## Add the PingOne for Enterprise IdP Connection to GitHub

- 1. Sign on to GitHub Enterprise Server as an administrator.
- 2. Click the **Rocket** icon.
- 3. Click Management Console.

🖋 Site admin	
License info & search	
Management console	
Audit log	T

4. Click Authentication.

Password
SSH access
Hostname
Time
Authentication
Privacy

5. Click SAML and select the idP initiated SSO (disables AuthnRequest) check box.



6. In the Single sign-on URL field, enter https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=idpid-valuefrom-PingOne.



7. In the Issuer field, enter the PingOne for Enterprise Issuer value.



- 8. Click Choose File for the Verification Certificate and upload the PingOne signing certificate that you downloaded.
- 9. Click Save Settings.

Note

(i)

GitHub

## Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to your Ping desktop as a user with GitHub access.

To find the Ping desktop URL in the Admin console, go to Setup  $\rightarrow$  Dock  $\rightarrow$  PingOne Dock URL.

2. Complete the PingOne for Enterprise authentication.

You're redirected to your GitHub server.

	Ping Sign On	
USERNAME		
PASSWORD		
	Remember Me	
	Sign On	
· · · · ·		
	Forgot Password	

## Test the PingOne SP-initiated SSO integration

1. Go to your GitHub server.

2. After you're redirected to PingOne for Enterprise, enter your PingOne username and password.

	Ping Kentity Sign On	
USERNAME		
PASSWORD		
	Remember Me	
	Forgot Password	

You're redirected back to GitHub.

# Greenhouse

## Configuring SAML SSO with Greenhouse and PingOne

Learn how to configure SAML single sign-on (SSO) with Greenhouse and PingOne.

## Before you begin

(i)

You must have an Advanced or Expert subscription tier to configure SAML. Learn more in see https://support.greenhouse.io/hc/en-us/articles/210259723-Single-Sign-On-overview<sup>[2]</sup>.

**Note** This is a tested integration.

## **Configure SSO in Greenhouse**

- 1. Sign on to your Greenhouse portal and select the **Gear** icon (\$) in the upper right hand corner.
- 2. In the left navigation pane, go to **Dev Center**  $\rightarrow$  **Single Sign-On** to begin configuring SSO.



## (i) Note

If you don't see **Single Sign-On**, you'll need to contact Greenhouse customer support to update your permissions.

3. On the following page, click Begin Configuration.

The configuration page opens.

4. In the Add Greenhouse to your Single Sign-on provider section, note the SSO Assertion Consumer URL. You'll need this later.



## **Configure Greenhouse in PingOne**

1. On a new tab, sign on to your PingOne SSO admin account.

You'll use the settings from the previous procedure to start configuring Greenhouse in PingOne.

2. Go to **Connections**  $\rightarrow$  **Applications** and click the + icon.

P	ingIdentity.		
Enviro Admir Produc	nments nistrators ~ tion	Applications	
	< Connections	Q Search	Filter
*		20 Applications by Application Name	
เย	IDENTITY PROVIDERS	Aha Labs Client ID:	
0	External IDPs	-	
	PING PRODUCTS	AppDynamics Client ID:	
.((2	PingFederate	Datadog	
	PingIntelligence	Client ID:	

3. On the New Application page, click Advanced Configuration, and on the SAML line, click Configure.

LECT AN APPLICATION TYPE				
Web applications that are accessed within a browser.	Applications that are stored and run from a device or desktop.	A front-end application that uses an API.	Management API integrations that can perform actions using Roles.	Apps configured by advanced users fir the ground up.
• .NET web apps • Java apps WEB APP	IOS and Android apps     Deskto apps     Push Authentication     NATIVE APP	Angular     Node.js SINGLE PAGE APP	Non-Interactive service integrations     Client Credentials w/Role Assignment     Interactive admin consoles & portals     WORKER	Your choice     No barriers     Complete flexibility
	CHOOSE CO	ONNECTION TYPE		
	SAML Apps the	it utilize an Identity Provider (IDP) to authenticate users a	nd provides Service Providers an Authentication Assertion	n.

- 4. On the Create App Profile page, enter:
  - Application Name (Required)
  - Description (Optional)
  - Icon (Optional)

Create App Profile	ique profile. The description will help
APPLICATION NAME	
Greenhouse	
DESCRIPTION	
Greenhouse SSO Connection	
ICON	
g	
Remove Image	

- 5. Click Save and Continue.
- 6. On the **Configure SAML Connection** page, in the **Provide App Metadata** section, click **Manually Enter**.

	_	
Import From URL	۲	Manually Enter
	Import From URL	Import From URL

- 7. Input the service provider (SP) data:
  - In the ACS URLS field, paste in the SSO Assertion Consumer URL that you copied from Greenhouse in the previous procedure.

ITER METADATA FOR YOUR APPLICATION	
https://app4.greenhouse.io/f ?f/users/saml/consume	×

• In the Entity ID field, enter greenhouse.io.

ENTITY ID	
greenhouse.io	

• In the Assertion Validity Duration (In Seconds), enter a value, for example, 3600.

3600	SSERTION V	ALIDITY I SECON	DS)
	3600		

- 8. Click Save and Continue.
- 9. On the Attribute Mapping page, add the following attributes, selecting the Required check box for each attribute.
  - o saml\_subject = Email Address



This is automatically assigned to User ID, but will need to be updated.

- User.FirstName = Given Name
- User.LastName = Family Name

PPLICATION ATTRIBUTE		OUTGOING VALUE				
saml_subject	÷	Email Address	<b>*</b>	1	Required	
			Advanced Expression			
User.FirstName	←	Given Name	~	~	Required	
			Advanced Expression			
User.LastName	÷	Family Name	~	~	Required	
			Advanced Expression			

## 10. Click Save and Close.

11. On the **Applications** page, enable the connection by toggling the slider:

g Greenhouse Client ID: (	Arg daily sign-on:	0 Past 7 days	No data yet	%	:

- 12. Click on the newly created application to open it.
- 13. On the **Configuration** tab, in the **Connection Details** section, click **Download** to download the IdP metadata.

You'll need this to complete the next step.

Client ID:		
Profile Configuration Att	bute Mappings Policies Access	
2 <b></b>		1
<ul> <li>CONNECTION DETAILS</li> </ul>		
DOWNLOAD METADATA:	Download	
ISSUER ID :	https://auth.pingone.com//	
SINGLE LOGOUT SERVICE:	https://auth.pingone.com//	
SINGLE SIGNON SERVICE:	https://auth.pingone.com/t	
IDP METADATA URL:	https://auth.pingone.com//	
INITIATE SINGLE SIGN-ON URL:	https://auth.pingone.com/i	

14. Return to Greenhouse and, in the **Upload your Single Sign-On Provider** section, click **Choose File** and upload the IdP metadata that you downloaded in the previous step.

2. Upload your Single Sign-On Provider Metadata XML file to prefill the information below. (optional) Upload XML metadata file Choose File

All required fields will be populated automatically, except for the Name Identifier Format.

15. Update the Name Identifier Format to urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress.

Click Save.

pload XML metadata file	
Choose File	
Fill out the information below.	
ntity ID / Issuer *	
reenhouse.io	
ngle sign-on Url *	
ttps://auth.pingone.com/	File and an and a start
ngle logout url (optional)	
P Certificate Fingerprint *	
P Gertificate Fingerprint *	
P Certificate Fingerprint *	
P Certificate Fingerprint * ame Identifier Format * um:oasis:names:tc:SAML:11:nam	
P Certificate Fingerprint * me Identifier Format * urn:oasis:names:tc:SAML:11:nam  urn:oasis:names:tc:SAML:11:nameid-	
Certificate Fingerprint *	
<sup>o</sup> Certificate Fingerprint * ime Identifier Format * urn:oasis:names:tc:SAML:11:nam urn:oasis:names:tc:SAML:11:nameid- format:emailAddress urn:oasis:names:tc:SAML:11:nameid-	
<sup>o</sup> Certificate Fingerprint * Ime Identifier Format * urn:oasis:names:tc:SAML:11:nam urn:oasis:names:tc:SAML:1.1:nameid- format:emailAddress urn:oasis:names:tc:SAML:1.1:nameid- format:unspecified	
P Certificate Fingerprint *	), users will have the option to log in either using your SSO Identity Provider or using a
<sup>2</sup> Certificate Fingerprint * <sup>2</sup> Certificate Fingerprint *         ume Identifier Format *         urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress         format:unspecified         urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified         urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified         urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified	h, users will have the option to log in either using your SSO Identity Provider or using a o longer be able to log in using the Sign in with Google button. Users who do not have a by clicking the Forcat Password button on the Greenbuse Recruiting login name. Once you

## Create and assign identities

Before you can test the integration, you must create and assign identities in PingOne. If you've already assigned identities and groups in PingOne, move on to Test the integration.

1. In PingOne, go to Identities Groups and click the + icon next to Groups.

- 2. On the Create New Group page, enter values for the following:
  - Group Name (Required)
  - Description (Optional)
  - **Population** (Optional)
- 3. Click Finish & Save.

Groups  Administrators can manage their groups including creating groups, updating group membership manually or dynamically and more. Learn Q. Search Groups	Create New Group  Groups provide application access for users.
Name Apps	Enter Profile Data Group Name
Administrators Population	Description
Admin Admin	
	Population Administrators Population
	Finish & Save

4. To add identities to the group, on the **Identities** tab, go to **Users**  $\rightarrow$  + Add User.

Pi	ngldentity.			() - (S) Ex	splore • Ryan Schafer •
Environ Admini Product	iments istrators ~ ion	Users			
⊕	< Identities	Q Search or SCIM Query	Filters 🗸		+ Add User
	Users		Example SCIM Queries		
	Groups	4 users by Family Name ~			
ų	Populations				€
1	Attributes				
e	Roles				<b>•</b>
0		Test, Adam adamtest			
8					
		Test, Joe joetest			

5. On the Add User page, enter all the necessary information for a user.

# Important Verify that the first name, last name, and email address are correct, as these are values passed in the SAML assertion.

6. Click Save.

Add	User			$\otimes$
	COUNTRY CODE	LOCALITY	REGION	
	ZIP CODE			
C	OMPANY INFORMATION			
-	ACCOUNT ID		POPULATION @	
			Administrators Population	
	USERNAME			
	1			
	ТҮРЕ			
	TITLE			
PI	REFERENCES			
	PREFERRED LANGUAGE		LOCALE	
	None	~	None ~	
	TIMEZONE Select a timezone ~			
Sa	Cancel			
				_

- 7. Assign the user that you created to the group that you created previously. Locate the user you created and do the following:
  - Expand their section.
  - Select the Groups tab.
  - Click + Add.

Fest, Adam adamtest							
Profile	Roles	Authentication	Groups	Consent	API	Sync Status	Credentials
Group Men	nberships 1	+ Add					
Apps							

8. In the **Available Groups** section, select the group that you created and click the + icon to add it to the user's group memberships. Click **Save**.

Back to Users		
Adam Test		
Profile         Roles         Authentication         Groups           0         Groups define a collection of users using membership or by dynamic filtering criteria. Groups can be used to assign application access to us         Q.         Search Available Groups	5015.	
VAILABLE GROUPS	GROUP MEMBERSHIPS	
ii Admin 🕂	Apps Administrators Population	$\bigcirc$

- 9. On the Connections tab, for the Greenhouse application, do the following:
  - Click the Access tab.
  - $\,\circ\,$  Click the Pencil icon to edit the configuration.

8	Greenhouse Client ID: (			
Profile	Configuration	Attribute Mappings	Policies	Access
GRC	DUP MEMBERSHIP PC	DLICY		

10. Select the group that you created and add it to the Applied Groups section. Click Save.

8 Greenhouse > Edit 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 ac The following selections determine groups that have access to the application.	cess when no groups are listed.
Q Search Groups	
ALL GROUPS	APPLIED GROUPS
ii Admin (+	Apps

## Test the integration

- 1. In the PingOne admin console, go to **Dashboard**  $\rightarrow$  **Environment Properties**.
- 2. Right-click on the Application Portal URL and open it in a private browser session.



3. Sign on as the test user that you created and click the Greenhouse tile.

All Applications	Ping			Q Find application	ons				Rj	yan Schafer 🚺
	ALL APPLICATIONS									
	Aha!	DATADOG	freshworks	8	٢	<b>1</b>	outsystems	PagerDuty	् quickbase	
	Aha Labs	Datadog	Freshworks	Greenhouse Test	Heap	Litmos	Outsystems Test	PagerDuty	QuickBase	

You're signed on to the user's Greenhouse account.

4. On the SSO configuration page in Greenhouse, click Finalize Configuration.

	Edit	Finalize Configuration
Status: • In testing How do I test my SSO?		
The SSO configuration on your account is in a testing state. Users may log in using y require all users to log in via your IdP once you've completed testing.	our IdP or using a Greenhouse passwor	d. Finalize your configuration to
SO Assertion Consumer URL		
https://app4.greenhouse.io/		
intity ID / Issuer		
greenhouse.io		
Single sign-on Url		
nttps://auth.pingone.com/		
dP Certificate Fingerprint		
lame Identifier Format		
ırn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress		
mployee log in method		
Email		

5. When prompted, enter **Configure** . Click **Finalize** to complete the connection.

Single Sign-On			Edit	Finalize Configuration
nalize Configuration				
Status: • In testing H	ow do I test my SSO?			
The SSO configuration on y require all users to log in vis	your account is in a testing state. Users may log in using your IdP or a your IdP once you've completed testing.	using a Greenho	ouse passwor	d. Finalize your configuration to
SSO Assertion Consumer	Finalize Configuration ×	rs/saml/con	sume	
	wate the internet which for them the internet the test			
Entity ID / Issuer	By finalizing Single Sign-On, all existing user			
greenhouse.io	passwords will be deleted permanently. This cannot be undone.			
Single sign-on Url	Are you sure you want to finalize your Single Sign-On			
https://auth.pingone.c	configuration?	p/sso		
IdP Certificate Fingerprin	Type "CONFIGURE" to Confirm			
2d519b75a6ee8e0715(	CONFIGURE			
Name Identifier Correct	Cancel Finalize			
Name Identifier Format				
urn:oasis:names:tc:SA				
Employee log in method				
Email				

# Неар

## Configuring SAML SSO with Heap and PingOne

Learn how to configure SAML single sign-on (SSO) with Heap and PingOne.

## **Configure SSO with Heap**

- 1. Sign on to your Heap admin portal and make sure that you're in the **Development** section.
- 2. In the left hand pane, go to Account  $\rightarrow$  Manage  $\rightarrow$  General Settings.
- 3. In the Single Sign-On section, copy the Metadata URL. You'll need this later.

Main Developmen	t (No data)	Account	General Settings	
Analysis		General Settings	Mandatory Two-Factor Protect your account by req	or Authentication uiring admins or all users to enable two-factor authentication.
🕐 Overvi	ew	Data Governance	Not Required 🗸	
88 Dashb	oards	Privacy & Security		
T Report	s	User Identities	Single Sign-On Heap SAML service provider det	ails
ណ៍ Analyz	e	Features	You'll need these to configu	re your Identity Provider to allow Heap access to your users.
		Teammates	Metadata URL	https://heapanalytics.com/saml/metadata/3056845492/
Data Managen	nent	Teama	SAML Version	2.0
💖 Definit	ions	leans	Assertion Consumer URL	https://heapanalytics.com/saml/finalize/3056845492/
C Event	/isualizer	Projects	Consumer Binding	urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
(••) Live		Roles	NameID Format	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
		Plan Usage	Attributes	None required
Administration	n	Evoluded IPe	Entity ID	heapanalytics.com
🛱 Update	es	Excluded IFS	Your SAML Identity Provider cert	lificate
Co Integra	ite >	Signed in as ryanschafer@pingidentity.co		4
🕄 Accou	nt v	m	Your SAML Identity Provider deta Remote login URL	alls
→ Ma	nage		Logout landing URL (optio	inal)
Get Su	pport		Save Configuration	
Sign O	ut		Time Zone	

- 4. In a new tab, sign on to your PingOne admin account and go to **Connections**  $\rightarrow$  **Applications**.
- 5. Click the + icon next to **Applications**.



- 6. On the New Application page, click Advanced Configuration.
- 7. In the Choose Connection Type list, on the SAML line, click Configure.

ECT AN APPLICATION TYPE				
609		A foot and application that uses an API		
browser.	device or desktop.	A front-end application that uses an API.	perform actions using Roles.	the ground up.
• .NET web apps • Java apps	<ul> <li>iOS and Android apps</li> <li>Desktop apps</li> <li>Push Authentication</li> </ul>	• Angular • Node.js	Non-interactive service integrations     Client Credentials w/Role Assignment     Interactive admin consoles & portals	Your choice     No barriers     Complete flexibility
WEB APP	NATIVE APP	SINGLE PAGE APP	WORKER	ADVANCED CONFIGURATION
	CHOOSE CC	DNNECTION TYPE		
	SAML	at utiliza an Irlantitu Providar (IDD) to suthanticate usors a	nd noveldas Sandra Drouldars an Authantication Assartion	Configure
		r unice an identity rivinger (Cr) to addrenocate users an	in provides Service Providers an Autrentication Assention	· · · · · · · · · · · · · · · · · · ·
	OIDC Employs	Universal Login and redirect users to the login page.		Confi

- 8. On the Create App Profile page, enter the values for:
  - Application Name (Required)
  - Description (Optional)
  - Icon (Optional)
| Create App Profile   |
|--|
| Personalize your application by creating a unique profile. The description |
|  |
| APPLICATION NAME   |
| Неар   |
| DESCRIPTION  |
| Heap SSO Integration   |
| ICON   |
|  |
|  |
| Remove Image   |

9. On the Configure SAML Connection page, in the Provide App Metadata section, click Import From URL.

Paste in the URL that you copied previously and click Import.

CC	Onfigure SAML Connection
0.11	
	Import Metadata Import From URL Manually Enter
	IMPORT URL
	https://heapanalytics.com/saml/metadata/:

After import, all necessary fields are auto-populated except for the Assertion Validity Duration.

- 10. In the **Assertion Validity Duration** field, enter a valid duration value (in seconds), such as 3600.
- 11. Update the SUBJECT NAMEID FORMAT section to urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress.

## (i) Note

If you don't update this section, you'll get an error for the integration. **SUBJECT NAMEID FORMAT** does not automatically update when you upload the service provider metadata.

12. In the Signing Key section, select Download Signing Certificate and download in the X509 PEM (.crt) format. Click Save and Continue.



13. On the Attribute Mapping page, update the Outgoing Value to Email Address for the saml\_subject application attribute.

(i) Note	
No other attributes are required.	

14. Click **Save and Close** to finalize the creation of the application.

SAML ATTRIBUTES		
APPLICATION ATTRIBUTE	OUTGOING VALUE	
saml_subject	← Email Address	Y Required
		Advanced Expression
+ ADD ATTRIBUTE		

15. After you create the application, click the toggle next to the application to enable it.

88	-8b09-4086-a6	75-df7a456f1fa7		
nfi	guration	Attribute Mappings	Policies	Access
	Advanced (	Configuration (SAML)		
	Heap SSO	Integration		
	4fa29988-8	b09-4086-a675-df7a456f1	a7	
	No Home P	age Configured		
	Default Sign	non Page		

- 16. Select **Configuration** and copy the following values. You'll need these later.
  - Single Logout Service
  - Single SignOn Service

Client ID		<b>•</b> : ×
Profile Con	figuration Attribute Mappings Policies Access	
APP TYPE:	Advanced Configuration (SAML)	
DESCRIPTIC	DN: Heap SSO Integration	
CLIENT ID:		
HOME PAGE	E URL: No Home Page Configured	
SIGNON UR	L: Default Signon Page	

17. In your Heap account, go to the **Your SAML Identity Provider certificate** section and paste in the Ping X509 certificate that you downloaded previously.

(i) Note You must include	the <b>BEGIN CERTIFICATE</b> and <b>END CERTIFICATE</b> text as part of the certificate upload.
Client ID:	
Profile Configuration Attr	ibute Mappings Policies Access
CONNECTION DETAILS	
DOWNLOAD METADATA :	Download
ISSUER ID :	https://auth.pingone.com/
SINGLE LOGOUT SERVICE:	https://auth.pingone.com/
SINGLE SIGNON SERVICE:	https://auth.pingone.com/
IDP METADATA URL:	https://auth.pingone.com/
INITIATE SINGLE SIGN-ON URL:	https://auth.pingone.com/
✓ SAML SETTINGS	

- 18. Paste the URLs that you copied previously into the corresponding fields:
  - Single SignOn Service= Remote login URL
  - Single Logout Service= Logout landing URL (optional)

#### 19. Click Save Configuration.

Metadata URL	https://heapanalytics.com/saml/metadata/
SAML Version	2.0
Assertion Consumer URL	https://heapanalytics.com/saml/finalize
Consumer Binding	urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
NameID Format	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
Attributes	None required
Entity ID	heapanalytics.com
our SAML Identity Provider cert BEGIN CERTIFICATE- MIIDejCCAmKgAwIBAgIG	ificate  AXrpzcRbMAOG

After saving the configuration, a **Test Configuration** button appears.

## 20. Click Test Configuration.

You're signed out and then prompted to sign on with your username and password.

## Single Sign-On

You've configured your SAML Identity Provider but not enabled it yet. Your teammates won't be able to authenticate against the provider until it's been enabled.

You can enable your Identity Provider after a successful test.

Login URL	https://auth.pingone.com/
Identity Provider certificate fingerprint	
Certificate expires	in 9 months
Test Configuration	1
Remove Configurat	ion

21. After signing on to your Heap account, go to the **Single Sign-On** settings section and select **Enable Configuration** to finalize the SSO connection.

## Single Sign-On

You've successfully authenticated with your SAML Identity Provider. You can now enable SSO login for Heap.

The following details were obtained with the test authentication.

Email address		
Session valid until	2021-10-20T23:04:22.995Z	
Login URL	https://auth.pingone.com/	
Logout URL	https://auth.pingone.com/	
Identity Provider certificate fingerprint		
Certificate expires	in 9 months	
Enable Configurati	ion	
Remove Configurat	ion	

#### **Create and assign identities**

Before testing your integration, you must create and assign identities in PingOne. If you've already assigned identities and groups in PingOne, move on to Test your integration.

1. In PingOne, go to **Identities**  $\rightarrow$  **Groups** and click the + icon next to **Groups**.

PingIdentity.					
Enviro Admir Produc	nments histrators ~ tion				
⊕	< Identities	Q Search Groups			
	Users	Name			
2	Groups	Apps Administrators Population			
ເຍ	Populations				
0	Attributes	Admin			
e	Roles				
Ô					
ᢒ					

- 2. On the **Create New Group** page, enter values for the following:
  - Group Name (Required)
  - Description (Optional)
  - Population (Optional)
- 3. Click Finish & Save.

Groups 🚭	× Create New Group
Administration can manuage their glocps including creating groups, updating group memorensity manually or dynamically and more. Least Q. Search Groups	Groups provide application access for users.
Name	Enter Profile Data
Apps Apps Administrators Population	Group Name
Admin Admin	Description
	Population
	Finish & Save

4. To add identities to the group, on the **Identities** tab, go to **Users**  $\rightarrow$  + Add User.

P	ingldentity.			⑦ • ⑤ Explore • Provide and
Enviror Admin Produc	nments istrators ~	Users		
•	< Identities	Q Search or SCIM Query	Filters ~	+ Add User
	Users		Example SCIM Queries	
	Groups	4 users by Family Name ~		
-	Populations			
2	Attributes			-
e	Roles			
ø		Test, Adam adameet		
S				
		Test, Joe joetest		

5. On the **Add User** page, enter in all the necessary information for a user.

## 🔿 Important

Verify that the first name, last name, and email address are correct, as these are values passed in the SAML assertion.

#### 6. Click Save.

Add User				$\otimes$
COUNTRY CODE	LOCALITY	REGION		
ZIP CODE				
	N			
ACCOUNT ID				
		Administrators Population	~	
USERNAME				
1				
TYPE				
TITLE				
PREFERENCES				
PREFERRED LANGUAGE	0	LOCALE		
None	~	None 🗸		
TIMEZONE Select a timezone ~				
Save Cancel				

- 7. Assign the user that you created to the group that you created previously. Locate the user you created and do the following:
  - 1. Expand the section for the user.
  - 2. Select the **Groups** tab.
  - 3. Click **+ Add**.

Test, Adam adamtest								Reset Password	D	Ī
Profile	Roles	Authentication	Groups	Consent	API	Sync Status	Credentials	]		
Group Mer	mberships 1	+ Add								
Apps										
										1

8. In the Available Groups section, select the group that you created and click the + icon to add it to the user's group memberships. Click Save.

< Back to Users		
Adam Test		
Profile         Roles         Authentication         Groups           ①         Groups define a collection of users using membership or by dynamic filtering criteria. Groups can be used to assign application acce	eess to users.	
Q Search Available Groups		
AVAILABLE GROUPS	GROUP MEMBERSHIPS	
ii Admin	+ Hops Administrators Population	$\bigcirc$

- 9. On the **Connections** tab, for the Heap application:
  - Click the Access tab
  - $\circ\,$  Click the Pencil icon to edit the configuration

٢	Heap Client ID: 4f	a29988-8b09-4086-a6	75-df7a456fffa7							Avg daily sign-ons:	0 Past 7 days	12 wk trend	%	
	Profile GROUP MEI Apps	Configuration MBERSHIP POLICY	Attribute Mappings	Policies	Access									

10. Select the group that you created and add it to the Applied Groups section. Click Save.

in Application L	ist							
Client ID:	4							
Profile	Configuration	Attribute Mappings	Policies	Access				
Admin Only Acces	55							
Must have ad	lmin role							
3roup Membershi	ip Policy							
Groups can be add	ed to control user a	ccess to the application. A ups that have access to th	All users have ac he application.	ccess when no g	roups are listed.			
The following selec	uons determine gro							
The following selec	os							
C Search Group	25						APPLIED GROUPS	
C Search Group C Search Group C GROUPS C Apps Administrate	ors Population					(+)	APPLIED GROUPS	Add access control for groups by dragging them here

## **Test your integration**

- 1. In the PingOne admin console, go to **Dashboard**  $\rightarrow$  **Environment Properties**.
- 2. Right-click on the **Application Portal URL** and open it in a private browser session.

Environment Forvironment Audit Audit Audit Audit DESCRIPTION The administrator environment created when the organization was orvisioned. UCENSE ADMIN ENVIRONMENT ID Reference (US) Reference (US) CREATED 202107-277211014.3132 CONSOLE LOGIN URL @ https://console.pingone.com/?d655de53.38814.4006-bep Copy Link Address Set UNIFORM Console.pingone.com/?d655de53.38814.4006-bep Copy Link Address Set UNIFORM Console.pingone.com/?d655de53.38814.4006-bep Copy Link Address Copy Link Console.pingone.com/?d65de53.38814.4006-bep Copy Link Address	P	i <b>ng</b> ldentıty.	
Consolution Means Consolution Means Consolution Means Consolution Means Consolution Means Consolution C	Enviror Admin Produc	inments istrators ~ tion	
Audit   Audit   Audit   Alerts   This is the administrator environment created when the organization was provisioned.   ILCENSE   ADMIN   ILCENSE   ADMIN   CO    CO <	⊕	< Environment	internal
Audit DESCRIPTION   Alerts This is the administrator environment created when the organization was provisioned.   ICENSE ADMIN   ADMIN ICENSE   ENVRONMENT ID ICENSE   CREATED ICENSE   CONSOLE LOGIN URL ICENSE   ADVICTORSOLE LOGIN URL ICENSE   ADVILATION PORTAL URL ICENSE   ADPULCATION PORTAL URL ICENSE   APPLICATION PORTAL URL ICENSE   APPLICATION PORTAL URL ICENSE   ADVILATION PORTAL URL ICENSE   APPLICATION PORTAL URL ICENSE   APPLICATION PORTAL URL ICENSE   APPLICATION PORTAL URL ICENSE   APPLICATION PO	-	Properties	Administrators
Alerts This is the administrator environment created when the organization was provisioned.   ILCENSE   ADMIN   ILCENSE   ADMIN   ILCENSE   ADMIN   ICONSCIENCE   ICONSCIENCE  <	*	Audit	DESCRIPTION
LICENSE   ADMIN   ENVIRONMENT ID fd65de53-8841-4006-b907- GORGANIZATION ID 2a02a4bf-54da-424f-830c- TYPE Production REGION North America (US) CREATED 2021-07-277121:10:14.313Z CONSOLE LOGIN URL @ https://console.pingone.com/?d65de53-8841-4006-b907 SelF-SERVICE URL @ https://apos.pingone.com/?d65de53-8841-4006-b907 Copy Link to Highlight Print	ห	Alerts	This is the administrator environment created when the organization was provisioned.
EDMA     EDMA   ENVIRONMENT ID fd65de53-8841-4006-b907 GRGANIZATION ID 2a02a4bf-54da-424f-830c    CRGANIZATION ID 2a02a4bf-54da-424f-830c    TYPE Production REGION North America (US) CREATED 2021-07-27T21:0:14.313Z CONSOLE LOGIN URL    CONSOLE LOGIN URL    CONSOLE LOGIN URL    SELF-SERVICE URL    SELF-SERVICE URL    https://console.pingone.com//d65de53-8841-4006-b90   APPLICATION PORTAL URL	٢		
ENVIRONMENT ID fd65de53-8841-4006-b907 ORGANIZATION ID 2a02a4bf-54da-424f-830c- TYPE Production REGION North America (US) CREATED 2021-07-27T21:10:14.313Z CONSOLE LOGIN URL CONSOLE LOGIN URL SELF-SERVICE URL https://console.pingone.com/fd65de53-8841-4006-b90 https://apps.pingone.com/fd65de53-8841-4006-b90	Ô		ALITTIN
ORGANIZATION ID 2a02a4bf-54da-424f-830c- TYPE Production REGION North America (US) CREATED 2021-07-27T21:10:14.313Z CONSOLE LOGIN URL https://console.pingone.com/?env=fd65de53-8841-4006-b90 Save Link in Incognito Window Open Link in Inc	\$		ENVIRONMENT ID fd65de53-8841-4006-b907-
TYPE Production REGION North America (US) CREATED 2021-07-27121:014.313Z CONSOLE LOGIN URL CONSOLE LOGIN URL Mttps://console.pingone.com/?env=r/d65de53-8841-4 SELF-SERVICE URL https://apps.pingone.com/?d65de53-8841-4006-b90 APPLICATION PORTAL URL Mttps://apps.pingone.com/?d65de53-8841-4006-b90			ORGANIZATION ID 2a02a4bf-54da-424f-830c-
REGION North America (US) CREATED 2021-07-27T21:10:14.313Z CONSOLE LOGIN URL https://console.pingone.com/?env=fd65de53-8841-4006-b90 SELF-SERVICE URL https://apps.pingone.com/fd65de53-8841-4006-b90 APPLICATION PORTAL URL https://apps.pingone.com/fd65de53-8841-4006-b90			TYPE Production
CREATED       Open Link in New Tab         2021-07-27T21:10:14.313Z       Open Link in New Window         CONSOLE LOGIN URL       Image: Construction of the second s			REGION
2021-07-27721:10:14.313Z       Open Link in New Window         CONSOLE LOGIN URL       Open Link in Incognito Window         https://console.pingone.com/?env=fd65de53-8841-4       Save Link As         SELF-SERVICE URL       Copy Link Address         https://apps.pingone.com/fd65de53-8841-4006-b90       Copy         APPLICATION PORTAL URL       Copy Link to Highlight         Print       Print			CREATED Open Link in New Tab
CONSOLE LOGIN URL  CONSOLE LOGIN			2021-07-27T21:10:14.313Z Open Link in New Window Open Link in Incognito Window
SELF-SERVICE URL    SELF-SERVICE URL    Copy Copy Copy Copy Copy Copy Copy Co			CONSOLE LOGIN URL @ https://console.pingone.com/?env=fd65de53-8841-4 Save Link As Consv Link Address
APPLICATION PORTAL URL @ Copy Link to Highlight Print Print			SELF-SERVICE URL @ Copy Link Address Copy Link A
			APPLICATION PORTAL URL  Copy Link to Highlight Print

3. Sign on as the test user that you created and click the Heap tile.

You're signed on to the user's Heap account using SSO and testing is complete.

All Applications	Ping			Q Find applica						Ryan Schafer 🚺
	ALL APPLICATIONS									
	Aha!	DATADOG	freshworks	$\bigcirc$	õ	outsystems	PagerDuty	ଟ୍ quickbase	💎 wrike	
	Aha Labs	Datadog	Freshworks	Heap	Litmos	Outsystems Test	PagerDuty	QuickBase	Wrike	

# **HubSpot**

## Configuring SAML SSO with HubSpot and PingFederate

Learn how to enable HubSpot sign-on from a PingFederate URL (IdP-initiated sign-on) and direct HubSpot sign-on using PingFederate (SP-initiated sign-on).

#### Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users requiring application access.
- Populate HubSpot with at least one user to test access.
- You must have administrative access to PingFederate and HubSpot.

#### Create a PingFederate SP connection for HubSpot

- 1. Obtain the HubSpot SSO details.
  - 1. Sign on to HubSpot, click the **Gear** icon (\$), and select **Account Details** from the **Settings** menu.
  - 2. In the Single Sign-on section, click Set up.

< Back	Security	
Settings	Export Login History Export a login history report showing when users logged in to your HubSpot account in the last 90 days.	Export
Your Preferences Basic Info	Export HubSpot employee access history Export a HubSpot employee access history report showing when HubSpot employees accessed your account in the last 90 days.	Export
Notifications Security	Export Security Activity History Export a history report showing notable security actions taken in your HubSpot account in the last year.	Export
Account Setup	Require Two-factor Authentication (2FA)	
Account Defaults	Require all users to set up 2FA to log-in.	
Users & Teams Integrations	Single Sign-on Use your company's login credentials	Set up

3. Copy the Audience URI and Sign on URL, ACS, Recipient, or Redirect values.

Most Identity Providers	Microsoft AD FS	
Audience URI (Service Provid	er Entity ID)	
https://api.hubspot.com	/login-api/v1/saml/login?portalld=	Сору
Sign on URL, ACS, Recipient,	or Redirect	
https://api.hubspot.com	/login-api/v1/saml/acs?portalld=	Сору

- 2. Sign on to the PingFederate administrative console.
- 3. Create an SP connection for HubSpot in PingFederate.
  - 1. Configure using Browser SSO profile SAML 2.0.
  - 2. Set Partner's Entity ID to the HubSpot Audience URI value.
  - 3. Enable IdP-Initiated SSO and SP Initiated SSO.
  - 4. In Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfillment, map the SAML\_SUBJECT to the email attribute.
  - 5. In **Protocol Settings: Assertion Consumer Service URL**, set **Binding** to **POST** and set **Endpoint URL** to the HubSpot Sign on URL, ACS, Recipient, or Redirect value.
  - 6. In Protocol Settings: Allowable SAML Bindings, enable POST.
  - 7. In Credentials: Digital Signature Settings, select the PingFederate signing certificate.
- 4. Export the metadata for the newly-created HubSpot SP connection.
- 5. Export the signing certificate.
- 6. Open the metadata file and copy the values of the entityID and the Location entry (https://your-value/idp/SSO.saml2).

#### Add the PingFederate connection to HubSpot

- 1. Sign on to HubSpot, click the Gear icon (\$), select Account Details, and access the Single Sign-on settings.
- 2. Paste the entityID value that you copied previously to the Identity Provider Identifier or Issuer URL field.
- 3. Paste the Location value you copied previously to the Identity Provider Single Sign-on URL field.
- 4. Paste the PingFederate certificate into the X.509 Certificate field.

Then provide the values from your identity provider.
Identity Provider Identifier or Issuer URL
Identity Provider Single Sign-on URL
X.509 Certificate
BEGIN CERTIFICATE

#### 5. Click Verify.

6. In the left sidebar menu, click **Account Defaults**.

7. In the Single Sign-on (SSO) section, select the Require Single Sign-on to log in check box.

ecurity	
Single Sign-on (SSO) Use your company's log in credentials	Edit Disable
Require Single Sign-on to log in.	
Exclude users	

## ) Note

The user setting this up is automatically excluded to ensure their access is not lost in case of setup issues.

## Test the PingFederate IdP-initiated SSO integration

- 1. Go to the PingFederate SSO Application Endpoint for the HubSpot SP connection.
- 2. Complete PingFederate authentication.

You're redirected to your HubSpot domain.

Contacts - Conversations - Marketing -	Sales - Service - Autom	aation ~ Reports ~			(	<b>्र 🖷</b>	٥	. I 💿 👘
Contacts 💌 2 Contacts	Contacts  Actions  Import Create contact Create contact							
All contacts 👻 🖈 My contacts	★ Unassigned contacts	+ Add view	All views					
Search name, phone, e <b>Q</b> Contact ow	ner 👻 Create date 👻	# More filters				Table a	ctions 🔻	Save view
NAME \$	EMAIL	÷	PHONE NUMBER	¢ CONTACT OW	INER		÷	ASSOCIATED COMPANY

#### Test the PingFederate SP-initiated SSO integration

- 1. Go to https://app.hubspot.com/login/sso  $\square$ .
- 2. When you are redirected to PingFederate, enter your PingFederate username and password.

After successful authentication, you're redirected back to HubSpot.

<b>`</b> >>	Contacts v Convers	ations ~ Marketing ~	Sales - Service - Auton	nation ~ Reports ·	•			오 📅 🌣			~
	Contacts  Actions  Actions  Create contact										
	* All contacts 👻	* My contacts	★ Unassigned contacts	+ Add view	All views						
	Search name, phone,	e Q Contact ow	mer 👻 Create date 👻	# More filters				Table actions	•	Save view	
	NAME 🗘		EMAIL	÷	PHONE NUMBER	÷	CONTACT OWNER	÷	ASS	OCIATED COMPANY	

## Configuring SAML SSO with HubSpot and PingOne for Enterprise

Learn how to enable HubSpot sign-on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct HubSpot sign-on using PingOne for Enterprise (SP-initiated sign-on).

#### Before you begin

- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Populate HubSpot with at least one user to test access.
- You must have administrative access to PingOne for Enterprise and HubSpot.

#### **Obtain the HubSpot SSO details**

- 1. Sign on to HubSpot, click the **Gear** icon (\$), and select **Account Details** in the **Settings** menu.
- 2. In the Single Sign-on section, click Set up.

< Back	Security	
Settings	Export Login History Export a login history report showing when users logged in to your HubSpot account in the last 90 days.	Export
Your Preferences	Evro at Unix Sect annulation access history	
Basic Info	Export HubSpot employee access history Export a HubSpot employee access history report showing when HubSpot employees accessed your account in the last 90 days.	Export
Notifications		
Security	Export Security Activity History Export a history report showing notable security actions taken in your HubSpot account in the last year.	Export
Account Setup	Require Two-factor Authentication (2FA)	
Account Defaults	Require all users to set up 2FA to log-in.	
Users & Teams	Single Sign-on	
Integrations 🗸	Use your company's login credentials	Set up

3. Copy the Audience URI and Sign on URL, ACS, Recipient, or Redirect values.

## Add the HubSpot application to PingOne for Enterprise

- 1. Sign on to PingOne for Enterprise and go to **Applications**  $\rightarrow$  **My Applications**.
- 2. On the SAML tab, click Add Application.

<b>ng</b> One'		DASHBOARD	APPLICATIONS	USERS	SETUP	ACCOUNT	•	Sign Off
My Applications	Application Catalog	Pingid SDK A	pplications	OAuth Se	ettings			
My Applicati	ions							
SAML OIDC								
								-
Applications you've	e added to your account	are listed here. Y	'ou can search	by applic	ation na	me, description or entit	yld	
<ul> <li>Active applicat</li> <li>Details display</li> </ul>	ions are enabled for sing s the application details.	le sign-on (SSO)	).					
Applicatio	on Name	Туре	Status		Enab	led		
Add Application							Pause All SSO	-
Search Applicat	tion Catalog							9
New SAMI Apr				_				9
	plication							9

- 3. For the application name, enter HubSpot.
- 4. Enter a suitable description.
- 5. For the category, select **CRM**.
- 6. Click Continue to Next Step.
- 7. Set Assertion Consumer Service (ACS) to the HubSpot Sign on URL, ACS, Recipient, or Redirect value and Entity ID to the HubSpot Audience URI value.

#### 8. Click Continue to Next Step.

9. HubSpot needs the email passed in.

- If you use an email address to sign on using PingOne for Enterprise, click **Continue to Next Step**.
- If you sign on with a username, enter your email attribute in the SAML\_SUBJECT mapping, then click Continue to Next Step.

Attribute M	Mapping							
Map you	Map your identity bridge attributes to the attributes required by the application.							
	Application Attribute	Description	Identity Bridge Attribute or Literal Value					
	SAME SUBJECT	Man your email address attribute	Email (Work)					
1	1 *	(mail in AD)	As Literal					
			Advanced					

10. Click **Add** for all user groups that should have access to HubSpot.

roup Access		
Select all user groups that should have access to th see this application on their personal dock.	his application. Users that are members of the added groups will be able to SSO to	this application and wil
Group1, Group2, etc	Search	
Group Name		
Users@directory		Remove
Domain Administrators@directory		Add

#### 11. Click Continue to Next Step.

12. Copy and save the Issuer and Initiate Single Sign-On (SSO) URL values.

Issuer	https://pingone.com/idp/
idpid	
Protocol Version	SAML v 2.0
ACS URL 👩	
entityId 💿	
Initiate Single Sign-On (SSO) URL @	https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=1

13. Download the PingOne for Enterprise signing certificate.

Signing Certificate	Download
SAML Metadata	Download

14. Click Finish.

#### Add the PingOne for Enterprise connection to HubSpot

- 1. Sign on to HubSpot, click the Gear icon (\$\$), select Account Details from the Settings menu, and open the Single Sign-on settings.
- 2. In the **Identity Provider Identifier or Issuer URL** field, enter the PingOne for Enterprise **Issuer** value.
- 3. In the Identity Provider Single Sign-on URL field, enter the PingOne for Enterprise Initiate Single Sign-On (SSO) URL value.
- 4. Paste the PingOne for Enterprise signing certificate into the **X.509 Certificate** field.

Then provide the values from you	identity provider.	
Identity Provider Identifier or Issu	r URL	
	_	
Identity Provider Single Sign-on U	λL.	
X.509 Certificate		
BEGIN CERTIFICATE		

#### 5. Click Verify.

6. In the sidebar menu, click **Account Defaults**.

7. In the Single Sign-on (SSO) section, select the Require Single Sign-on to log in check box.

Security	
Single Sign-on (SSO) Use your company's log in credentials	Edit Disable
Require Single Sign-on to log in.	
Exclude users	

## (i) Note

The user setting this up is automatically excluded to ensure that their access is not lost in case of setup issues.

## Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to your PingOne for Enterprise desktop as a user with HubSpot access.

## (i) Note

To find the PingOne for Enterprise desktop URL in the Admin console, go to Setup  $\rightarrow$  Dock  $\rightarrow$  PingOne Dock URL.

2. Complete PingOne for Enterprise authentication.

You're redirected to your HubSpot domain.



Sontacts - Conversa	ations ~ Marketing ~	Sales – Service – Auto	omation ~ Reports ~				० n 🗘	🔹   🕘 🛛 👻
Contacts 💌 2 Contacts	Contacts  Actions  Import Create contact Create contact						Create contact	
* All contacts 👻	★ My contacts	オ Unassigned contacts	+ Add view	All views				
Search name, phone,	Search name, phone, e 🔍 Contact owner * Create date * 🕸 More filters Table actions *							
NAME 👙		EMAIL	÷	PHONE NUMBER	÷	CONTACT OWNER	÷	ASSOCIATED COMPANY

## Test the PingOne for Enterprise SP-initiated SSO integration

1. Go to https://app.hubspot.com/login/sso  $\square$ .

You're redirected to PingOne for Enterprise.

2. Enter your PingOne for Enterprise username and password.

	Ping Sign On	
USERNAME		
PASSWORD		
	Hemember Me	
	Sign On	
	Forgot Password	

After successful authentication, you're redirected back to HubSpot.

%	Contacts v Convers	sations ~ Marketing ~	Sales – Service – Auto	omation ~ Reports ·			< 🖷 🌣	🔺   🕘 🛛 👻
2	Contacts 💌 Contacts					Actions	- Import	Create contact
	* All contacts 👻		★ Unassigned contacts	+ Add view	All views			
	Search name, phone,	e Q Contact o	wner 👻 Create date 👻	‡ More filters			Table actions •	Save view
	NAME \$		EMAIL	÷	PHONE NUMBER	OWNER	\$	ASSOCIATED COMPANY

# Jamf

Jamf

## **Configuring SAML SSO with Jamf Pro and PingFederate**

Enable Jamf Pro sign-on from the PingFederate console (IdP-initiated sign-on) and direct Jamf Pro sign-on using PingFederate (SP-initiated sign-on).

#### Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users requiring application access.
- Populate Jamf Pro with at least one user to test access.
- You must have administrative access to PingFederate.

#### Create a PingFederate SP connection for Jamf Pro

- 1. Sign on to the PingFederate administrative console.
- 2. Create an SP connection for Jamf Pro in PingFederate:
  - Configure using Browser SSO profile SAML 2.0.
  - Set Partner's Entity ID to https://your-instance.jamfcloud.com/saml/metadata.
  - Enable the IdP-Initiated SSO and SP Initiated SSO SAML profiles.
    - In Assertion Creation → Authentication Source Mapping → Attribute Contract Fulfillment, map the SAML\_SUBJECT to your email attribute.
    - In Protocol Settings → Assertion Consumer Service URL, set Binding to POST and set Endpoint URL to https://your-instance.jamfcloud.com/saml/SS0.
    - In Protocol Settings → Allowable SAML Bindings, enable POST.
    - In Credentials → Digital Signature Settings, select the PingFederate Signing Certificate.
- 3. Export the metadata for the newly-created Jamf Pro SP connection.
- 4. Export the signing certificate.

#### Add the PingFederate connection to Jamf Pro

- 1. Sign on to the Jamf Pro console as an administrator.
- 2. Click the **Gear** icon (🏟]).
- 3. Go to System Settings  $\rightarrow$  Single Sign-On.



- 4. Click the **Edit** icon.
- 5. Select the Enable Single Sign-On Authentication check box.



- 6. In the Identity Provider list, select Ping Identity.
- 7. Confirm that the **Entity ID** value matches the value you set previously in PingFederate.
- 8. In the **Upload Metadata File** field, upload the PingFederate metadata file.

Single Sign-On Enable Single Sign-On Authentication Selecting this option prevents all other passwords from authenticating	ings : System Settings	
Enable Single Sign-On Authentication Selecting this option prevents all other passwords from authenticating  Pailover Login URL Users with Single Sign-On Update privileges can authenticate with a Jamf Pro user account by going to the following URL: Copy to clipboard https://pingnfr.jamfcloud.com/?faillover  Identity Provider Identity Provider Identity Provider SAML 2.0 identity provider to use for Single Sign-On Ping Identity  Total Com/saml/metadata Identity Provider Metadata Source Upload an identity provider metadata file or provide a metadata URL  Metadata File  Uploed Metadata File  Uploed Metadata File  The file must use .xml format.  Com Expiration (Minutes) Amount of time before the SAML token expires  480	Single Sign-On	
Enable Single Sign-On Authentication   Selecting this option prevents all other passwords from authenticating		
Selecting this option prevents all other passwords from authenticating  Pailover Login URL Users with Single Sign-On Update privileges can authenticate with a Jamf Pro user account by going to the following URL: Copy to dipboard https://pingnfr.jamfcloud.com/?failover  Identity Provider Identity Provider Identity Provider Identity Provider SAML 2.0 identity provider to use for Single Sign-On Ping Identity  To Name that identifies your Jamf Pro instance in the identity provider  Intty ID Name that identifies your Jamf Pro instance in the identity provider  Intty ID Name that identifies your Jamf Pro instance in the identity provider  Intty ID Name that Identifies your Jamf Pro instance in the identity provider metadata file or provide a metadata URL  Metadata File  Upload Metadata File  The file must use xml format.  Define and drop or Browse for a file Remove  Token Expiration (Minutes) Amount of time before the SAML token expires  480	Enable Single Sign-On Authentication	
Fallover Login URL Users with Single Sign-On Update privileges can authenticate with a Jamf Pro user account by going to the following URL: Copy to dipboard https://pingnfr.jamfcloud.com/?failover Identity Provider Edentity Provider SAML 2.0 identity provider to use for Single Sign-On Ping identity v Entity ID Name that identifies your Jamf Pro instance in the identity provider Ittps://pinglef.jamfcloud.com/sami/metadata Identity Provider Metadata Source Upload an identity provider metadata file or provide a metadata URL. Metadata File v Upload Metadata File The file must use xml format. Interdata (3).xml Token Expiration (Minutes) Amount of time before the SAML token expires 480	Selecting this option prevents all other passwords from authenticating	
Copy to dipboard https://pingnfr.jamfcloud.com/?failover  Identity Provider Identity Provider Identity Provider SAML 2.0 Identity provider to use for Single Sign-On Ping Identity  Entity ID Name that Identifies your Jamf Pro Instance in the Identity provider  Inttps://pii_fi_jamfcloud.com/samt/metadata Identity Provider Metadata Source Upload an Identity provider metadata file or provide a metadata URL  Metadata File  Upload Metadata File  Drag and drop or Browse for a file Remove  Token Expiration (Minutes) Amount of time before the SAML token expires  480	Failover Login URL Users with Single Sign-On Update privileges can au	thenticate with a Jamf Pro user account by going to the following URL:
Identity Provider Identity Provider SAML 2.0 identity provider to use for Single Sign-On Ping Identity   Entity ID Name that identifies your Jamf Pro instance in the identity provider Inttps://pinclimi.jamfcloud.com/saml/metadata Identity Provider Metadata Source Upload an identity provider metadata file or provide a metadata URL. Metadata File   Upload Metadata File The file must use xml format. Upload Metadata File The file must use xml format. Description of Browse for a file Remove Token Expiration (Minutes) Amount of time before the SAML token expires 480	Copy to clipboard https://pingnfr.jamfcloud.com/?failover	
Identity Provider SAML 2.0 identity provider to use for Single Sign-On          Ping Identity       •         Entity ID       Name that Identifies your Jamf Pro instance in the Identity provider         Inttps://pinclen_jamfcloud.com/saml/metadata         Identity Provider Metadata Source       Upload an identity provider metadata file or provide a metadata URL         Metadata File       •         Upload Metadata File       •         Upload Metadata File       •         Drag and drop or Browse for a file Remove         Token Expiration (Minutes)       Amount of time before the SAML token expires         [480]		
Identity Provider       SAML 2.0 identity provider to use for Single Sign On         Ping Identity <ul> <li>Entity ID</li> <li>Name that identifies your Jamf Pro instance in the identity provider</li> <li> <li>https://pinf_Bin_jamfcloud.com/saml/metadata       </li> <li>Identity Provider Metadata Source</li> <li>Upload an identity provider metadata file or provide a metadata URL.</li> <li>Metadata File        </li> <li>Upload Metadata File The file must use .xml format.</li> <li> <ul> <li>metadata (3).xml</li> <li>Drag and drop or Browse for a file Remove</li> <li>Taken Expiration (Minutes)</li> <li>Amount of time before the SAML token expires</li> <li>480</li> </ul> </li> </li></ul>	Identity Provider	
Ping Identity       •         Entity ID       Name that identifies your Jamf Pro instance in the identity provider         https://pin_tim_jamfcloud.com/saml/metadata         Identity Provider Metadata Source       Upload an identity provider metadata file or provide a metadata URL.         Metadata File       •         Upload Metadata File       The file must use xml format.         Image:	Identity Provider SAML 2.0 identity provider to use for Single Sign-On	
Entity ID Name that identifies your Jamf Pro Instance in the identity provider  https://plice_fr_jamfcloud.com/sami/metadata  Identity Provider Metadata Source Upload an identity provider metadata file or provide a metadata URL.  Metadata File  Upload Metadata File The file must use use format.  Define the file must use use for a file must use format.  Define the file must use file the file must use format.  Define the file must use file file the file must use file format.  Define the file must use format.  Define the file must use file file the file must use file file the file must use format.  Define the file file the file must use file file the file must use file file the file file the file file the file must use file file the file file file file file file file fil	Ping Identity -	
Entity ID Name that identifies your Jamf Pro instance in the identity provider  https://plicer.jamfcloud.com/saml/metadata  Identity Provider Metadata Source Upload an identity provider metadata file or provide a metadata URL  Metadata File  Upload Metadata File The file must use .xml format.  Upload Metadata File The file must use .xml format.  Drag and drop or Browse for a file Remove  Token Expiration (Minutes) Amount of time before the SAML token expires  480		
Inttps://pinc intigamfcloud.com/sami/metadata         Identity Provider Metadata Source       Upload an identity provider metadata file or provide a metadata URL.         Metadata File <ul> <li>Upload Metadata File</li> <li>The file must use .xml format.</li> <li>metadata (3).xml</li> <li>Drag and drop or Browse for a file Remove</li> <li>Token Expiration (Minutes) Amount of time before the SAML token expires</li> <li>480</li> </ul>	Entity ID Name that identifies your Jamf Pro instance in the identity provider	
Identity Provider Metadata Source Upload an identity provider metadata file or provide a metadata URL.  Metadata File  Upload Metadata File  The file must use .xml format.  Drag and drop or Browse for a file Remove  Token Expiration (Minutes) Amount of time before the SAML token expires  480	https://www.helloud.com/com/instadata	
Identity Provider Metadata Source       Upload an identity provider metadata file or provide a metadata URL.         Metadata File <ul> <li>Upload Metadata File</li> <li>The file must use .xml format.</li> <li>metadata (3).xml</li> <li>Drag and drop or Browse for a file Remove</li> <li>Token Expiration (Minutes)</li> <li>Amount of time before the SAML token expires</li> <li>480</li> </ul>	nttps://pii L iii .jamicloud.com/sami/metadata	
Metadata File       •         Upload Metadata File       The file must use xml format.	Identity Provider Metadata Source Unload an identity provider metadata file o	r provido a metadata I IDI
Wetadata File       *         Upload Metadata File       The file must use xml format.         Image: Im	Material Planet	i provinci o metopolito one
Upload Metadata File The file must use .xml format.	Metadata File 👻	
metadata (3).xml     Drag and drop or Browse for a file     Remove  Token Expiration (Minutes) Amount of time before the SAML token expires  480	Upload Metadata File The file must use xml format.	
metadata (3).xml     Drag and drop or Browse for a file     Remove  Token Expiration (Minutes) Amount of time before the SAML token expires  480		
Token Expiration (Minutes) Amount of time before the SAML token expires  480		
Image: Drag and drop or Browse for a file Remove         Token Expiration (Minutes)         Amount of time before the SAML token expires         480		metadata (3).xmi
Remove       Token Expiration (Minutes) Amount of time before the SAML token expires       480		Drag and drop or Browse for a file
Token Expiration (Minutes) Amount of time before the SAML token expires 480		Remove
Token Expiration (Minutes) Amount of time before the SAML token expires 480		
480		
480	Token Expiration (Minutes) Amount of time before the SAML token expires	
	480	

9. In the Jamf Pro User Mapping section, click Email.



10. In the Single Sign-On Options for Jamf Pro section, select the Allow users to bypass the Single Sign-On authentication check box.

Single Sign-On Options for Jamf Pro
Allow users to bypass the Single Sign-On authentication Users will be able to access the default Jamf Pro login page directly
Enable Single Sign-On for Self Service for macOS Allows Self Service to access any existing usernames from the identity provider
Enable Single Sign-On for User-Initiated Enrollment Allows users to enroll via the login page from the identity provider

### 11. Click Save.

## Test the PingFederate IdP-initiated SSO integration

- 1. Go to the PingFederate SSO application endpoint for the Jamf Pro SP connection.
- 2. Complete the PingFederate authentication.

You're redirected to your Jamf Pro domain.

## Test the PingFederate SP-initiated SSO integration

- 1. Go to your Jamf Pro application.
- 2. After you are redirected to PingFederate, enter your PingFederate username and password.

After successful authentication, you're redirected back to Jamf Pro.

## Configuring SAML SSO with Jamf Pro and PingOne for Enterprise

Enable Jamf Pro sign-on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct JAMF Pro sign-on using PingOne for Enterprise (SP-initiated sign-on) with single logout (SLO).

#### Before you begin

- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Populate Jamf Pro with at least one user to test access.
- You must have administrative access to PingOne for Enterprise.

## Add the Jamf Pro application to PingOne for Enterprise

- 1. Sign on to PingOne for Enterprise and go to Applications  $\rightarrow$  My Applications.
- 2. On the SAML tab, click Add Application.

		DASHBOARD	APPLICATIONS	USERS	SETUP	ACCOUNT		0	Sign Off
My Applications	Application Catalog	Pingid SDK A	pplications	OAuth Se	ttings				
My Applicati	ions								
SAML OIDC									
Applications you've • Active applicati • Details display:	e added to your account ions are enabled for sin s the application details	t are listed here. Y gle sign-on (SSO)	'ou can search ).	by applic	ation nar	me, description or e	ntityld		
Applicatio	on Name	Туре	Status		Enabl	ed			
Applicatio	on Name	Туре	Status		Enabl	ed		D	
Application -	ion Name	Туре	Status		Enabl	ed		Pause All SSO	ø
Application Add Application Search Applicat New SAML App	on Name tion Catalog	Туре	Status		Enabi	ied		Pause All SSO	9

## 3. Enter Jamf Pro as the application name.

- 4. Enter a suitable description.
- 5. Choose a suitable category.

## 6. Click Continue to Next Step.

7. Enter the following values:

Field	Value
Assertion Consumer Service (ACS)	https://your-instance.jamfcloud.com/saml/SSO
Entity ID	https://your-instance.jamfcloud.com/saml/metadata
Single Logout (SLO) Endpoint	https://your-instance.jamfcloud.com/saml/SingleLogout
Single Logout Binding Type	POST

You will need to download this SAML metada	ata to configure the application:
Signing Certificate	PingOne Account Origination Certificate (2021) 🗸
SAML Metadata	Download
Provide SAML details about the application y	you are connecting to:
Protocol Version	SAML v 2.0 ○ SAML v 1.1
Upload Metadata 🛛 😡	Select File Or use URL
Assertion Consumer Service (ACS)	https://pingntift.jamfcloud.com/saml/SSC
Entity ID 💿	https://µingmir.jamfcloud.com/saml/met
Application URL @	
Single Logout Endpoint @	https://µin @nir.jamfcloud.com/saml/Sinc
Single Logout Response Endpoint @	example.com/sloresponse.endpoint

- 8. On the SAML Metadata line, click Download.
- 9. Click Continue to Next Step.
- 10. Click Add new attribute.

3. SSO Attribute Mapping		
Map the necessary application	n provider (AP) attributes to attributes used by your iden	tity provider (IdP).
Application Attribute	Identity Bridge Attribute or Literal Value	Required
Add new attribute		

11. Add the **SAML\_SUBJECT** attribute and map it to your email attribute.

3. SSO Attrib	ute Mapping		
Map the	necessary application provider	(AP) attributes to attributes used by your identity provide	r (IdP).
	Application Attribute	Identity Bridge Attribute or Literal Value	Required
		Email (Work)	
1	SAML_SUBJECT	As Literal	□ ×

#### 12. Click Continue to Next Step.

13. Click **Add** for each user groups that should have access to JAMF Pro.

5. Group Access	
Select all user groups that should have access to this application. Users that are members of the added groups will b see this application on their personal dock.	e able to SSO to this application and wil
Group1, Group2, etc Search	
Crown Manna	
Users@directory	Remove
Demain Administratore @directory	
Domain Administration accuraciony	700

#### 14. Click Continue to Next Step.

15. Click Finish.

## Add the PingOne for Enterprise connection to JAMF Pro

- 1. Sign on to the Jamf Pro console as an administrator.
- 2. Click the **Gear** icon (🏟]).
- 3. Go to System Settings  $\rightarrow$  Single Sign-On.

Ę	ŝ	All Settings	System Set	tings	
Ī	100	System Settings	Jamf Pro User	Single Sign-	@ LDAP Servers
(		Global Management	Accounts & Groups	On	
	3	Jamf Applications			

4. Click the **Edit** icon.



5. Select the Enable Single Sign-On Authentication check box.

Settings : System Settings ← Single Sign-On
Enable Single Sign-On Authentication Selecting this option prevents all other passwords from authenticating

- 6. In the Identity Provider list, select Ping Identity.
- 7. Confirm that the **Entity ID** value matches the value you set previously in PingOne for Enterprise.
- 8. In the Upload Metadata File section, upload the PingOne for Enterprise metadata file.

Single Sign-On	
Enable Single Sign-On Authentication	
Selecting this option prevents all other passwords from authenticating	
Fallover Login URL Users with Single Sign-On Update privileges ca	in authenticate with a Jamf Pro user account by going to the following URL:
Copy to clipboard https://pingnfr.jamfcloud.com/?failov	/er
Identity Provider	
Identity Provider SAML 2.0 identity provider to use for Single Sign-On	
Ping Identity -	
Entity ID Name that identifies your Jamf Pro instance in the identity provide	r
https://pincim".jamfcloud.com/saml/metadata	
Identity Provider Metadata Source Upload an identity provider metadata f	ile or provide a metadata URL
Identity Provider Metadata Source Upload an identity provider metadata f Metadata File	lle or provide a metadata URL
Identity Provider Metadata Source Upload an identity provider metadata f Metadata File •	ile or provide a metadata URL
Identity Provider Metadata Source Upload an identity provider metadata f Metadata File  Upload Metadata File The file must use xml format.	lie or provide a metadata URL
Identity Provider Metadata Source Upload an identity provider metadata f Metadata File  Upload Metadata File The file must use .xml format.	lle or provide a metadata URL
Identity Provider Metadata Source Upload an identity provider metadata f Metadata File  Upload Metadata File The file must use comi format.	ile or provide a metadata URL
Identity Provider Metadata Source Upload an identity provider metadata f Metadata File  Upload Metadata File The file must use scml format.	ile or provide a metadata URL metadata (3).xml
Identity Provider Metadata Source Upload an identity provider metadata f Metadata File  Upload Metadata File The file must use .xml format.	lie or provide a metadata URL metadata (3).xml Drag and drop or Browse for a f Remove
Identity Provider Metadata Source Upload an identity provider metadata f Metadata File  Upload Metadata File The file must use comi format.	lie or provide a metadata URL metadata (3).xml Drag and drop or Browse for a f Remove
Identity Provider Metadata Source Upload an identity provider metadata f Metadata File  Upload Metadata File The file must use .xml format.	lie or provide a metadata URL metadata (3).xml Drag and drop or Browse for a f Remove
Identity Provider Metadata Source Upload an identity provider metadata f Metadata File  Upload Metadata File The file must use .xml format.  Token Expiration (Minutes) Amount of time before the SAML token expires	lie or provide a metadata URL metadata (3).xml Drag and drop or Browse for Remove

9. In the Jamf Pro User Mapping section, click Email.



10. In the Single Sign-On Options for Jamf Pro section, select the Allow users to bypass the Single Sign-On authentication check box.

Sir	igle Sign-On Options for Jamf Pro	
~	Allow users to bypass the Single Sign-On authentication Users will be able to access the default Jamf Pro login page directly	
	Enable Single Sign-On for Self Service for macOS Allows Self Service to access any existing usernames from the identity	provider
	Enable Single Sign-On for User-Initiated Enrollment Allows users to enroll via the login page from the identity provider	

11. Click Save.

## Test the PingOne for Enterprise identity provider (IdP)

1. Go to your Ping desktop as a user with Jamf Pro access.

### (i) Note

To find the Ping desktop URL, in the PingOne admin console, go to **Setup**  $\rightarrow$  **Dock**  $\rightarrow$  **PingOne Dock URL**.

2. Complete the PingOne authentication.

🗖 jamf	PRO			
Computers	[] Devices	لکے) Users	SET LOGIN SCREEN MESSAGE	
version 10.27.0-t16	612450030		0.2%	ALL CLIENTS: MACOS 10.11 OR GREATER

You're redirected to your Jamf Pro application.

#### Test the PingOne for Enterprise service provider (SP)

- 1. If you are using PingOne for Enterprise as the standard authentication method for Jamf Pro access, sign on to the Jamf Pro console as an administrator after you've completed PingOne for Enterprise IdP testing.
- 2. Go to Settings → System Settings → Single Sign-On and click Edit.



3. Clear the Allow users to bypass the Single Sign-On authentication check box.

Single	Sign-On Options for Jamf Pro
Allow Users	v users to bypass the Single Sign-On authentication s will be able to access the default Jamf Pro login page directly
Allow	ole Single Sign-On for Self Service for macOS s Self Service to access any existing usernames from the identity provider
Allow	ole Single Sign-On for User-Initiated Enrollment s users to enroll via the login page from the identity provider

#### 4. Click Save.

5. Go to your Jamf Pro application.

┛ jamt	f			
Computers	[ Devices	L) Users	SET LOGIN SCREEN MESSAGE	
version 10.27.0-t1	612450030		0.2%	ALL CLIENTS: MACOS 10.11 OR GREATER

You're redirected to PingOne for Enterprise.

6. Enter your PingOne for Enterprise username and password.

After successful authentication, you're redirected back to Jamf Pro.

# Jira/Confluence

## Configuring SAML SSO with Jira/Confluence and PingFederate

Learn how to configure SAML single sign-on with Jira/Confluence on premise and PingFederate.

#### About this task

The following table details the required and optional attributes to be configured in the assertion attribute contract.

Attribute Name	Description	Required / Optional
SAML_SUBJECT	Username	Required

#### Create a PingFederate SP Connection for Jira/Confluence

#### γ Νote

The following configuration is untested and is provided as an example. Additional steps might be required.

- 1. Sign on to Atlassian application as an administrator and go to Administration  $\rightarrow$  System  $\rightarrow$  SAML Authentication.
- 2. Select SAML Single Sign Onand note the Audience URL (Entity ID) and Assertion Consumer Service URL values.
- 3. Download the signing certificate.
- 4. Sign on to the PingFederate administrative console.
- 5. Using the details retrieved from the Atlassian application UI:
  - 1. Configure using Browser SSO profile SAML 2.0.
  - 2. Enable IdP-Initiated SSO and SP Initiated SSO.
  - 3. In Assertion Creation: Attribute Contract, set the Subject Name Format to urn:oasis:names:tc:SAML: 1.1:nameid-format:unspecified.
  - 4. In the Assertion Creation: Attribute Contract Fulfilment, map the attribute SAML\_SUBJECT to the attribute username.
  - 5. In Protocol Settings: Allowable SAML Bindings, enable Post and Redirect.
- 6. Export the metadata for the newly-created SP connection.
- 7. Export the signing certificate public key.

#### Configure the PingFederate IdP connection for Jira/Confluence on premise

- 1. Sign on to Atlassian application as an administrator and go to Administration  $\rightarrow$  System  $\rightarrow$  SAML Authentication.
- 2. Select SAML Single Sign-On.
- 3. Configure the following.

Setting	Value
Single sign-on issuer	The issuer ID for your PingFederate instance. You can retrieve this from the metadata that you downloaded.
Identity provider single sign-on URL	The PingFederate <b>SingleSignOnService</b> URL. You can retrieve this from the metadata that you downloaded. For example, https://hostname:port/idp/SS0.saml2
X509 Certificate	Upload the PingFederate signing public certificate.
Login Mode	Choose whether SAML is primary or secondary authentication.

Configuration is complete.

## Configuring SAML SSO with Jira/Confluence and PingOne for Enterprise

Learn how to configure SAML single sign-on (SSO) with Jira/Confluence on premise and PingOne for Enterprise.

#### About this task

The following table details the required and optional attributes to be configured in the assertion attribute contract.

Attribute Name	Description	Required / Optional
SAML_SUBJECT	Username	Required

#### 🕥 Note

A predefined application exists in the application catalog for use with Atlassian Cloud. It is recommended that this is used for Atlassian Cloud integrations.

#### Create a PingOne for Enterprise application for Jira/Confluence on premise

#### (i) Note

The following configuration is untested and is provided as an example. Additional steps might be required.

1. Sign on to the Atlassian application as an administrator and go to Administration  $\rightarrow$  System  $\rightarrow$  SAML Authentication.

- 2. Select SAML Single Sign On and note the Audience URL (Entity ID) and Assertion Consumer Service URL values.
- 3. Download the signing certificate.
- 4. Sign on to PingOne for Enterprise and click **Applications**.
- 5. On the SAML tab, click Add Application.
- 6. Click New SAML Application.

SAML OI	DC						Î
Applications yo • Active appl • Details disp	uive added to your account are liste ications are enabled for single sign- plays the application details.	ed here. You can search on (SSO).	by application name, d	escription or entityId			ł
	Application Name	Туре	Status	Enabled			
*Ь	BambooHR	SAML	Active	Yes	Remove		
ьох	Box	SAML	Active	Yes	Remove		
	Dropbox	SAML	Active	Yes	Remove		
	simpleSAMLphp	SAML	Active	Yes	Remove		
>	Splunk Cloud	SAML	Active	Yes	Remove		
Add Applicati Search App New SAML/ Request Pir	on	the application catalog			Pause All SSO	Θ	

7. In the **Application Details** section, enter the following:

- A suitable application name, such as Confluence.
- A suitable description.
- A suitable category, such as **Information Technology**.
- (Optional) Upload an icon to be used in the PingOne for Enterprise dock.

P	Ping	Dne - I	My Applications × +					-	t	1	×
←	$\rightarrow$	G	admin.pingone.com/web-portal/cas/connections#/						*	θ	:
			New Application	SAML	Incomplete	NO					^
			1. Application Details								
			Application Name	Confluence	x						
			Application Description	Atlassian Confluence							ļ
				M	.4 lax 500 characters						
			Category	Information Technology	*						
			Graphics	Application Icon For use on the dock Network Acatastic Change							
											-

8. Click Continue to Next Step.

9. Select I have the SAML configuration.

10. In the **Signing Certificate list**, select a suitable signing certificate.

11. For Protocol Version, click SAML v.2.0.

12. In the Assertion Consumer Service (ACS) field, enter the ACS value from the Atlassian single sign-on settings.

13. In the Entity ID field, enter the Entity ID value from the Atlassian single sign-on settings.

14. For **Primary Verification Certificate**, select the signing certificate that you downloaded.

ſ	P1 PingOne -	My Applications × +		-			×	
•	← → C	admin.pingone.com/web-portal/cas/connection	ns#/	☆	*	0	) :	
		Signing Certificate @	PingOne Account Origination Certificate (2021) 🗸					^
		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 🛛 🛛	Select File Or use URL					
		Assertion Consumer Service (ACS)	•					
		Entity ID @	•					l
		Application URL @						
		Single Logout Endpoint @	example.com/silo.endpoint					
		Single Logout Response Endpoint @						
		Single Logout Binding Type @	⊖ Redirect ⊖ Post					
		Primary Verification Certificate	Choose File					
		Secondary Verification Certificate @	Choose File No file chosen					
		Encrypt Assertion @						
		Signing @	Sign Assertion ○ Sign Response					
								٠

#### 15. Click Continue to Next Step.

16. In the SSO Attribute Mapping section, add the following mapping for the SAML\_SUBJECT:

- For **Identity Bridge Attribute or Literal Value**, select the appropriate attribute. This should match the username for the user in the application.
- Select the **Required** check box.
| PingOne - My Applications × +  | - 0       | ×   |
|--|-----------|-----|
| ← → C 🔒 admin.pingone.com/web-portal/cas/connections#/   | * 8       | ) E |
| simpleSAMLphp SAML Active Yes Remove   |           | ^   |
| Splunk Cloud SAML Active Yes Remove  |           |     |
| New Application SAML Incomplete No   |           |     |
| 3. SSO Attribute Mapping<br>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 |
| Username   |           |     |
| 1 SAML_SUBJECT   |           |     |
| Add new attribute NEXT: Group Access Cancel Back Continue to Next Step Save & Exit   |           |     |
| © 2003 - 2021 Ping Identity Corporation. All rights reserved. Privacy I Term   | s   About |     |

18. Add the user groups for the application.

A. Group Access  Select all user groups that should have access to this application. Users that are members of the added groups will be able to SSO to this application and will  foroup1, Group2, etc  foroup Name Domain Administrators@directory Users@directory Remove R	- > G	🗎 ad	min.pingone.com/web-portal/cas/connections#/	1	<u>ل</u> ا م	• \varTheta	:	
Select all user groups that should have access to this application. Users that are members of the added groups will be able to SSO to this application and will see this application on their personal dock.         Group 1, Group 2, etc       Search         Domain Administrators@directory       Remove         Users@directory       Remove         Wass@directory       Remove		4. G	roup Access					
Group 1, Group 2, etc       Search         Group Name       Remove         Domain Administrators@directory       Remove         Users@directory       Remove         Users@directory       Remove			Select all user groups that should have access to this application. Users that are members of the added groups will be able to SSC see this application on their personal dock.	) to this applicati	on and	will		
Group Name       Remove         Domain Administrators@directory       Remove         Users@directory       Remove			Group 1, Group 2, etc Search					
Domain Administrators@directory     Remove       Users@directory     Remove			Group Name					
Users@directory Remove Remove Continue to Next Step			Domain Administrators@directory	Remove	]			
NEXT: Review Setup Continue to Next Step			Users@directory	Remove	]			
NEXT: Review Setup Continue to Next Step								
NEXT: Review Setup Continue to Next Step								
NEXT: Review Setup Continue to Next Step								
NEXT: Review Setup Continue to Next Step				_		_		
		NEXT: Review Setup						

20. Review the settings.

PingOne - My Applications × +		_	[		×	
$\leftrightarrow$ $\rightarrow$ C $($ admin.pingone.com/web-portal/cas/connection	ns#/	☆	*	θ	:	
Test your connection to the application						•
Icon	e					
Name	Confluence					
Description	Atlassian Confluence					
Category	Information Technology					
Connection ID						
(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 confid	Jure your connection					
saasid						
Issuer	https://pingone.com/idp/					
idpid						
Protocol Version	SAML v 2.0					
ACS URL @						
entityld @						
Initiate Single Sign-On (SSO) URL @	https://sso.connect.pingidentity.com/sso/sp/initsso					
Single Sign-On (SSO) Relay State @	https://pingone.com/1.0/					
Signing Certificate @	Download					
SAML Metadata	Download					
SAML Metadata URL						Ŧ

21. Copy the Single Sign-On (SSO) URL value to a temporary location.

This is the IdP-initiated SSO URL that you can use for testing.

22. Note the **idpid** and **Issues** values.

#### 23. On the Signing Certificate line, click Download.

You'll use this for the application configuration.

#### 24. On the SAML Metadata line, click Download.

You'll use this for the application configuration.

25. Click Finish.

#### Configure the PingOne for Enterprise IdP Connection for Jira/Confluence on-premise

- 1. Sign on to the Atlassian application as an administrator.
- 2. Go to Administration  $\rightarrow$  System  $\rightarrow$  SAML Authentication.
- 3. Select SAML Single Sign On.
- 4. Configure the following.

Setting	Value
Single sign-on issuer	The issuer from PingOne for Enterprise application details noted earlier.
Identity provider single sign-on URL	Enter the <b>Single Sign-On Service URL</b> in the following form, using the idpid previously noted. <a href="https://sso.connect.pingidentity.com/sso/idp/SS0.saml2?idpid=idpid">https://sso.connect.pingidentity.com/sso/idp/SS0.saml2?idpid=idpid</a> Alternatively, you can retrieve the URL from the metadata that you downloaded.
X509 Certificate	Upload the PingOne for Enterprise signing public certificate that you downloaded.
Login Mode	Choose whether SAML is your primary or secondary authentication.

Configuration is complete.

# Jive

# **Configuring SAML SSO with Jive and PingFederate**

Learn how to configure SAML SSO with Jive and PingFederate.

#### About this task

The following table details the references that are used within this guide that are environment specific. Replace these with the suitable value for your environment.

Reference	Description
jiveinstance	The host and port for the Jive instance.

#### ) Note

The following configuration is untested and is provided as an example. Additional steps might be required.

#### **Create the PingFederate SP Connection for Jive**

- 1. Sign on to the Jive Admin Console and enable single sign-on:
  - 1. Go to People  $\rightarrow$  Settings  $\rightarrow$  Single Sign-On  $\rightarrow$  SAML.
  - 2. Check Enabled.
  - 3. Click Save.
  - 4. Restart Jive.

#### (i) Note

Until SAML configuration is complete, you'll need to sign on by going directly to the admin console, http://jiveinstance/admin.

- 2. Download the Jive metadata from http://jiveinstance/saml/metadata .
- 3. Sign on to the PingFederate administrative console.
- 4. Using the metadata that you downloaded, create an SP connection in Ping Federate:
  - 1. Configure using Browser SSO profile SAML 2.0.

- 2. Enable the following SAML Profiles:
  - IdP-Initiated SSO
  - SP-Initiated SSO
- 3. In Assertion Creation: Attribute Contract, set the Subject Name Format to urn:oasis:names:tc:SAML: 1.1:nameid-format:unspecified.
- 4. In the Assertion Creation: Attribute Contract Fulfilment, map the attribute SAML\_SUBJECT to the attribute username.
- 5. Add any additional attributes required into the attribute contract and contract fulfillment.
- 6. In Protocol Settings: Allowable SAML Bindings, enable POST, and Redirect.
- 5. Export the metadata for the newly-created SP connection.
- 6. Export the signing certificate public key.

#### Configure the PingFederate IdP connection for Jive

- 1. Sign on to the Jive Admin Console and go to People  $\rightarrow$  Settings  $\rightarrow$  Single Sign-On  $\rightarrow$  SAML.
- 2. On the IdP Metadata tab, copy the contents of the metadata file into the metadata field.
- 3. Click Save All SAML Settings.
- 4. On the **User Attribute Mapping** tab, map the user attributes in the Jive profile to the attributes that you configured in PingFederate.
- 5. **Optional:** Select **Group Mapping Enabled** if you want to assign users to groups with a group attribute passed in the assertion.
- 6. Click Save Settings.

## Configuring SAML SSO with Jive and PingOne for Enterprise

Learn how to configure SAML SSO with Jive and PingOne for Enterprise.

#### About this task

The following table details the references that are used within this guide that are environment specific. Replace these with the suitable value for your environment.

Reference	Description
jiveinstance	The host and port for the Jive instance.

#### ) Note

The following configuration is untested and is provided as an example. Additional steps might be required.

#### Create a PingOne for Enterprise Application for Jive

- 1. Sign on to the Jive Admin Console and enable single sign-on:
  - 1. Go to People  $\rightarrow$  Settings  $\rightarrow$  Single Sign-On  $\rightarrow$  SAML.
  - 2. Check Enabled.
  - 3. Click Save.
  - 4. Restart Jive.

#### 🕥 Note

Until SAML configuration is complete, you'll need to sign on by going directly to the admin console, http://jiveinstance/admin.

- 2. Download the Jive Metadata from http://jiveinstance/saml/metadata.
- 3. Sign on to PingOne for Enterprise and click Applications.
- 4. On the SAML tab, click Add Application.

PingOne - My Applications × +	-		×
← → C admin.pingone.com/web-portal/cas/connections#/	☆	Θ	:
PingOne' dashboard Applications users setup account (?)	Sign Of	0	í
My Applications Application Catalog PingID SDK Applications OAuth Settings			
My Applications          SAML       OIDC         Applications you've added to your account are listed here. You can search by application name, description or entityld         • Active applications are enabled for single sign-on (SSO).         • Details displays the application details.			
Application Name         Type         Status         Enabled           Use the button below to add your first application.         Item (Content on the content o			
Add Application - Pause All SSO	Θ		
Search Application Catalog New SAML Application			1
Request Ping Identity add a new application to the application catalog			

- 5. Click Search Application Catalog and search for Jive.
- 6. Click the Jive Production row or click Jive UAT for a non-production environment.

Pı	PingOne - Application Catalog	× +					-		×
÷	→ C  admin.ping	one.com/web-portal/cas	/applicationcatalog				☆	* 6	) E
	<b>Ping</b> One"		DASHBOARD APPLICATI	ONS USERS SETUP ACO		0	Sig	n Off	Î
	My Applications	Application Catalog	PingID SDK Application	s OAuth Settings					
	Application	Catalog			Applications	/ Application Catalog			
	Browse for the applic	ation you want to add or s	earch for it by name. Don't	see the application you're look	ing for? Fill out our Application Reque	st Form.			
	jive		Search						
		Application Name	* T	ype					
	jive	Jive - Production		SAML with Provisioning (AP	1)	►			
	jive	Jive - UAT		SAML with Provisioning (AP	I)	►			

#### 7. Click Setup.

- 8. Select the appropriate signing certificate from the list.
- 9. Review the steps, and note the PingOne for Enterprise SaaS ID, IdP ID, Single Sign-on URL, and Issuer values.

#### 10. Click Continue to Next Step.

11. On the **Upload Metadata** row, click **Select File**, and upload the Jive metadata file that you previously downloaded.

P1 PingOne	e - Application Catalog × +		-		×	
$\leftrightarrow \rightarrow c$	admin.pingone.com/web-portal/cas/applicati	oncatalog?x=zeH0IEk6qHA	*	0	) :	
	2. Connection Configuration					*
	Assign the attribute values for single sig	n-on (SSO) to the application.				
	Upload Metadata 🛛 😡	Select File Or use URL				
	ACS URL	Replace the parameter(s) "\$(customer.name)" above with your configuration information.				l
	Entity ID	Replace the parameter(s) '\$(customer.name)' above with your configuration information.				
	Target Resource @					
	Single Logout Endpoint @	example.com/slo.endpoint				
	Single Logout Response Endpoint @	example.com/sloresponse.endpoint				
	Primary Verification Certificate @	Choose File				
	Secondary Verification Certificate @	Choose File No file chosen				
	Force Re-authentication @					
	Encrypt Assertion @					
	Signing @	● Sign Assertion ○ Sign Response				
	Signing Algorithm @	RSA_SHA256 V				-

- 12. Click Continue to Next Step.
- 13. In the **Attribute Mapping** section, complete the attribute mappings as required.

P1	PingOn	e - Applicatio	n Catalog	× +			-	. [		×
←	$\rightarrow$ (	C 🔒 ad	lmin.ping	one.com/web-portal/cas	/applicationcatalog?x=zeH0IEk6qHA		☆	*	Θ	:
				Application Name	^ Туре					*
		jive		Jive - Production	SAML with Pro	vvisioning (API)				
		3. Att	tribute M Map you	lapping r identity bridge attribu	tes to the attributes required by the ap	plication.				l
				Application Attribute	Description	Identity Bridge Attribute or Literal Value				I
			1	sAMAccountName *	Map your account name attribute	Usemame As Literal Advanced				
			2	givenName *	First Name: givenName in AD	First Name				
			3	sn	First Name: givenName in AD	Last Name				
	4	mail	Email address: mail in AD	Email (Work)						
			5	objectGUID	ObjectGuid: objectGUID in AD	Name or Literal				
										*

15. Update the Name, Description, and Category fields as required.

P1 Ping	One - Application Catalog × +		-		×	
$\leftrightarrow$ $\rightarrow$	C admin.pingone.com/web-portal/cas/application	icatalog?x=zeH0IEk6qHA	☆	* (	<b>)</b> :	
	Application Name	* Туре				*
	Jive - Production	SAML with Provisioning (API)				
	4. PingOne App Customization - Jive - Producti	ion				
	Icon @	jive				
	Name @	Select image Jive - Production *				
	Description @	* Jive combines powerful features of customer community software, collaboration software, social networking & social media monitoring into the leading social business solution.				
	Category @	Collaboration 🗸				
	NEXT: Group Access	Cancel Back Continue to Next Step				+

17. Add suitable user groups for the application.

P	1 Ping	One - /	Applicatio	n Catalog 🛛 🗙	+						-	- [	]	×
~	$\rightarrow$	С	🗎 ad	lmin.pingone.	com/web-porta	l/cas/applicatio	oncatalog	?x=zeH0IEk	k6ql	HA	☆	*	0	:
					Application	Name		<b>^</b>	۰٦	Туре				
			jive		Jive - Pro	duction				SAML with Provisioning (API)				
			5. Gr	oup Access Select all user see this applic	groups that sh ation on their p	ould have acce ersonal dock.	ess to this	applicatior	n. U	Isers that are members of the added groups will be able to SSO to the	s applicatio	n and w	ill	ļ
				Group1, C	Group2, etc			Search						l
			1	Group Nam	e									
				Domain Adı	ministrators@di	irectory					Rem	ove		I
				Users@dire	ectory						Rem	ove		l
														l
4														+

19. Review the settings.

P	PingO	ne - Application Catalog 🛛 🗙	+		-		×
←	$\rightarrow$	C 🏻 admin.pingone.co	m/web-portal/cas/application	catalog?x=zeH0IEk6qHA	☆	* 6	<b>3</b> :
		A	Application Name	<b>^</b> Туре			*
		jive	Jive - Production	SAML with Provisioning (API)			
		6. Review Setup					
		Test your conne	ection to the application				
			Icon @	jive			1
			Name @	Jive - Production			
			Description @	Jive combines powerful features of customer community software, collaboration software, social networking & social media monitoring into the leading social business solution.			
			Category @	Collaboration			
			Connection ID				
		You may need	to configure these connect	tion parameters as well.			
			saasid				
			idpid				
			lssuer				-

P1	PingO	ine - /	Application Catalog × +		-			×
←	$\rightarrow$	G	admin.pingone.com/web-portal/cas/applicatio	ncatalog?x=zeH0IEk6qHA	\$	*	θ	:
			Encrypt Assertion @	) false				*
			ACS URL					
			SP entityld					
			Initiate Single Sign-On (SSO) URL	https://sso.connect.pingidentity.com/sso/sp/initssc				
			Single Sign-On (SSO) Relay State					
			Single Logout Endpoint	t				
			Single Logout Response Endpoint	t				
			Force Re-authentication	alse				
			Signing Certificate	Download				
			SAML Metadata	Download				
			SAML Metadata URL	https://admin-api.pingone.com/latest/metadata				
			Application Attribute	Identity Bridge Description Attribute or Literal Value				
			1 sAMAccountName *	Map your account name attribute Username				
			2 givenName *	First Name: givenName in AD First Name				-

20. Copy the Single Sign-On (SSO) URL value to a temporary location.

This is the IdP-initiated SSO URL that you can use for testing.

- 21. On the **Signing Certificate** row, click **Download**. You'll use this for the Jive configuration.
- 22. On the **SAML Metadata** row, click **Download**. You'll use this the Jive configuration.
- 23. Click Finish.

#### Configure the PingOne for Enterprise IdP connection for Jive

- 1. Sign on to the Jive Admin Console and go to **People**  $\rightarrow$  **Settings**  $\rightarrow$  **Single Sign-On**  $\rightarrow$  **SAML**.
- 2. On the IdP Metadata tab, copy the contents of the metadata file into the metadata field.
- 3. Click Save All SAML Settings.
- 4. On the **User Attribute Mapping** tab, map the user attributes in the Jive profile to the attributes configured in PingOne for Enterprise.
- 5. Optional: Select Group Mapping Enabled if you want to assign users to groups using a group attribute passed in the assertion.
- 6. Click Save Settings.

# **Lookout Secure Access**

## **Configuring SAML SSO with Lookout Secure Access**

The Ping Identity and Lookout SAML integration supports service provider (SP) and identity provider (IdP) initiated single sign-on (SSO).

#### What it is

Lookout Cloud Security (Lookout SSE platform) is a data-centric cloud security solution that protects users from internet-based threats and protects data stored in cloud applications, private applications, and websites.

Lookout Cloud Security supports the following cloud security components:

#### Lookout Secure Internet Access

Protection for web or non-web internet-based traffic.

#### Lookout Secure Private Access

Protection for private application traffic.

#### Lookout Secure Cloud Access

Protection for cloud application traffic.

#### i) Note

Users must authenticate with your enterprise SSO provider during their initial access before accessing solutions such as Secure Internet Access and Secure Cloud Access.

The Lookout Cloud Security platform leverages the user or user group context to enforce access and activity policies on cloud apps, private apps, and websites.

#### What you'll need

- Have a PingOne account. Learn more in Starting a PingOne trial .
- Verify that you can sign on to the PingOne admin console. Learn more in Accessing the PingOne admin console
- Have a Lookout SSE platform account. To enroll in a Lookout SSE platform account, contact Lookout

#### What you'll do

To configure SAML SSO with Lookout Secure Access:

- 1. Gather the service provider (Lookout Secure Access) metadata.
- 2. Configure the service provider in PingOne.
- 3. Configure the identity provider (PingOne) in Lookout.
- 4. Enable SSO for the Lookout management console, endpoint client, and proxy authentication.
- 5. Configure IdP-initiated sign-on for Lookout management console.
- 6. Test SSO with Lookout Secure Access.

#### Step 1: Gather the SP metadata

To use PingOne as an IdP, you'll capture SAML values from the Lookout Management console:

- 1. In the Lookout Management console, go to Administration  $\rightarrow$  Enterprise Integration.
- 2. Go to Configuration  $\rightarrow$  Single Sign-On.
- 3. On the **SSO Groups** tab, go to the default group.
- 4. In the SP Metadata column, click the Download icon.
  - The SP Metadata window opens.
- 5. Copy the Assertion Consumer Service (ACS) URL and Entity ID values.

#### Step 2: Configure the SP in PingOne

After you've captured the SAML values from Lookout Secure Access, you'll configure a SAML-based application in PingOne. This gives PingOne the information it needs to communicate with the Lookout Cloud Security Platform so that the platform can enforce policies based on user credentials.

- In the PingOne admin console, go to Applications → Application Catalog and browse or search for Lookout Secure Access.
- 2. Click the Lookout Secure Access entry to open the details panel.
- 3. For Quick Setup, enter the following information:
  - ACS URL: Enter the Assertion Consumer Servicevalue that you copied previously.
  - Entity ID: Enter the Entity ID value that you copied previously.
- 4. Click Next.
- 5. On the Map Attributes page, click Next.
- 6. On the Select Groups page, click Savewithout assigning groups.

This allows users to have access to all applications by default.

i) Note

Assign groups to the application to restrict access to only those groups.

- 7. In Application Instances, select the Lookout Secure Access Application entry to open the Connection Details page.
- 8. On the Connection Details page, copy the IDP Metadata URL to use when configuring the SP.

#### Step 3: Configure the IdP in Lookout

Next, you'll link your PingOne instance to the Lookout Cloud Security Platform by configuring a new IdP instance. Lookout uses to retrieve user information from PingOne.

- 1. In the Lookout Management Console, go to **Administration**  $\rightarrow$  **Enterprise Integration**.
- 2. Go to Configuration  $\rightarrow$  Single Sign-On.
- 3. On the SSO Providers tab, click New.
- 4. Enter or select the following values:
  - Name: Enter a name that contains no more than 255 characters.
  - Type: Select Identity Provider.
  - SSO Group: Select Default.
  - Metadata Link: Enter the IDP Metadata URL value that you copied from the PingOne.
- 5. Click Validate and confirm that the Management Console populates the Entity ID field.
- 6. Click Save.

#### Step 4: Enable SSO for the Lookout management console, endpoint client, and proxy authentication

After you've configured the service provider, you'll enable SSO for the Lookout Cloud Security Platform.

- 1. In the Lookout Management Console, go to Administration → System Settings → Enterprise Authentication.
- 2. In the Identity Provider list, choose the IdP that you created.
- 3. To enable the Management SSO, click the toggle.
- 4. To enable the **Endpoint**, click the toggle.

#### ) Note

The Native Proxy Authentication toggle is enabled by default and cannot be disabled.

5. Click Save.

#### Step 5: Configure IdP-initiated sign-on for Lookout management console

Next, to set up IdP-initiated sign-on for the Lookout Management Console, you'll configure relay state on PingOne.

- 1. In the Lookout Management Console, go to Administration → System Settings → Enterprise Authentication.
- 2. In the Enterprise Single Sign-on Settings field, click Copy to copy the Relay State value.
- 3. In the PingOne admin console, go to **Applications**  $\rightarrow$  **Applications**.
- 4. Click the Lookout Secure Access entry.
- 5. On the Overview tab, click Enable Advanced Configuration.
  - The Enable Advanced Configuration window opens.
- 6. Click Enable.
- 7. On the **Configuration** tab, click on the **Pencil** icon to edit the **Connection Details**.
- 8. In the Target Application URL field, paste the Relay State value that you copied from the Lookout Management Console.

9. Click Save.

#### Step 6: Test SSO with Lookout Secure Access.

After you've configured IdP-initiated sign-on, you'll verify that SSO works.

- 1. In the PingOne admin console, go to **Applications**  $\rightarrow$  **Applications**.
- 2. Click the Lookout Secure Access entry.
- 3. On the **Configuration** tab, copy the **Initiate Single Sign-On URL** value.
- 4. Paste the URL in a new browser window and hit enter.

You are successfully redirected to the Lookout Management Console.

# **Configuring SAML SSO with Marketo and PingFederate**

Learn how to enable Marketo sign-on from PingFederate (IdP-initiated sign-on).

#### Before you begin

- Configure PingFederate to authenticate against an identity provider (IdP) or datastore containing the users requiring application access.
- Populate Marketo with at least one user to test access.
- You must have administrative access to PingFederate.

#### **Obtain your Munchkin Account ID**

- 1. Sign on to the Marketo console as an administrator.
- 2. Select Admin in the toolbar.
- 3. Select Intergration in the left-hand pane.
- 4. Copy and Save your Munchkin Account ID.

#### Create an SP connection for Marketo in PingFederate

- 1. Sign on to PingFederate.
- 2. Configure using Browser SSO profile SAML 2.0.
- 3. Set Partner's Entity ID to https://www.marketo.com/SAML/your-Munchkin-account-ID.
- 4. Enable the IDP-initiated SSO SAML Profile.

#### (i) Note

Marketo does not currently support SP-initiated SSO.

- 5. In Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfillment, map the SAML\_SUBJECT to your email attribute.
- 6. In Protocol Settings: Assertion Consumer Service URL, set Binding to POST and set Endpoint URL to https:// login.marketo.com/saml/assertion/your-Munchkin-account-ID.
- 7. In Protocol Settings: Allowable SAML Bindings, enable POST.
- 8. In Credentials: Digital Signature Settings, select the PingFederate Signing Certificate and download it.

#### **Enable SAML SSO in Marketo**

- 1. Sign on to the Marketo console as an administrator.
- 2. Select Admin in the toolbar.
- 3. Select **Other Stuff** in the left navigation pane.
- 4. Select Single Sign-On.

#### (j) Note

If you don't see Single Sign-On, contact support@marketo.com to enable SAML for your account.

- 5. Next to SAML Settings, select Edit.
- 6. For the Issuer ID, enter the value you entered for the IdP Entity ID in PingFederate.
- 7. For the Entity ID, enter the value you entered for the IdP Entity ID in PingFederate.
- 8. For the User ID Location, click the In Name identifier element of Subject.
- 9. Click Browse next to Identity Provider Certificate and upload your public certificate.
- 10. Click Save.

#### Test the PingFederate IdP-initiated SSO Integration

- 1. Go to the PingFederate SSO Application Endpoint for the Marketo SP connection.
- 2. Authenticate with PingFederate.

You're redirected to your Marketo domain.

#### Configuring SAML SSO with Marketo and PingOne

Learn how to enable Marketo sign-on from PingOne (IdP-initiated sign-on).

#### Before you begin

- Link PingOne to an identity repository containing the users requiring application access.
- Populate Marketo with at least one user to test access.
- Gather your Munchkin Account ID.
- You must have administrative access to PingOne and an admin account on Marketo.

#### Add the Marketo Application to PingOne

1. In PingOne, go to **Connections**  $\rightarrow$  **Applications** and click the + icon.



- 2. When you're prompted to select an application type, select **WEB APP** and then click **Configure** next to **SAML** for the chosen connection type.
- 3. Enter Marketo as the application name.
- 4. Enter a suitable description.
- 5. Optional: Upload an icon.
- 6. Click Next.
- 7. For Provide App Metadata, select Enter Manually.
- 8. For ACS URLS, enter https://login.marketo.com/saml/assertion/your-Munchkin-account-ID.
- 9. For EntityID enter https://login.marketo.com/saml/your-Munchkin-account-ID.
- 10. Choose the Signing Key to use and then click Download Signing Certificate to download as X509 PEM (.crt).
- 11. Leave SLO Endpoint and SLO Response Endpoint blank.
- 12. In the Subject NameID Format list, select urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress.
- 13. Enter a suitable value for Assertion Validity Duration (in seconds). A value of 300 seconds is typical.
- 14. Click Save and Continue.
- 15. Marketo expects an email address to identify a user in the SSO security assertion:
  - $\circ\,$  If you use an email address to sign on through PingOne, click Save and Close.
  - If you sign on with a username, in the **PingOne User Attribute** list, select **Email Address** to map that to the **SAML\_SUBJECT**, then click **Save and Close**.

16. Click the toggle to enable the application.

17. On the Configuration tab of the newly-created Marketo application, copy and save the IDP Metadata URL value.

You'll need this when configuring SAML on Marketo.

^	CONNECTION DETAILS		
	DOWNLOAD METADATA:	Download	
	ISSUER ID :	https://auth.pingone.eu	
	SINGLE LOGOUT SERVICE:	https://auth.pingone.eu	saml20/idp/slo
	SINGLE SIGNON SERVICE:	https://auth.pingone.eu	saml20/idp/sso
	IDP METADATA URL:	https://auth.pingone.eu	saml20/metadata/852de8c0-3f8d-4fa9-a405-74c5345f9d28
	INITIATE SINGLE SIGN-ON URL:	https://auth.pingone.eu	saml20/idp/startsso?spEntityId=https://login.marketo.com/saml/xxxxxxx

#### **Enable SAML SSO with Marketo**

- 1. Sign on to the Marketo console as an administrator.
- 2. Select Admin in the toolbar.
- 3. Select **Other Stuff** in the left navigation pane.
- 4. Select Single Sign-On.

#### i) Note

If you don't see Single Sign-On, contact support@marketo.com to enable SAML for your account.

- 5. Select Edit next to SAML Settings.
- 6. For the Issuer ID, enter the value you entered for the IdP Entity ID in PingOne.
- 7. For the Entity ID, enter the value you entered for the IdP Entity ID in PingOne.
- 8. For the User ID Location, click the In Name identifier element of Subject.
- 9. Click Browse next to Identity Provider Certificate and upload your public certificate.
- 10. Click Save.

#### Test the PingOne IdP integration

1. Go to the PingOne Application Portal and sign on with a user account.

#### i) Note

In the Admin console, go to **Dashboard** → **Environment Properties** to find the **PingOne Application Portal URL**.

2. Click the Marketo icon.

You're redirected to the Marketo website and signed on with SSO.

# Microsoft 365

# Configuring SAML SSO with Microsoft 365 and PingFederate

Learn how to enable Microsoft 365 sign-on from a PingFederate URL (IdP-initiated sign-on) and direct Microsoft 365 sign-on using PingFederate (SP-initiated sign-on).

#### Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users requiring application access.
- Make sure Microsoft 365 has a valid, non-default domain and is populated with at least one AD synced user in that domain to test access.
- You must have administrative access to PingFederate and Microsoft 365.
- You must have access to run the Microsoft Azure Active Directory Module for Windows PowerShell.

#### **Create a PingFederate SP connection for Microsoft 365**

- 1. Download the Microsoft 365 SAML metadata from https://nexus.microsoftonline-p.com/federationmetadata/saml20/ federationmetadata.xml<sup>C</sup>.
- 2. Sign on to the PingFederate administrative console.
- 3. Create an SP connection for Microsoft 365 in Ping Federate:
  - 1. Configure using Browser SSO profile SAML 2.0.
  - 2. Import the metadata from the downloaded Microsoft 365 metadata file.
  - 3. Enable the following SAML Profiles:
    - IdP-Initiated SSO
    - SP-Initiated SSO
    - SP Initiated SLO
  - 4. In Assertion Creation: Attribute Contract, extend the contract to add the attributes guid and SAML\_NAME\_FORMAT.
  - 5. In Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfillment map the following:
    - SAML\_SUBJECT to guid (guid should map to your attribute holding the Microsoft 365 user objectID and be in Base64 binary format)
    - SAML\_NAME\_FORMAT to urn:oasis:names:tc:SAML:2.0:nameid-format:persistent.

- 6. In Protocol Settings: Allowable SAML Bindings, enable POST and REDIRECT.
- 7. In Protocol Settings: Signature Policy, select Always Sign Assertion.
- 8. In Credentials: Digital Signature Settings, select the PingFederate signing certificate.
- 4. Save the configuration.
- 5. Export the signing certificate.
- 6. Export and then open the metadata file and copy the values for the following:
  - entityID
  - Location entry for SSO (https://your-value/idp/SSO.saml2)
  - Location entry for SLO ( https://your-value/idp/SLO.saml2 )

#### Add the PingFederate connection to Microsoft 365

1. Open an elevated Windows PowerShell Command Prompt window on any internet-connected computer and type:

\$cred = Get-Credential

2. Enter the username and password of your Microsoft 365 administrator account in the pop-up.

Administrator: Windows PowerShell			_		×
Windows PowerShell Copyright (C) Microsoft Corporation. All rights rese	rved.				
Try the new cross-platform PowerShell https://aka.ms	Windows PowerShel	l credential request	?	×	
PS C:\Windows\system32> <pre>\$cred=Get-Credential</pre>			AF		
cmdlet Get-Credential at command pipeline position 1 Supply values for the following parameters: Credential	¥ 1		T		
	Enter your credentials	5.			
	<u>U</u> sername:	🖸 user@mydomain.c	om	×	
	Password:	•••••			
		OK	Can	icel	

3. Connect with MsolService.

Connect-MsolService -Credential \$cred

4. List your domains.

```
Get-MsolDomain
```

5. Select the domain for which you would like to enable SSO.

```
$dom = "your-0365-domain"
```

6. Set the **uri** parameter to the PingFederate **entityID** value.

\$uri ="your-entityID"

7. Set the url parameter to the PingFederate Location for SSO value.

\$url="your-Passive-Log-On-Uri"

8. Set the logouturl parameter to the PingFederate Location for SLO value.

\$logouturl="your-Log-Off-Uri"

9. Open the downloaded signing certificate in Notepad, copy the encoded contents, and paste them into the command below to set the certificate parameter.

\$cert="your-certificate-contents"

10. Run the following command to setup SAML SSO for your domain.

```
Set-MsolDomainAuthentication `
-DomainName $dom `
-FederationBrandName $dom `
-Authentication Federated `
-PassiveLogOnUri $url `
-SigningCertificate $cert `
-IssuerUri $uri `
-LogOffUri $logouturl `
-PreferredAuthenticationProtocol SAMLP
```

11. Run the following command to see the completed SSO settings.

Get-MSolDomainFederationSettings -DomainName "your-0365-domain" | Format-List \*

#### Test the PingFederate IdP-initiated SSO integration

- 1. Go to the PingFederate SSO application endpoint for the Microsoft 365 SP connection.
- 2. Complete PingFederate authentication.

You're redirected to your Microsoft 365 domain.

#### Test the PingFederate SP-initiated SSO integration

- 1. Go to https://portal.office.com  $\square$ .
- 2. Enter your email address.
- 3. After you're redirected to PingFederate, enter your PingFederate username and password.

You're redirected back to Microsoft 365.

# Configuring SAML SSO with Microsoft 365 and PingOne for Enterprise

Learn how to enable Microsoft 365 sign-on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct Microsoft 365 sign-on using PingOne for Enterprise (SP-initiated sign-on).

#### Before you begin

- Link PingOne for Enterprise to an identity repository containing the users requiring application access. Learn more in Connecting to an identity repository <sup>[]</sup> in the PingOne for Enterprise documentation.
- Make sure Microsoft 365 has a valid, non-default domain and is populated with at least one AD synced user in that domain to test access.
- You must have administrative access to PingOne for Enterprise and Microsoft 365.
- You must have access to run the Microsoft Azure Active Directory Module for Windows PowerShell.

#### Obtain the PingOne for Enterprise values for the Microsoft 365 application

- 1. Sign on to PingOne for Enterprise and go to **Applications**  $\rightarrow$  **Application Catalog**.
- 2. Search for Microsoft 365.
- 3. Expand the Microsoft 365 entry and click the **Setup** icon.

# Application Catalog Application You want to add or search for it by name. Don't see the application you're looking for? Fill out our Application Request Form. Office 365 Search Office 365 Office 365 Office 365 SAML with Provisioning (API)

#### 4. Click Continue to Next Step.

- 5. Copy the Issuer URI, Passive Log On Uri, and Log Off Uri values.
- 6. Download the signing certificate.

#### Office 365 Federation Settings

While configuring federation for Office 365, you will need to provide the following details when running the PowerShell cmdlets.



#### Add the PingOne for Enterprise IdP Connection to Microsoft 365

1. Open an elevated Windows PowerShell Command Prompt window on any internet-connected computer and type:

	\$cred = Get-Credential
2.	Enter the username and password of your Microsoft 365 administrator account in the pop-up.



3. Connect with MsolService.

Connect-MsolService -Credential \$cred

4. List your domains.

Get-MsolDomain

5. Enter the domain for which you would like to enable SSO.

\$dom = "your-0365-domain"

6. Set the uri parameter to the PingOne for Enterprise Issuer URI value.

\$uri ="your-Issuer-URI"

7. Set the url parameter to the PingOne for Enterprise Passive Log On Uri value.

\$url="your-Passive-Log-On-Uri"

8. Set the logouturl parameter to the PingOne for Enterprise Log Off Uri value.

\$logouturl="your-Log-Off-Uri"

9. Open the downloaded signing certificate in Notepad, copy the encoded contents, and paste them into the command below to set the certificate parameter.

\$cert=your-certificate-contents

10. Run the following command to set up SAML SSO for your domain.

```
Set-MsolDomainAuthentication `
-DomainName $dom `
-FederationBrandName $dom `
-Authentication Federated `
-PassiveLogOnUri $url `
-SigningCertificate $cert `
-IssuerUri $uri `
-LogOffUri $logouturl `
-PreferredAuthenticationProtocol SAMLP
```

11. Run the following command to see the completed SSO settings.

Get-MSolDomainFederationSettings -DomainName "your-0365-domain" | Format-List \*

#### Complete the Microsoft 365 setup in PingOne for Enterprise

1. Continue editing the Microsoft 365 entry in PingOne for Enterprise.

#### (i) Note

If the session has timed out, complete the initial steps to the point of clicking Setup.

- 2. Click Continue to Next Step until you reach the Attribute mapping page.
- 3. Map subject to SAML\_SUBJECT.
- 4. Map guid to your attribute containing the Microsoft 365 user objectGUID.

#### 4. Attribute Mapping

	Application Attribute	Description	Identity Bridge Attribute or Literal Value
		Active Directory Attribute:	SAML_SUBJECT
1	subject *	userPrincipalName	As Literal
2		Active Directory Attribute:	myGUID
2	guia	objectGUID	As Literal

Map your identity bridge attributes to the attributes required by the application.

#### 5. Click Continue to Next Step twice.

6. Click Add for all user groups that should have access to Microsoft 365.

#### 5. Group Access

Select all user groups that should have access to this application. Users that are members of the added groups will be able to SSO to this application and will see this application on their personal dock.

Group1, Group2, etc	Search	
Group Name		
Users@directory		Remove
Domain Administrators@directory		Add

#### 7. Click Continue to Next Step.

8. Click Finish.

#### Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to your Ping desktop as a user with Microsoft 365 access.

<b>(</b> )	Note

To find the Ping desktop URL in the Admin console, go to Setup  $\rightarrow$  Dock  $\rightarrow$  PingOne Dock URL.

2. Complete PingOne for Enterprise authentication.

You're redirected to your Microsoft 365 domain.

	Ping Keekity Sign On	
USERNAME		
PASSWORD		
	Remember Me	
	Sign On	
	Forgot Password	

#### Test the PingOne for Enterprise SP-initiated SSO integration

- 1. Go to https://portal.office.com<sup>[]</sup>.
- 2. Enter your email address.
- 3. After you're redirected to PingOne for Enterprise, enter your PingOne for Enterprise username and password.

	Ping Sign On	
USERNAME		
PASSWORD		
	Remember Me	
	Sign On	
	Forgot Password	

You're redirected back to Microsoft 365.

# **Mimecast**

# **Configuring SAML SSO with Mimecast and PingFederate**

Learn how to enable Mimecast sign-on from PingFederate (IdP-initiated sign-on) and direct Mimecast sign-on using PingFederate (SP-initiated sign-on).

#### Before you begin

- Configure PingFederate to authenticate against an identity provider (IdP) or datastore containing the users requiring application access.
- Populate Mimecast with at least one user to test access.
- You must have administrative access to PingFederate.

#### Create the Mimecast metadata

- 1. In PingFederate, create a service provider (SP) connection for Mimecast:
  - 1. Configure using Browser SSO profile SAML 2.0.
  - 2. Set Partner's Entity ID to your-Mimecast-account-hosting-location-api.mimecast.com.accountcode.
  - 3. Enable the following SAML profiles:
    - IdP-Initiated SSO
    - SP-Initiated SSO
  - 4. In Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfilment, map the SAML\_SUBJECT to your email attribute.
  - 5. In Protocol Settings: Assertion Consumer Service URL, set Binding to POST and set Endpoint URL to https:// your-Mimecast-account-hosting-location-api.mimecast.com/sign on/saml.
  - 6. In Protocol Settings: Allowable SAML Bindings, enable POST.
  - 7. In Credentials: Digital Signature Settings, select the PingFederate Signing Certificate.

# (i) Note

Note the metadata URL for the newly-created Mimecast SP connection.

#### Add the PingFederate connection to Mimecast

1. Sign on to the Mimecast console as an administrator.

- 2. Select Administration on the lefthand pane.
- 3. Click the **Services** tab.
- 4. Select Application Settings.
- 5. Select Authentication Profiles.

mimecast <sup>®</sup> Administration Console							
Account -	Gateway	Services -	Archive -	Directories -	Stationery -	Monitoring	Reporting
You are here:	Services > App	blications					
Application Set	ttings 🙁	Dashboard					
New Applicatio	on Setting: Aut	thentication Profi	les Registere	ed Applications V	iew •		
Search		Q					
Description	1				G	iroup	

- 6. Click New Authentication Profile.
- 7. Select the Enforce SAML Authentication for Administration Console option.

The page expands to reveal the SAML Settings.

- 8. Under Provider, select Other.
- 9. Enter the Metadata URL for the Mimecast SP Connector in PingFederate.

#### Test the PingFederate IdP-initiated SSO integration

- 1. Go to the PingFederate SSO Application Endpoint for the Mimecast SP connection.
- 2. Authenticate with PingFederate.

You're redirected to your Mimecast domain.

#### Test the PingFederate SP-initiated SSO integration

- 1. Sign on to Mimecast  $\square$ .
- 2. After you're redirected to PingFederate, enter your PingFederate username and password.

After successful authentication, you're redirected back to Mimecast.

# Configuring SAML SSO with Mimecast and PingOne

Learn how to enable Mimecast sign-on from the PingOne console (IdP-initiated sign-on) and direct Mimecast sign-on using PingOne (SP-initiated sign-on).

#### Before you begin

- Link PingOne to an identity repository containing the users requiring application access.
- Populate Mimecast with at least one user to test access.
- You must have administrative access to PingOne and a Super Admin account for an Enterprise Organization on Mimecast.

#### Add the Mimecast application to PingOne

1. In PingOne, go to **Connections**  $\rightarrow$  **Applications** and click the + icon.

Pingldentity.			
Environments Sandbox - Phil ~ Sandbox		Applications 🔸	
::	< Connections	Q Search	Filter
2	Applications	3 Applications by Application Name	
R	IDENTITY PROVIDERS	PingOne Admin Console Client ID	
٢		PingOne Application Portal	
Ô	PingFederate		
	PingIntelligence	PingOne Seit-Service - MyAccount Client ID: d	

- 2. When you're prompted to select an application type, select **WEB APP** and then click **Configure** next to **SAML** for the chosen connection type.
- 3. Enter Mimecast as the application name.
- 4. Enter a suitable description.
- 5. Optional: Upload an icon.
- 6. Click Next.
- 7. For Provide App Metadata, select Enter Manually.
- 8. In the ACS URL field, enter https://account-hosting-location-api.mimecast.com/login/saml.
- 9. Select the Signing Key to use and then click Download Signing Certificate to download as X509 PEM (.crt).

- 10. For Entity ID, enter https://account-hosting-location-api.mimecast.com.accountcode.
- 11. Leave SLO Endpoint and SLO Response Endpoint blank.
- 12. In the Subject NameID Format list, select urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress.
- 13. Enter a suitable value for Assertion Validity Duration (in seconds). A value of 300 seconds is typical.
- 14. Click Save and Continue.
- 15. Mimecast expects an email address to identify a user in the SSO security assertion:
  - If you use an email address to sign on through PingOne, click **Save and Close**.
  - If you sign on with a username, in the **PingOne User Attribute** list, select **Email Address** to map that to the **SAML\_SUBJECT**, then click **Save and Close**.
- 16. Click the toggle to enable the application.
- 17. On the **Configuration** tab of the newly-created Mimecast application, copy and save the **IDP Metadata URL** value.

You'll need this metadata when configuring SAML on Mimecast.

^	CONNECTION DETAILS		
	DOWNLOAD METADATA :	Download	
	ISSUER ID :	https://auth.pingone.eu/f	l
	SINGLE LOGOUT SERVICE :	https://auth.pingone.eu/f	saml20/idp/slo
	SINGLE SIGNON SERVICE :	https://auth.pingone.eu/f	saml20/idp/sso
	IDP METADATA URL:	https://auth.pingone.eu/f	saml20/metadata/c6c91962-45a9-4379-84bf-77576fa582f7
	INITIATE SINGLE SIGN-ON URL:	https://auth.pingone.eu/f	saml20/idp/startsso?spEntityId=https://xx-api.mimecast.com/login/saml

#### Add PingOne as identity provider (IdP) in Mimecast

- 1. Sign on to Mimecast with an Admin account for your Enterprise Organization.
- 2. Go to Administration  $\rightarrow$  Services  $\rightarrow$  Applications.
- 3. Select Authentication Profiles.
- 4. Select New Authentication Profile.
- 5. Enter a **Description** for the new profiled.
- 6. Select Enforce SAML Authentication for Administration Console.
- 7. For Provider, select Other.
- 8. In the Metadata URL field, enter the URL value that you copied previously.
- 9. Go to Administration  $\rightarrow$  Services  $\rightarrow$  Applications.
- 10. Click **Lookup** to find the authentication profile that you created.
- 11. Click Save and Exit.

#### Test the PingOne IdP integration

1. Go to the PingOne Application Portal and sign on with a user account.

# Note In the Admin console, go to Dashboard → Environment Properties to find the PingOne Application Portal URL.

2. Click the Mimecast icon.

You're redirected to the Mimecast website and logged in with SSO.

#### Test the PingOne SP integration

- 1. Go to login.mimecast.com<sup>[2]</sup>, and choose the option to sign on with SSO. Enter your email address only.
- 2. In the PingOne sign-on prompt, enter your PingOne username and password.

Ping Sign On				
USERNAME				
PASSWORD				
	Remember Me			
	Forgot Password			

You're redirected back to Mimecast and signed on.
# **Configuring SAML SSO with Namely and PingFederate**

Learn how to enable Namely sign-on from the PingFederate console (IdP-initiated sign-on) and direct Namely sign-on using PingFederate (SP-initiated sign-on).

#### Before you begin

- PingFederate should be configured to authenticate against an identity provider (IdP) or datastore containing the users requiring application access.
- Populate Namely with at least one user to test access.
- You must have administrative access to PingFederate.

#### Create the Namely metadata

- 1. In PingFederate, create a service provider (SP) connection for Namely:
  - 1. Configure using Browser SSO profile SAML 2.0.
  - 2. Set Partner's Entity ID to https://your-subdomain.namely.com/saml/metadata.
  - 3. Enable the following SAML profiles:
    - IdP-Initiated SSO
    - SP-Initiated SSO
  - 4. In Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfilment, map the SAML\_SUBJECT to your email attribute.
  - 5. In Protocol Settings: Assertion Consumer Service URL, set Binding to POST and set Endpoint URL to https:// your-subdomain.namely.com/saml/consume.
  - 6. In Protocol Settings: Allowable SAML Bindings, enable POST.
  - 7. In Credentials: Digital Signature Settings, select the PingFederate Signing Certificate.
  - 8. Note the metadata URL for the newly-created Namely SP connection.

#### Add the PingFederate connection to Namely

- 1. Sign on to the Namely console as an administrator.
- 2. Select **Company** on the top navigation bar.

Namely

- 3. Click the **Settings** tab.
- 4. In the left navigation pane, click Login Page.
- 5. In the Login Methods section, click SAML.
- 6. Enter the Identity Provider SSO URL from PingFederate.
- 7. Copy and paste the IdP Provider Certificate value into the Identity provider certificate.
- 8. Enter the SAML Metadata URL from PingFederate.

General	Login methods
Company Info	Login methods
Invitations	Please determine which Login Method employees will use to access Namely. Employees may log in using: either their Namely or Google credentials, only their Google credentials, or only through SAML.
Overhead	Password and Google
Import Data	Only Google SAML
Resources	SAML Settings
Home Page Updates	Identity provider SSO url
Notifications	certificate
Login Page >	BEGIN CERTIFICATE
Employee Data	
Profile Fields	
Termination Reasons	
Organizational Structure	If your identity provider requires a SAML metadata endpoint, please use the following URL.

9. Click Save.

#### Test the PingFederate IdP-initiated SSO integration

- 1. Go to the PingFederate SSO Application Endpoint for the Namely SP connection.
- 2. Authenticate with PingFederate.

You're redirected to your Namely domain.

#### Test the PingFederate SP-initiated SSO integration

1. Go to https://your-subdomain.namely.com/users/login.

2. After you're redirected to PingFederate, enter your PingFederate username and password.

You're redirected back to Namely.

# Configuring SAML SSO with Namely and PingOne

Learn how to enable Namely sign-on from the PingOne console (IdP-initiated sign-on) and direct Namely sign-on using PingOne (SP-initiated sign-on).

#### Before you begin

- Link PingOne to an identity repository containing the users requiring application access.
- Populate Namely with at least one user to test access.
- You must have administrative access to PingOne and an Admin account on Namely.

#### Add the Namely application to PingOne

1. In PingOne, go to **Connections**  $\rightarrow$  **Applications** and click the + icon.

P	ingldentity.		
Enviro Sandi Sandb	nments pox - Phil v ox	Applications 🔸	
#	< Connections APPLICATIONS Applications	Q Search 3 Applications by Application Name	Filter
1H (	IDENTITY PROVIDERS	PingOne Admin Console Client ID	
©	PING PRODUCTS PingFederate	PingOne Application Portal Client ID: 1	
	PingIntelligence	PingOne Self-Service - MyAccount           Client ID: c	

- 2. When you're prompted to select an application type, select **WEB APP** and then click **Configure** next to **SAML** for the chosen connection type.
- 3. Enter Namely as the application name.
- 4. Enter a suitable description.
- 5. Optional: Upload an icon.
- 6. Click Next.

- 7. For Provide App Metadata, select Enter Manually.
- 8. In the ACS URLS field, enter https://your-subdomain.namely.com/saml/consume.
- 9. In the Entity ID field, enter https://your-subdomain.namely.com/saml/consume.
- 10. Select the Signing Key to use and then click Download Signing Certificate to download as X509 PEM (.crt).
- 11. Leave SLO Endpoint and SLO Response Endpoint blank.
- 12. In the Subject NameID Format list, select urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress.
- 13. Enter a suitable value for Assertion Validity Duration (in seconds). A value of 300 seconds is typical.
- 14. Click Save and Continue.
- 15. Namely expects an email address to identify a user in the SSO security assertion:
  - If you use an email address to sign on through PingOne, click Save and Close.
  - If you sign on with a username, in the **PingOne User Attribute** list, select **Email Address** to map that to the **SAML\_SUBJECT**, then click **Save and Close**.
- 16. Click the toggle to enable the application.
- 17. On the **Configuration** tab of the newly-created Namely application, copy and save the **IDP Metadata URL** value.

You'll need this when configuring SAML on Namely.

∧ CONNECTION DETAILS		
DOWNLOAD METADATA :	Download	
ISSUER ID :	https://auth.pingone.eu/f	
SINGLE LOGOUT SERVICE :	https://auth.pingone.eu/f	saml20/idp/slo
SINGLE SIGNON SERVICE:	https://auth.pingone.eu/t	saml20/idp/sso
IDP METADATA URL:	https://auth.pingone.eu/t	saml20/metadata/c6c91962-45a9-4379-84bf-77576fa582f7
INITIATE SINGLE SIGN-ON URL	https://auth.pingone.eu/t	saml20/idp/startsso?spEntityId=https://xx-api.mimecast.com/login/saml

#### **Enable SAML SSO in Namely**

- 1. Sign on to the Namely console as an administrator.
- 2. Select **Company** on the top navigation bar.
- 3. Click the **Settings** tab.
- 4. In the left navigation pane, click Login Page.
- 5. In the Login Methods section, click SAML.
- 6. In the Identity Provider SSO URL field, enter the Initiate Single Sign-On URL value from PingOne.
- 7. Copy and paste the IdP Provider Certificate value into the Identity provider certificate field.
- 8. In the SAML Metadata field, enter the IdP Metadata URL value from PingOne.

Reports Goals Se	ttings
General	Login methods
Company Info	Login methods
nvitations	Please determine which Login Method employees will use to access Namely. Employees may log in using: either their Namely or Google credentials, only their Google credentials, or only through SAML.
Overhead	Password and Google
mport Data	Only Google SAML
Resources	SAML Settings
Home Page Updates	Identity provider SSO url
Notifications	certificate
Login Page >	BEGIN CERTIFICATE
Employee Data	
Profile Fields	
Termination Reasons	
Organizational Structure	If your identity provider requires a SAML metadata endpoint, please use the following URL.

9. Click Save.

#### Test the PingOne IdP integration

1. Go to the PingOne Application Portal and sign on with a user account.



2. Click the Namely icon.

You're redirected to the Namely website and logged in with SSO.

#### Test the PingOne SP integration

- 1. Go to https://your-subdomain.namely.com/users/login and enter your email address only.
- 2. In the PingOne sign-on prompt, enter your PingOne username and password.

	Ping Keetative Sign On	
USERNAME		
PASSWORD		
	Remember Me	
	Forgot Password	

You're redirected back to Namely and signed on.

# Osano

# Configuring SAML SSO with Osano and PingOne

Learn how to enable Osano sign-on from the PingOne console (IdP-initiated sign-on) and direct Osano sign-on using PingOne (SP-initiated sign-on).

#### Before you begin

- Link PingOne to an identity repository containing the users requiring application access.
- Populate Osano with at least one user to test access.
- You must have administrative access to PingOne and an Admin account for an Enterprise Organization on Osano.

#### Add the Osano application to PingOne

- 1. In PingOne, in the left menu, click Connections, then Applications.
- 2. To add a new application, click the + icon next to the **Applications** heading.

P	ingldentity.		
Enviro Sandi Sandb	nments pox - Phil v xx	Applications	
88	< Connections	Q Search	Filter
*	APPLICATIONS Applications	3 Applications by Application Name	
11	IDENTITY PROVIDERS	PingOne Admin Console Client ID	
0	PING PRODUCTS	PingOne Application Portal Client ID:	
NO22	PingFederate PingIntelligence	PingOne Self-Service - MyAccount Client ID: d	

- 3. Select **Web App** when prompted to select an application type and click **Configure** next to **SAML** for the chosen connection type.
- 4. Enter **0sano** as the application name.
- 5. Enter a suitable description.

- 6. Upload an icon if desired.
- 7. Click Next.
- 8. For Provide App Metadata, select Manually Enter.
- 9. For ACS URL, enter the value: https://auth.osano.com/saml2/idpresponse.
- 10. Select the Signing Key to use and click Download Signing Certificate to download as X509 PEM ( .crt ).
- 11. For Entity ID, enter the value: urn:amazon:cognito:sp:us-east-1\_7GtagkRKw.

## (i) Note

Leave SLO Endpoint and SLO Response Endpoint blank. Osano does not support single logout (SLO).

- 12. In the Subject NameID Format list, select urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress.
- 13. Set a suitable value for Assertion Validity Duration (in seconds). A value of 300 seconds is typical.
- 14. Click Save and Continue.
- 15. Change the **saml\_subject** attribute to **Email Address**.

# i Note

Osano expects an email address to identify a user in the SSO security assertion.

16. Select Add Attribute and Ping One Attribute and enter http://schemas.xmlsoap.org/ws/2005/05/identity/claims/ emailaddress as the Application Attribute.

Map this to the PingOne User Attribute for Email Address.

17. Select Add Attribute and Ping One Attribute and enter http://schemas.xmlsoap.org/ws/2005/05/identity/claims/ name as the Application Attribute.

Map this to the **PingOne User Attribute** for **Name**.

- 18. Click Save and Close.
- 19. Enable user access to this new application by moving the toggle to the right.
- 20. On the **Configuration** tab of the newly created Osano application, download the metadata.

^ CONNECTION DETAILS		
DOWNLOAD METADATA:	Download	
ISSUER ID :	https://auth.pingone.eu	
SINGLE LOGOUT SERVICE :	https://auth.pingone.eu	/saml20/idp/slo
SINGLE SIGNON SERVICE:	https://auth.pingone.eu	/saml20/idp/sso
IDP METADATA URL:	https://auth.pingone.eu	/saml20/metadata/863db32b-5cfe-44d9-bf92-2f4a3de191c7
INITIATE SINGLE SIGN-ON URL:	https://auth.pingone.eu	/saml20/idp/startsso?spEntityId=urn:amazon:cognito:sp:us-east-1_7GtagkRKw

#### Add PingOne as the identity provider (IdP) to Osano

- 1. Open a Support request with your Osano Support Representative and supply the Metadata File exported in the previous procedure. This file should contain the following:
  - Identity Provider Issuer
  - Identity Provider Single Sign-On URL
  - X.509 Certificate

Osano configures these settings for your account, and the connection is established.

#### Test the PingOne IdP integration

- 1. Go to the PingOne SSO Application Endpoint for the Osano SP connection.
- 2. Complete the PingOne authentication.

You're redirected to your Osano domain.

#### Test the PingOne SP connection

1. Go to https://my.osano.com<sup>[2]</sup>, select the option to sign on with SSO, and enter your email address only.

You're redirected and presented with a PingOne sign on prompt.

2. Enter your PingOne username and password.



After successful authentication, you're redirected back to Osano and signed on.

# RingCentral

# Configuring SAML SSO with RingCentral and PingFederate

Learn how to enable RingCentral sign-on for the PingFederate console (IdP-initiated sign-on) and direct RingCentral sign-on using PingFederate (SP-initiated sign-on).

#### Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users that need application access.
- Populate RingCentral with at least one user for testing access.
- You must have administrative access to PingFederate and RingCentral.

#### **Export the PingFederate metadata**

- 1. In the PingFederate administrative console, go to System  $\rightarrow$  Protocol Metadata  $\rightarrow$  Metadata Export.
- 2. Select I am the identity provider then click Next.
- 3. On the Metadata Mode tab, select Select information to include in metadata manually. Click Next.
- 4. On the Protocol tab, click Next.
- 5. On the Attribute Contract tab, click Next.
- 6. On the Signing Key tab, select a signing certificate. Click Next.
- 7. Optional: On the Metadata Signing tab, select a certificate to sign the metadata XML file. Click Next.
- 8. On the XML Encryption Certificate tab, click Next.
- 9. On the Export & Summary tab, click Export.
- 10. Save the metadata.xml file.
- 11. Click Done.

## **Configure RingCentral for SSO**

1. In the RingCentral administrative console, go to More  $\rightarrow$  Security and Compliance  $\rightarrow$  Single Sign-on.

- 2. Select Set up SSO by yourself.
- 3. Upload the PingFederate metadata that you downloaded previously.
- 4. Select the email attributes to map.

- 5. In the **Certificate Management** section, upload the certificate and set it as the primary.
- 6. Download the RingCentral SP metadata file.
- 7. Toggle Enable SSO and click Save.

#### **Create a PingFederate SP connection for RingCentral**

- 1. In the PingFederate administrative console, go to **Applications**  $\rightarrow$  **SP Connections**  $\rightarrow$  **Create Connection**.
- 2. Configure using Browser SSO profile SAML 2.0.
- 3. Import the RingCentral metadata file that you downloaded previously.
- 4. Enable the following SAML profiles:
  - IdP-Initiated SSO
  - SP-Initiated SSO
- 5. In Assertion Creation: Attribute Contract, next to SAML\_SUBJECT, map the Subject Name Format to urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress.
- 6. In Assertion Creation: Authentication Policy Mapping: Attribute Contract Fulfillment, map SAML\_SUBJECT to your email attribute.
- 7. In Protocol Settings: Allowable SAML Bindings, enable POST and REDIRECT.
- 8. In Credentials: Digital Signature Settings, in the Signing Certificate list, select your signing certificate.
- 9. Note the SSO Application Endpoint for your newly-created SP connection.

#### Test the PingFederate IdP-initiated SSO integration

- 1. Go to the PingFederate SSO Application Endpoint for the RingCentral SP connection.
- 2. Authenticate with PingFederate.

You're redirected to RingCentral.

#### Test the PingFederate SP-initiated SSO integration

- 1. Go to https://service.ringcentral.com/login/startupSSOLogin.html
- 2. Enter your email address and click Submit.
- 3. After you're redirected to PingFederate, enter your PingFederate username and password. s+ You're redirected to RingCentral.

# Salesforce

# **Configuring SAML SSO with Salesforce and PingFederate**

Enable Salesforce sign-on from a PingFederate URL (IdP-initiated sign-on) plus single logout (SLO).

#### Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users requiring application access.
- Populate Salesforce with at least one user to test access.
- You must have administrative access to PingFederate and Salesforce.

#### **Create a PingFederate SP connection for Salesforce**

- 1. Sign on to the PingFederate administrative console.
- 2. Create an SP connection for Salesforce in PingFederate:
  - 1. Configure using Browser SSO profile SAML 2.0.
  - 2. Set Partner's Entity ID to Entity ID.
    - Enable the following SAML Profiles:
    - IDP-Initiated SSO
    - SP Initiated SSO
    - IDP-Initiated SLO
    - SP Initiated SLO
  - 3. In Assertion Creation → Authentication Source Mapping → Attribute Contract Fulfillment, map the SAML\_SUBJECT to the attribute containing the Salesforce username.
  - 4. In Protocol Settings → Assertion Consumer Service URL, set Binding to POST and set Endpoint URL to ACS URL.
  - 5. In Protocol Settings → SLO Service URLs, set Binding to POST and set Endpoint URL to SLO URL.
  - 6. In Protocol Settings → Allowable SAML Bindings, enable POST.
  - 7. In Credentials → Digital Signature Settings, select the PingFederate Signing Certificate.
  - 8. In Credentials → Signature Verification, set Trust Model to Unanchored.
  - In Credentials → Signature Verification → Signature Verification Certificate, select the PingFederate Signing Certificate.

#### ) Note

This certificate is a placeholder and will be replaced with a Salesforce certificate.

- 3. Export the metadata for the newly created Salesforce SP connection.
- 4. Export the signing certificate.

i i

#### Add the PingFederate IDP Connection to Salesforce

- 1. Sign on to your Salesforce domain as an administrator.
- 2. Click the Gear icon, then go to Setup  $\rightarrow$  Identity  $\rightarrow$  Single Sign-On Settings.

-	Q, Search Setup	**	• ?	章	* (	3
Setup Home Object	Manager 🗸	to Setup		C <sup>R</sup>		
> Development					S. 3	
> Environments	Stude Size On Settings	Manage Sc	bscription			
> User Engagement	Single Sign-On Settings	Developer Conso	le			
> Integrations					_	
> Notification Builder	Single Sign-On Settings			Help for	this Page 🜖	•
SETTINGS	Configure single sign on in order to authenticate users in salesforce com from external environments. Your organization has the following options available for single sign-on:					
> Company Settings	<ul> <li>Delegated authentication is a single sign-on method that uses a Web service call sent from salestocic com to an endpoint.</li> <li>Pedenated authentication, a single sign-on method that uses SAML assertions sent to a Salestforce endpoint.</li> </ul>					
> Data Classification	Edit SAM, Assartin Validator					
<ul> <li>Identity</li> </ul>	Delegated Authentication					
Auth. Providers	Disable login with Saleshore credentials					
Identity Provider	Federated Single Ston-On Using SAML					-
Identity Provider Event Log	Identity Provider Event Log SAME, Fashing SAME, Fashing Same Same Same Same Same Same Same Same					
Identity Verification						
Identity Verification History	SAML Single Sign-On Settings New York Monthleaders File New Horn Mittaders (R)					
Login Flows	No SAAS, Brige Sign-Cn Settings					
Login History						
OAuth Custom Scopes						
Single Sign-On Settings						
> Security						

3. On the Single Sign-On Settings page, click Edit.

Setup Single Sign-On Settings
Single Sign-On Settings
Configure single sign-on in order to authenticate users in salesforce.com from external environments.
<ul> <li>Delegated authentication is a single sign-on method that uses a Web service call sent from salesfore</li> <li>Federated authentication, a single sign-on method that uses SAML assertions sent to a Salesforce enderstanding and the service service</li></ul>
Edit SAML Assertion Validator

4. Select the SAML Enabled check box to enable the use of SAML single sign-on. Click Save.

Single Sign-On Setting	S	
		Save Cancel
Delegated Authentication		
Disable login with Salesforce credentials	i	
Federated Single Sign-On Using SAM	۱L	
SAML Enabled		
		Save

#### 5. Click New From Metadata File.

SAML Single Sign-On Settings	New New from Metadata File New from Metadata URL
No SAML Single Sign-On Settings	

6. Click Choose File, select the metadata that you downloaded from PingFederate, and click Create.

SAML Single Sign-On Settings			
Create configuration using an XML file (1	MB or smaller) containing SAML 2.0 settings		
	Create Cancel		
Metadata File	Choose File No file chosen		
	Create		

The summary screen opens.

- 7. In the **Identity Provider Certificate** section, click **Choose file** and select the signing certificate that you downloaded from PingFederate.
- 8. Clear the Single Logout Enabled check box if you don't require single logout.

#### The summary page opens.

ML Single Sign-On Se	ettings	
	Save 8. New Cancel	
Name	API Na:	
SAML Version	2.0	
Issuer	Entry Entry	b https:// .my.salesforce.
Identity Provider Certificate	Choose File 1771B6ADC4E.crt Current Certifica	CN=Signing cert, O=PingTest, C=U Expiration: 19 Jan 2022 16:12:04 G
Request Signing Certificate	SelfSignedCert_02Feb2021_175028 V	
Request Signature Method	RSA-SHA256 V	
Assertion Decryption Certificate	Assertion not encrypted	
SAML Identity Type	Assertion contains the User's Salesforce username     Assertion contains the Federation ID from the User object     Assertion contains the User ID from the User object	
SAML Identity Location	Identity is in the Nameldentifier element of the Subject statement     Identity is in an Attribute element	
Service Provider Initiated Request Binding	HTTP POST     HTTP Redirect	
Identity Provider Login URL	https://j / / / / / / / / / / / / / / //SSO.saml2	
Custom Logout URL		
Custom Error URL		
Single Logout Enabled		
se Selected Request Signature Method for Single Logout		
Identity Provider Single Logout URL	https://	
Single Logout Request Binding	HTTP POST     HTTP Redirect	

#### 9. Click Save.

10. On the summary page for the configuration that you saved in the previous step, click Edit.

SAML Single Sign-On Back to Single Sign-On Settings	Settings			
		Edit Delete Clone I	Download Metadata	SAML Assertion Validator
Name SAML Version	- Ng - <del>Se</del> <b>Child (C. Poe</b> c 2.0			

11. Click the link on the **Request Signing Certificate** line.

Identity Provider Certificate	CN=Signing cert, O=PingTest, C=UK Expiration: 19 Jan 2022 16:12:04 GMT		
Request Signing Certificate	SelfSignedCert_02Feb2021_175028		
Request Signature Method	RSA-SHA256		

#### 12. Click Download Certificate.

Certificates	
Certificates	
Certificate and Key Detail	Edit Delete Download Certificate
Label	SelfSignedCert_02Feb2021_175028
Туре	Self-Signed
Expiration Date	02/02/2022, 12:00
Key Size	2048

#### Import the Salesforce certificate into PingFederate

- 1. Sign on to the PingFederate administrative console.
- 2. Open the Salesforce SP connection and click Signature Verification Certificate.
- 3. Delete the placeholder certificate and upload the certificate that you downloaded from Salesforce.
- 4. Save the configuration.

#### Test the PingFederate IdP-initiated SSO integration

- 1. Go to the PingFederate SSO application endpoint for the Salesforce SP connection.
- 2. Complete PingFederate authentication.

You're redirected to your Salesforce domain.

Al ♥ 9, Seach	法・ 🖬 ? 幸 皋 👼
Sales Home Getting Started Accounts v Contacts v Leads v Opportunities v Tasks v Calendar v Dashboard	is 🗸 Notes 🗸 Reports 🗸 Groups 🗸 Forecasts. More 💌 🖋
Quarterly Performance	Assistant
CLOSED £69,000 CHEN(+70%) £184,500 COM. £250,000 /	> Opportunity has overtise tasks Acres = 1,200 Widgets (Sample)
200x	> 20 days without any activity Acme : 1250 Widgets (Sample) 18 🗰 🗙
	> 20 days without any activity Global Media - 110 Widgets (Sample) 18 B ×
240x	> 20 days without any activity Global Media - 1750 Widgets (Sample) 11 🖬 🗶
10.	> 20 days without any activity the salestone corn - 200 Widgets (Sample) 18 🖷 🗙
1204	> 20 days without any activity TE B ×
	> 20 days without any activity Acme - 150 Widgets (Sample) 18 🗃 🗙
60x	> 20 days without any activity Calobal Media - 400 Widgets (Sample) 18 🗃 🗙
0 Dec Dec	> 20 days without any activity salesforce.com - 320 Widgets (Sample) TE 🗃 X
Closed Goal Closed + Cpen (>70%)	> 20 days without any activity Acres - 200 Widgets (Sample) 12 🐻 🗙
Today's Tasks 🛛 🖉 🔻 Today's Events	
Pathewith units (Income an Amine (Income a) Tarias	

#### Configure direct Salesforce sign-on using PingFederate (SP-initiated sign-on) plus single logout (SLO)

#### Before you begin

• You must first enable IdP-initiated sign-on.

#### Enable PingFederate authentication in Salesforce

- 1. Sign on to your Salesforce domain as an administrator.
- 2. Click the **Gear** icon, then go to **Setup**  $\rightarrow$  **Company Settings**  $\rightarrow$  **My Domain**.

SETTINGS				
∨ Con	✓ Company Settings			
	Business Hours			
>	Calendar Settings			
	Company Information			
	Critical Updates			
	Data Protection and Privacy			
	Fiscal Year			
	Holidays			
	Language Settings			
	Maps and Location Settings			
	My Domain			

3. Make a note of your domain name, such as https://your-company.my.salesforce.com.

4. In the Authentication Configuration section, click Edit.

Authentication Configuration	Edit
Login Page Type	Standard
Authentication Service	Login Form
Logo File	
Background Color	
Right Frame URL	
Use the native browser for user authentication on iOS	
Use the native browser for user authentication on Android	

5. In the Authentication Service list, select YourPingFederate. Click Save.

Authentication Configu	ration	
Authentication Configuration		Save Cancel Reset to Default
Login Page Type 🥹	Standard 🗸	
Authentication Service	<ul> <li>Login Form</li> <li>YourPingFederate</li> </ul>	

#### 🕥 Note

The "YourPingFederate" entry was created as a result of the IdP-initiated login tasks above.

Configuration is complete.

Salesforce will now redirect to PingFederate for authentication of all new sessions.

You should also select the **Login Form** check box during the testing phase in case of authentication issues. Testers will be offered the option of the standard Salesforce login form or PingFederate authentication. After you've successfully tested authentication against PingFederate, you can clear the **Login Form** check box so that authentication automatically defaults to PingFederate.

#### Test the PingFederate SP-initiated SSO integration

1. Go to your Salesforce domain.

#### (j) Note

If the **Login Form** check box is still selected, the Salesforce sign on screen still displays, and you're offered a choice of Salesforce sign on or PingFederate sign on, select **PingFederate**. If you've cleared the **Login Form** check box, you're not offered a choice.

2. When you are redirected to PingFederate, enter your PingFederate username and password.

After successful authentication, you're redirected back to Salesforce.



## **Configuring SAML SSO with Salesforce and PingOne for Enterprise**

Enable Salesforce sign-on from the PingOne for Enterprise console (IdP-initiated sign-on) plus single logout (SLO).

#### Before you begin

- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Populate Salesforce with at least one user to test access.
- You must have administrative access to PingOne for Enterprise and Salesforce.

#### Extract the PingOne for Enterprise metadata for Salesforce

- 1. Sign on to PingOne for Enterprise and go to Applications  $\rightarrow$  Application Catalog.
- 2. Search for Salesforce.

<b>ing</b> One <sup>®</sup>		DASHBOARD	APPLICATIONS	USERS	SETUP	ACCOUNT	?
My Applications	Application Catalog	PingiD SDK	Applications	OAuth Se	ttings		
Application	Catalog					÷.	Applications / Application Catalog
Browse for the applic	ation you want to add or se	arch for it by n	ame. Don't see	the applica	tion you'r	e looking for? Fill out our Appli	cation Request Form.
salesforce		Sea	rch				
Showing 1 to 10 of	12				Type		12>>:
$\bigcirc$	Salesforce				SA	ML with Provisioning (API)	•
<i>(</i>	Salesforce - With Just-in	-time Provisio	ning		SA	ML with Provisioning (JIT)	•
<b>e</b>	Salesforce Communities	3			SAJ	ML with Provisioning (API)	►
۵	Salesforce Communities	s Sandbox			SAJ	ML with Provisioning (API)	•
$\Leftrightarrow$	Salesforce Marketing Cl	oud			SAJ	ML	•
makeng text	Salesforce Marketing Cl	oud - Sandbo	x		SA	ML	•
<b>S</b>	Salesforce Sandbox				SA	ML with Provisioning (API)	•

- 3. Expand the Salesforce entry and click the **Setup** icon.
- 4. Click Continue to Next Step until you're on the Group Access page.

i Note
You'll configure the application settings later through metadata.

5. Click **Add** for each user group that should have access to Salesforce.

5. Group Access	
Select all user groups that should have access to this application. Users that are members of the added groups will be able to SSO to this application on their personal dock.	olication and will
Group1, Group2, etc Search	
Group Name	
Users@directory	Remove
Domain Administrators@directory	Add

#### 6. Click Continue to Next Step.

- 7. Download the PingOne for Enterprise signing certificate and SAML metadata.
- 8. Click Finish.

Single Logout Response Endpoint					
Force Re-authentication @ false					
Signing Certificate Download					
SAML Metadata	Download				

#### Add the PingOne for Enterprise IdP Connection to Salesforce

- 1. Sign on to your Salesforce domain as an administrator.
- 2. Click the **Gear** icon ( $\mathbf{a}$ ), then go to **Setup**  $\rightarrow$  **Identity**  $\rightarrow$  **Single Sign-On Settings**.

-	Q, Search Setup	ו 🖶	? ‡	* 👸
Setup Home Object	Manager 🖌	🔯 Setup	C <sup>R</sup>	
> Development		-		12
> Environments	Single Sign On Setting	Manage Subscripts	pm.	
> User Engagement	Single Sign-On Settings	Developer Console		
> Integrations				
> Notification Builder	Single Sign-On Settings		Help for	this Page 😣
SETTINGS	Configure single sign-on in order to authenticate users in salesforce com from external environments. Your organization has the following options available for single sign-on:			
> Company Settings	<ul> <li>Delegated authentication is a single sign-on method that uses a Web service call sent from salestocic com to an endpoint.</li> <li>Pederated authentication, a single sign-on method that uses SAML assertions sent to a Salestorce endpoint.</li> </ul>			
> Data Classification	Edit SAM, Assortion Validator			
✓ Identity	Delegated Authentication			
Auth. Providers	Disable login with Sales/lorge credentials 1			
Identity Provider				
Identity Provider Event Log	Pedersted Single Sign-On Using SAML			
Identity Verification				
Identity Verification History	SAML Single Sign-On Settings New New York Headers File New York Headers (RL)			
Login Flows	No SAM, Single Sign Cri Settings			
Login History				
OAuth Custom Scopes				
Single Sign-On Settings				
> Security				

3. On the Single Sign-On Settings page, click Edit.



4. Select the SAML Enabled check box to enable the use of SAML SSO. Click Save.

Single Sign-On Setting	S	
		Save Cancel
Delegated Authentication		
Disable login with Salesforce credentials	i	
Federated Single Sign-On Using SAM	۸L	
SAML Enabled		
		Save

#### 5. Click New From Metadata File.

SAML Single Sign-On Settings	New New from Metadata File New from Metadata URL
No SAML Single Sign-On Settings	

6. Click Choose File, select the SAML metadata file that you downloaded from PingOne for Enterprise, and click Create.

# SAML Single Sign-On Settings Create configuration using an XML file (1 MB or smaller) containing SAML 2.0 settings Create Cancel Metadata File Choose File No file chosen Create Cancel

The summary screen opens.

7. On the **Identity Provider Certificate** line, click **Choose File** and select the signing certificate that you downloaded from PingOne for Enterprise.

#### 8. Set Service Provider Initiated Request Binding to HTTP POST.

#### 9. Set Single Logout Request Binding to HTTP POST.

10. Clear the Single Logout Enabled check box if you don't require single logout.

The summary screen will resemble the following:

	Save Save & New Cancel		
Name	pingone	API Name	pingone
SAMI, Version	2.0		
Issuer	https://pingone.com/idp/cd-1.	Entity ID	https://g=stiellmy.salesforce.
Identity Provider Certificate	Choose File pingone-signing (1) crt	Current Certificate	CN=PingOne Account Origination Certificate (2021), O=Ping Identity, L=Denver, ST=CO, C=US Expiration: 21 Jan 2024 17:14:52 GMT
<b>Request Signing Certificate</b>	SelfSignedCert_02Feb2021_175028 V		
Request Signature Method	RSA-SHA256 ¥		
Assertion Decryption Certificate	Assertion not encrypted		
SAML identity Type	Assertion contains the User's Salesbuce username     Assertion contains the Federation (D from the User object     Assertion contains the User ID from the User object		
SAML Identity Location	letently is in the Nameldentifier element of the Subject statement     letently is in an Athibute element		
vice Provider Initiated Request Binding	HTTP POST     HTTP Redirect		
	Warning: The metadata file specifies multiple bindings for the login URL		
Identity Provider Login URL	https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=60b6cc34-11-		
Custom Logout URL			
Custom Error URL			
Single Logout Enabled			
Selected Request Signature Method for			
Identity Provider Single Logout URL	https://sso.connect.pingidentity.com/sso/SLO.sami2		
Single Logout Request Binding	@ HTTP POST		

- 11. Ignore the metadata file warnings and click Save.
- 12. Click Download Metadata to save the Salesforce metadata.

Endpoints View SAML endpoints for your organization	n, communities, or custom domains.
Your Organization	
Login URL	https://j ++ + = imy.salesforce.com
Logout URL	https://j += +=fi='.my.salesforce.com/services/auth/sp/saml2/logout
OAuth 2.0 Token Endpoint	https://umiliai.my.salesforce.com/services/oauth2/token
	Edit Delete Clone Download Metadata SAML Assertion Validator

#### Import the Salesforce metadata into PingOne.

- 1. Sign on to PingOne for Enterprise and go to **Applications**  $\rightarrow$  **My Applications**.
- 2. Expand the Salesforce entry and click Edit.
- 3. Click Continue to Next Step.
- 4. Click **Select File** and select the metadata file that you downloaded from Salesforce.

Assign the attribute values for single sig	n-on (SSO) to the application.
Upload Metadata 🏾 🔘	Select File Or use URL

The ACS URL, Entity ID, Single Logout Endpoint, and Primary Verification Certificate fields should now be populated.

Application Name	Type Status		Enabled
Salesforce	SAML Active		Yes
2. Connection Configuration			
Assign the attribute values for single sign	n-on (SSO) to the application.		
Upload Metadata 🛛 😡	Uploaded file:SAMLSP-00D4L00000 Select File Or use URL	0CzhM (2).xml	
ACS URL	https://prooffd.my.salesforce.com	*	
Entity ID	https://	*	
Target Resource 🗑			
Single Logout Endpoint @	https://	rvic	
Single Logout Response Endpoint @	example.com/sloresponse.endpoint		
Primary Verification Certificate	Choose File No file chosen sami20metadata.cer		
Secondary Verification Certificate	Choose File No file chosen		
Force Re-authentication @			
Encrypt Assertion			
Signing 📦	Sign Assertion O Sign Response	e	
Signing Algorithm @	RSA_SHA1 V		

5. Click Continue to Next Step on the remaining pages then click Finish.

#### i) Note

This step assumes that your usernames in Salesforce match the ones in PingOne for Enterprise. If this is not the case, then you must map the expected Salesforce username value on the third page.

#### Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to your Ping desktop as a user with Salesforce access.

#### (i) Note

To find the Ping desktop URL in the Admin console, go to Setup  $\rightarrow$  Dock  $\rightarrow$  PingOne Dock URL.

2. Complete PingOne for Enterprise authentication.

You're redirected to your Salesforce domain.

Al V Q Search	* 🖬 ? 幸 🖡 👩
Sales Home Getting Started Accounts v Contacts v Leads v Opportunities v Tasks v Calendar v Dashboard	ds 🗸 Notes 🗸 Reports 🗸 Groups 🗸 Forecasts. More 🔻 🖋
Quarterly Performance As of 15 Oct 2018 B:34 AM	Assistant
CLOSED E69,000 CMEN(+70%) E184,500 GOAL E250,000 /	Acres 1,200 Widgets (Sample)
10x	> 20 days without any activity Acme : 1250 Wiegets (Sample) 11 🗰 🗙
1775	> 20 days without any activity Global Media - 560 Widgets (Sample)
200	> 🔛 30 days without any activity Global Media - 1750 Widgets (Sample) 🛛 🟦 🗮 🗙
10x	> 🔛 30 days without any activity salesdores com - 200 Widgets (Sample) 18 🐻 🗙
10x	> 20 days without any activity salesdore.com - 230 Widges (Sample) TE B X
	> 20 days without any activity Aprile - 150 Widgets (Sample) 12 🗃 🗮 🗙
	Strain St
0 Dec Dec	> 📴 30 days without any activity salesforce.com - 320 Widgets (Sample) 111 🗃 🗶
Closed Goal Closed • Open (>70%)	> 🔛 30 days without any activity Acres - 200 Widgets (Sample)
Today's Tasks 🛛 🖉 💌 Today's Events	
Pathenal in adde Lineared an Ambra (Canada)	

### Configure direct Salesforce sign on using PingOne (SP-initiated login) plus SLO

#### Before you begin

• You must first enable identity provider (IdP)-initiated sign-on.

#### Enable PingOne authentication in Salesforce

- 1. Sign on to your Salesforce domain as an administrator.
- 2. Click the **Gear** icon, then go to **Setup**  $\rightarrow$  **Company Settings**  $\rightarrow$  **My Domain**.



3. Make a note of your domain name, for example, https://your-company.my.salesforce.com

4. In the Authentication Configuration section, click Edit.

Authentication Configuration	Edit
Login Page Type	Standard
Authentication Service	Login Form
Logo File	
Background Color	
Right Frame URL	
Use the native browser for user authentication on iOS	
Use the native browser for user authentication on Android	

5. In the Authentication Service list, select PingOne. Click Save.



#### (j) Note

This entry was created as a result of the IdP-initiated sign-on task.

Configuration is complete.

#### (i) Note

Salesforce will now redirect to PingOne for authentication of all new sessions. You should also select the **Login Form** check box during the testing phase in case of authentication issues.

Testers will be offered the option of the standard Salesforce login form or PingOne authentication. After you've successfully tested authentication, you can clear the **Login Form** check box so that authentication automatically defaults to PingOne.

#### Test the PingOne SP-initiated SSO integration

1. Go to your Salesforce domain.

#### (i) Note

If the **Login Form** check box is still selected, the Salesforce sign-on screen still displays, and you're offered a choice of Salesforce sign on or PingOne sign, select PingOne. If you've cleared the **Login Form** check box, you're not offered a choice.

2. When you are redirected to PingOne, enter your PingOne username and password.

After successful authentication, you're redirected back to Salesforce.



# **SAP Netweaver**

# **Configuring SAML SSO with SAP Netweaver and PingFederate**

Learn how to configure SAML SSO with SAP Netweaver and PingFederate.

#### Before you begin

Refer to the vendor documentation and complete the following:

- 1. Ensure that HTTPS is enabled for your SAP system.
- 2. Activate Secure Session Management.
- 3. Enable SAML 2.0 support:
  - 1. Create a local provider.
  - 2. Export metadata for local provider.

#### About this task

The following table details the required and optional attributes to be configured in the assertion attribute contract.

Attribute Name	Description	Required / Optional
SAML_SUBJECT	Username	Required

#### Create a PingFederate SP connection for SAP Netweaver

#### γ Νote

The following configuration is untested and is provided as an example. Additional steps might be required.

- 1. Sign on to the PingFederate administrative console.
- 2. Using the details retrieved from SAP Netweaver:
  - 1. Configure using Browser SSO profile SAML 2.0.
  - 2. Enable the following SAML Profiles:
    - IdP-Initiated SSO
    - SP-Initiated SSO

- In Assertion Creation: Attribute Contract, set the Subject Name Format to urn:oasis:names:tc:SAML:1.1:nameidformat:unspecified.
- 4. In Assertion Creation: Attribute Contract Fulfilment, map the attribute SAML\_SUBJECT to the attribute username.

This should match the username for the user in SAP Netweaver.

- 5. In Protocol Settings: Allowable SAML Bindings, enable Post and Redirect.
- 3. Export the metadata for the newly-created SP connection.
- 4. Export the signing certificate public key.

#### Configure the PingFederate IdP connection for SAP Netweaver

- 1. Sign on to SAP Netweaver as an administrator.
- 2. Go to Trusted Partners and select Identity Providers.
- 3. Click Add.
- 4. Click Upload Metadata File, select the file that you downloaded from PingFederate, and click Next.
- 5. On the Provider Name page, verify the data populated. Click Next.
- 6. On the Signature and Encryption page, verify the data populated. Click Next.
- 7. On the Single Sign-On Endpoints page, verify the data populated. Click Next.
- 8. On the Single Logout Endpoints screen, verify the data populated. Click Next.
- 9. Select Binding as HTTP POST. Click Finish.
- 10. Enable the provider.
- 11. Configuration is completed.

After testing, you can enable SP-initiated SSO for SAP Netweaver by editing the configuration in sap/opu/odata/iwfnd/ catalogservice.

## Configuring SAML SSO with SAP Netweaver and PingOne for Enterprise

Learn how to configure SAML SSO with SAP Netweaver and PingOne for Enterprise.

#### Before you begin

Refer to the vendor documentation and complete the following:

- 1. Ensure that HTTPS is enabled for your SAP system.
- 2. Activate Secure Session Management.
- 3. Enable SAML 2.0 support:
  - 1. Create a local provider.

2. Export metadata for local provider.

#### About this task

The following table details the required and optional attributes to be configured in the assertion attribute contract.

Attribute Name	Description	Required / Optional
SAML_SUBJECT	Username	Required

#### Create a PingOne for Enterprise application for SAP Netweaver

#### (i) Note

The following configuration is untested and is provided as an example. Additional steps might be required.

- 1. Sign on to PingOne for Enterprise and click **Applications**.
- 2. On the SAML tab, click Add Application.

G admin.)	pingone.com/web-portal/cas/connec	tions#/				ਸ	 9
SAML C	DIDC						
Applications y	you've added to your account are liste	ed here. You can search b	by application name	description or entityId			
<ul> <li>Details dis</li> </ul>	splays the application details.	-01 (550).					
	Application Name	Туре	Status	Enabled			
₹Ь	BambooHR	SAML	Active	Yes	Remove		
box	Вох	SAML	Active	Yes	Remove		
	Dropbox	SAML	Active	Yes	Remove		
	simpleSAMLphp	SAML	Active	Yes	Remove		
>	Splunk Cloud	SAML	Active	Yes	Remove		
Add Applica	ation -				Pause All SSO	0	
Search Ap	plication Catalog						
New SAM	L Application						
Request P	Ping Identity add a new application to	the application catalog					

- 3. Enter the following:
  - A suitable Application Name, such as SAP Netweaver .
  - A suitable Application Description.

- $^\circ$  A suitable  ${\mbox{Category}},$  such as  ${\mbox{Information Technology}}$  .
- $^\circ$  (Optional) Upload an icon to be used in the PingOne for Enterprise dock.

P1 PingOne	- My Applications × +			-	.		×
← → C	admin.pingone.com/web-portal/cas/connections	#/		☆	*	Θ	:
	New Application	SAML Incomplet	No				1
	1. Application Details						
	Application Name	SAP Netweaver	^				
	Application Description	SAP Netweaver	•				
		Max 500 charac	iers				
	Category	Information Technology	]*				
	Graphics	Application Icon					
	1	For use on the dock					
		No Image Assellation					
		Change					
	1	Max Size: 256px x 256px					

- 4. Click Continue to Next Step.
- 5. Select I have the SAML configuration.
- 6. In the **Signing Certificate list**, select a suitable signing certificate.
- 7. For Protocol Version, click SAML v.2.0.

P	PingOne	- My Applications × +		-			×
÷	$\rightarrow$ C	admin.pingone.com/web-portal/cas/connection	ons#/	7	* (	8	:
		You will need to download this SAML metad	ata to configure the application:				*
		Signing Certificate @	PingOne Account Origination Certificate (2021)				
		SAML Metadata	Download				
		Provide SAML details about the application	you are connecting to:				
		Protocol Version	● SAML v 2.0 ○ SAML v 1.1				
		Lipload Matadata					
			Select File				
		Assertion Consumer Service (ACS)	·				
		Entity ID @	•				
		Application URL @					
		Single Logout Endpoint @					
		Single Logout Response Endpoint @					
		Single Logout Binding Type 💿	● Redirect ○ Post				
		Primary Verification Certificate @	Choose File				
		Secondary Verification Certificate @	Choose File No file chosen				
							-

- 8. Upload the metadata from your SAP Netweaver local provider configuration.
- 9. Click Continue to Next Step.
- 10. In the SSO Attribute Mapping section, add the following mapping for the SAML\_SUBJECT:
  - For **Identity Bridge Attribute or Literal Value**, select the appropriate attribute. This should match the username for the user in SAP Netweaver.
  - $\,\circ\,$  Select the Required check box.

P	Pin	gOne -	My Applications	× +						-		×
←	$\rightarrow$	G	admin.pingon	e.com/web-portal/cas/conne	ections#/					☆	* 0	) :
				simpleSAMLphp	SAML	Active	Ye	5	Remove			^
			>	Splunk Cloud	SAML	Active	Ye	:5	Remove			
				New Application	SAML	Incomplete		No				
			3. SSO Attribu Map the n	te Mapping ecessary application provi	ider (AP) attributes to a	attributes used by you	ır identity provid	ier (IdP).				
				Application Attribute	Identity Br	ridge Attribute or Literal	Value	Req	uired			
					SAML_	SUBJECT						- 1
			1	SAML_SUBJECT	As Liter	ral 1			×			
			Add new	v attribute		Can	cel Back	Continue to Next Ste	p Save & Exit			
	0	2003	- 2021 Ping Identity (	Corporation. All rights reserve	ed.				Privacy	Terms	About	
												· · ·

#### 11. Click Continue to Next Step.

12. Add the user groups for the application.

1	P1 Pi	ingOne -	- My	Applicat	tions x +		-		×
<	-	⇒ C		🗎 adn	min.pingone.com/web-portal/cas/connections#/	4	. 1	• 6	) E
			4. Group Access Select all user groups that should have access to this application. Users that are members of the added groups will be able to SSO to the see this application on their personal dock.		his applicatior	n and	will	^	
					Group1, Group2, etc Search				
					Group Name Domain Administrators@directory	Remove			
					Users@directory	Remove			
				N	EXT: Review Setup	Continue to N	ext S	ер	

#### 13. Click Continue to Next Step.

14. Review the settings.
| PingOne - My Applications X +  | -  |     | ×   |
|--|--|-----|-----|
| $\leftrightarrow$ $\rightarrow$ C $($ admin.pingone.com/web-portal/cas/connection                        | ns#/ 🏠   | * 0 | :   |
| New Application  | SAML Incomplete No   |     | ^   |
| 5. Review Setup  |  |     |     |
| Test your connection to the application  |  |     |     |
| lcon 6   |  |     |     |
| Name @   | SAP Netweaver  |     |     |
| Description @  | SAP Netweaver  |     |     |
| Category @   | Information Technology   |     |     |
| Connection ID  |  |     |     |
| (Optional) Citick the link below to in<br>Invite SAAS Admin<br>These parameters may be needed to configu | vite this SaaS Application's Administrator to register their SaaS Application with PingOne.<br>Ire your connection |     |     |
| saasid   |  |     | - 1 |
| Issuer   | https://pingone.com/idp/   |     |     |
| idpid  |  |     |     |
| Protocol Version   | SAML v 2.0   |     |     |
| ACS URL @  |  |     |     |
| entityld ⊚<br>Initiate Single Sign-On (SSO) URL ⊚  | https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=  |     | Ŧ   |

15. Copy the Single Sign-On (SSO) URL value to a temporary location.

This is the IdP-initiated SSO URL that you can use for testing.

- 16. Note the **idpid** and **Issuer** values.
- 17. On the Signing Certificate line, click Download.

You'll use this for the application configuration.

18. On the SAML Metadata line, click Download.

You'll use this for the application configuration.

19. Click Finish.

### Configure the PingOne for Enterprise IdP connection for SAP Netweaver

- 1. Sign on to SAP Netweaver as an administrator.
- 2. Go to Trusted Partners and select Identity Providers.
- 3. Click Add.
- 4. Click Upload Metdata File, select the file that you downloaded from PingOne for Enterprise, and click Next.
- 5. On the **Provider Name** page, verify the data populated. Click **Next**.

- 6. On the Signature and Encryption page, verify the data populated. Click Next.
- 7. On the **Single Sign-On Enpoints** page, verify the data populated. Click **Next**.
- 8. On the Single Logout Endpoints page, verify the data populated. Click Next.
- 9. Select Binding as HTTP POST. Click Finish.
- 10. Enable the provider.

After testing, you can enable SP-initiated SSO for SAP Netweaver by editing the configuration in sap/opu/odata/iwfnd/ catalogservice.

326

# ServiceNow

# Configuring SAML SSO with ServiceNow and PingOne for Enterprise

Learn how to configure SAML SSO with ServiceNow and PingOne for Enterprise

### About this task

The following table details the required and optional attributes to be configured in the assertion attribute contract.

Attribute Name	Description	Required / Optional
NameID	NameID and format is configurable in ServiceNow. This guide uses email.	Required

The following table details the references that are used within this guide that are environment specific. Replace these with the suitable value for your environment.

Reference	Description
tenant	The instance name for your ServiceNow tenant you want to integrate with PingOne for Enterprise.

# Create a PingOne for Enterprise application for ServiceNow

- 1. Sign on to PingOne for Enterprise and go to **Applications**  $\rightarrow$  **Application Catalog**.
- 2. Search for **ServiceNow** and then click the **ServiceNow** row.

Application Request Form.
▲ Applications / Application Catalog ut our Application Request Form.
ut our Application Request Form.
•
•
•

## 3. Click Setup.

4. Review the steps and make a note of the PingOne SaaS ID, IdP ID, Single Sign-on URL, and Issuer values.

Application N	me • Type		
ServiceNow	SAML with Provisioning (API)		
1. SSO Instructions			1
Signing Certificate	PingOne Account Origination Certificate (2021)		
F	r reference, please note the following configuration parameters:		
SaaS ID			
IdP ID			
Initiate Single Sign-On (SSO) URL @	https://sso.connect.pingidentity.com/sso/sp/initsso?	15	1
Issuer	https://pingone.com/idp/		
T S O	configure Single Sign-On for Service-Now, navigate to the SAML 2.0 Single Sign-On properties". If you do not have the SAML 2.0 Single Sign-On plugin, please contact Sen poort who can assist you in obtaining the plugin. Follow the Configuration steps below infiguration within the ServiceNow Single-Sign On plugin.	plug-in and select viceNow customer to complete the	
SAML 2 Single Sign-On ->	roperties		
Log in to the SaaS Provide			
1000	Description		
Cana -			

## 5. Click Continue to Next Step.

### 6. Verify the following:

- ACS URL is set to https://tenant.service-now.com/navpage.do.
- Entity ID is set to https://tenant.service-now.com.

PingOne	- Application Catalog × +			Į.	×
← → C	admin.pingone.com/web-portal/cas/application	oncatalog?x=lcyuSUNHa60	\$ *	θ	1
j.	Application Name	* Туре			•
	serviceNow	SAML with Provisioning (API)			
	2. Connection Configuration				Ì
	Assign the attribute values for single sig	n-on (SSO) to the application.			
	Upload Metadata	Select File Or use URL			
	ACS URL	service-now.cor *			
	Entity ID	service-now.cor			ł
	Target Resource @				
	Single Logout Endpoint @	example convisio endpoint			
	Single Logout Response Endpoint @	example convisioresponse endpoint			
	Primary Verification Certificate @	Choose File No file chosen			
	Secondary Verification Certificate @	Choose File No file chosen			
	Force Re-authentication @	0			

### 7. Click Continue to Next Step.

8. In the **Attribute Mapping** section, in the **Identity Bridge Attribute or Literal Value** column of the **SAML\_Subject** row, select a suitable attribute, such as **SAML\_SUBJECT**.

> C	admin.pingone.com/web-porta	l/cas/applicationcatalog?x=lcyuSUNHa60			* *	<b>e</b> :
	10 A		10 1 C			
	servicenow	Search				
	Application Nam	е * Туре				
	ServiceNow	SAML w	th Provisioning (API)			
	3. Attribute Mapping Map your identity bridge at	ributes to the attributes required by the a	pplication.			
	3. Attribute Mapping Map your identity bridge att Application Attribu	ributes to the attributes required by the a te Description	pplication. Identity Bridge Attribute or Litera Value	1		
	3. Attribute Mapping Map your identity bridge att Application Attribut 1 SAML_SUBJEC	ributes to the attributes required by the a te Description T Identifies the authenticated principal	pplication. Identity Bridge Attribute or Litera Vakue SAML_SUBJECT			

NameID is configurable in ServiceNow.

# (i) Note

This guide assumes email is used and that **SAML\_SUBJECT** contains the email address for the user in PingOne for Enterprise.

- 9. Click Continue to Next Step.
- 10. Update the Name, Description, and Category fields as required.

4	→ C	i admin.pingo	ne.com/web-portal/cas/applicationc	italog?x=Icyu5UNHa60	Ŷ	* (	9	1
			000455200-00000-00040-00-0		_			
			Application Name	* Type				
			ServiceNow	SAML with Provisioning (API)				
		4. PingOne Ap	p Customization - ServiceNow Icon ⊕ Name ⊕	Select image ServiceNow				
			Description e	ServiceNow is a leading provider of cloud-based services that automate enterprise IT operations. Provisioning is supported for ServiceNow versions Orlando, New York and Madrid.				
			Category e	intornation systems				
		NEXT: Group	Access	Cancel Back Continue to Nex Ste	P			

# 11. Click Continue to Next Step.

12. Add suitable user groups for the application.

P1 PingOne -	Application Catalog × +	<u>~</u>			×
← → C	admin.pingone.com/web-portal/cas/applicationcatalog	☆	* (	9	:
	5. Group Access Select all user groups that should have access to this application. Users that are members of the added groups will be able to SSO to this see this application on their personal dock.	s application	on and w	vill	
	Group1, Group2, etc Search				
	Group Name	-			
	Domain Administrators@directory	Ren	nove		
	Users@directory	Ren	nove		
	NEXT: Review Setup	ontinue to I	Next Ste	р	
-					•

# 13. Click Continue to Next Step.

14. Review the settings.



### 15. Copy the Single Sign-On (SSO) URL value to a temporary location.

This is the IdP-initiated SSO URL that you can use for testing.

## (i) Note

Make a note of the following values. You'll use them later in the ServiceNow configuration:

- PingOne for Enterprise Issuer
- PingOne for Enterprise idpid

### 16. On the SAML Metadata line, click Download.

You will use this later for the ServiceNow configuration.

### 17. On the Signing Certificate line, click Download.

You will use this later for the ServiceNow configuration.

### 18. Click Finish.

Applications y	ou've added to your account are liste	d here. You can scarch	by application name.	description or entityId		
<ul> <li>Active app</li> <li>Details dis</li> </ul>	plications are enabled for single sign- splays the application details.	on (SSO).				
0:	Application Name	Туре	Status	Enabled		
	Atlassian Cloud	SAML	Active	Yes	Remove	
*6	BambooHR	SAML	Active	Yes	Remove	
box	Box	SAML	Active	Yes	Remove	
	Confluence	SAML	Active	Yes	Remove	
	Dropbox	SAML	Active	Yes	Remove	
	ServiceNow	SAML	Active	Yes	Remove	
	simpleSAMLphp	SAML	Adhe	Yes	Remove	
	Snowflake	SAML	Active	Yes	Remove	
>	Splunk Cloud	SAML	Active	Yes	Remove	

## Configure the PingOne for Enterprise IdP connection for ServiceNow

- 1. Sign on to ServiceNow as an administrator.
- 2. Activate SAML 2.0:
  - 1. Go to System Applications.

- 2. Click All Available Applications.
- 3. Click All.
- 4. Locate the Integration Multiple Provider Single Sign-On Installer plugin.



5. Check if the plugin is installed. If the plugin is not installed, click Install.

O Internation - Multiple Denoider 1 - W - A		- D ×
← → C ■ service-now.c	/nav to.do?uri=%2Fv plugin.do%3Ftvs i	d%30.integration.sso.multi.installer%26sysparm_stack%3D5allaposmo 💁 🕁 🗴 🗛 🕴
		Q 관 () 않
( Filter navigator	System Plugin Integration - Multiple Provider Sing	je Sigi-On installer 🗄 👓 🗧
Standard Ticket	ID com.snc.integration.ssc	amult.in: Provider ServiceNow
State Management	Name Integration - Multiple Pr	Status Active
Subscription Management		
System Applications	Help Tabiluowiki/course ook	un/munipe Provoer single sign-om
Getting Started	Requires	
Studio	Description The multiple providers (identity providers) usin it also supports authen	ingle sign-on plugin enables organizations to authenticate against multiple IDPs ig SANL scatton using multiple digest configurations.
▼ All Available Applications	Valated Links	
All	ctivate/Repair	
testalled	oad Demo Data Only	
Available To Obtain From Store	Plugin Activation Logs (12) Plugin Files (1)	
ServiceNow Products	Plugin Activation Logs	4 4 1 to 12 of 12 >> >> 🗁
My Company Applications	② ≡ Created ≡ Status	≡ Log
•	() <u>2019-12-11</u> Info 08:49-20 Info	Plugin activated/upgraded successfuly

- 3. Configure a new identity provider:
  - 1. In the left navigation pane, select **Multi-Provider SSO**.

O Identity Froviders   ServiceN	iow × +							- 0 ×
← → C 🔒	service-now.c	com/nav_to.do	?uri=%2Fsso_prop	erties_list.do%	63Fsysparm_first_row%3D1%	26sysparm_query%3DGOTC	DnameSTAR	° ☆ * 🛛 :
servicenow service	e Management							Q 🗗 🖗 🖨
(y sso	8	E Identity	Providers New	Search Nam	w v Search			
⊡ ★	©		me starts with _	Active		≡ Single Sign-On Script	≡ Default	■ Auto Redirect IdP
Multi-Provider SSO	i		-	Search	Search	Search	Search	Search
Identity Providers  Federations  Federations  Fooperties  x500 Certificate  installation Exits  Single Sign-On Surlyds  Configuration  Base Rems Accessories					No records to a	display		đ
0								

- 2. Click Identity Providers.
- 3. Click New.
- 4. Click SAML.



- 5. Click XML.
- 6. Paste the contents of the PingOne for Enterprise metadata file that you previously downloaded into the **Enter the XML** field.



7. Update the NameID Policy to urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified.

### 8. Click Update.

#### 9. Click Test.

A browser window opens to validate the configuration. It prompts you to authenticate at the IdP and then sign out of the session. If successful, you can then activate the connection.

#### 10. Click Activate.

If you receive an error stating that you must test the connection, something failed in the test. Validate the settings, and use the Script Debugger  $\rightarrow$  Debug log to re-run the test to determine the cause of the failure.

O https://pingone.com/idp/cd-74/ × +					- 0 ×
← → C ■ service-now.c	om/nav_to.do?uri=%2	FsamI2_update1_properties.do%3Fsys_	id%3Daea018891ba22810d7692	026ec4bcb3d%26sy	• ☆ <b>* ⊖</b> :
Service Management	-				Q 🗗 🖗 👹
(Y 550 🛞	<  it identity P https://pi	rovider ngone.com/idp/	Update	Ø Generate Metadata	√ ∄ oso ↑ ↓ Test Connection Activate
🖻 ★ 🕓					
Multi-Provider SSO	* Name	https://pingone.com/idp/cd-740	Active		Í
Getting Started	Default		Auto Redirect IdP		
identity Providers	* Identity	https://pingone.com/idp/td			
Federations	Provider URL				
▼ Administration	⇒ Identity Provider's AuthnReguest	https://so.connect.pingidertity.com/sos/i	dp/550.saml27idpid-		
Properties	Identity Provider's	https://sso.connect.pingidertity.com/sso/5	E.O. saml2		
x509 Certificate	SingleLogoutRequest				
Installation Edits	* ServiceNow Homepage	https:// service-now.com/navpag	e.do		
Single Sign-On Scripta	* Entity ID / Itsuer	https:///service-now.com			
Configuration	* Audience URI	https:// service-now.com			
▼ Base items	* NametD Policy	um.oasismames.tc:SAML:1.1:nameid-form	aturnspecified		
Accessories	External logout	external lossout complete.do			
0	redirect Failed				-

# Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to the **Single Sign-On (SSO) URL** from the PingOne for Enterprise application configuration to perform IdP-initiated SSO.

For example, https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=saasid&idpid=idpid

	Ping	
	Sign On	
USERNAME		- 1
PASSWORD		- 1
	Remember Me	- 1
	Sign On	
	Forgot Pessword	- 1



# Test the PingOne for Enterprise SP-initiated SSO integration

1. Go to your ServiceNow URL.

For example, https://your-environment.service-now.com

	Ping
	Sign On
USERNAME	
PASSWORD	
	Remember Mc
	Sign On
	Forgot Password

O ServiceNow	× +	- 0
- > C 💶	service-now.com	🕶 🖈 🍮 Incognito
ervicenow s	svice Kanagement	
User name		
Password		
Forgot Password 7	Login	
Use external login		
out ServiceNow rviceNow is changing the	way people work. With a service-orientation toward the activities, tasks and processes that ma	ke up day-to-day work life, we help the modern enterprise operate faster and be more
alable than ever before. C rvices for the enterprise. perience through our ent	istomers use our service model to define, structure and automate the flow of work, removing o envice/ow provides service management for every department in the enterprise including IT, h sprisecloud – built to manage everything as a service. To find out how, visit www.servicenow.ce	Jependencies on email and spreadsheets to transform the delivery and management of human resources, facilities, field service and more. We deliver a 'lights-out, light-speed' com.
		ð

## 2. Click Use external login.



### 3. Click Submit.

### 4. Click Continue.

You're redirected to PingOne for Enterprise for authentication.

5. After you're redirected to PingOne for Enterprise, enter your PingOne username and password.

	Ping	
	Sign On	
USERNAME		- L
PASSWORD		
	Hemember Mc	- 1
	Sign On	
	Forgot Pessword	



# Slack

# **Configuring SAML SSO with Slack and PingFederate**

Enable Slack sign-on from a PingFederate URL (IdP-initiated sign-on) and direct Slack sign-on using PingFederate (SP-initiated sign-on) with JIT provisioning.

### Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users that require application access.
- You must have administrative access to PingFederate and Slack.

## **Create a PingFederate SP connection for Slack**

- 1. Sign on to the PingFederate administration console.
- 2. Create a service provider (SP) connection for Slack in PingFederate:
  - 1. Configure using Browser SSO profile SAML 2.0.
  - 2. Set Partner's Entity ID to https://slack.com.
  - 3. Enable the following SAML Profiles:
    - IdP-Initiated SSO
    - SP-Initiated SSO
  - 4. In Assertion Creation > Attribute Contract, extend the contract with the following attributes:
    - SAML\_NAME\_FORMAT
    - User.Email
    - User.Username
    - first\_name
    - last\_name

Use the following attribute name format:

urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified

5. In Assertion Creation → Authentication Source Mapping → Attribute Contract Fulfillment:

1. Map SAML\_SUBJECT, User.Email, User.Username, first\_name, and last\_name.

2. Map **SAML\_NAME\_FORMAT** to a text value of **urn:oasis:names:tc:SAML:2.0:nameid-format:persistent**.

- 6. In **Protocol Settings** → **Assertion Consumer Service URL**, set the following properties:
  - Set Binding to POST.
  - Set Endpoint URL to https://your-slack-domain.slack.com/sso/saml.
- 7. In **Protocol Settings** → **Allowable SAML Bindings**, enable **POST** and **REDIRECT**.
- 8. In Protocol Settings → Signature Policy, select Always Sign Assertion.
- 9. In Credentials → Digital Signature Settings, select the PingFederate Signing Certificate.
- 3. Save the configuration.
- 4. Export the signing certificate.
- 5. Export the metadata file, open it in a text editor, and copy:
  - The entityID
  - The Location entry, https://your-value/idp/SS0.saml2

## Add the PingFederate connection to Slack

### Choose from:

### For Slack Standard or Plus, do the following

- 1. Sign on to your Slack Workspace as an administrator.
- 2. Go to Settings & Administration  $\rightarrow$  Workspace Settings.

D

Invite people to     <b>        </b>     : Create a channel		5:22 PM	
Preferences		Joined #sso-integration.	
Settings & administration	>	Settings	
		Workspace settings	
Tools	>	Customize	

- 3. Click the Authentication tab.
- 4. In the Configure an authentication method section, on the SAML authentication line, click Configure.

Settings	Permissions	Authentication	Attachments	Access Logs
Slack suppo below, or le	orts a number of single arn more about using	e sign-on (SSO) services. single sign-on with Slac	. Get started with setting up yo ck.	our workspace's SSO
Configur	e an authentica	tion method		
G G	oogle Apps authent	tication In a Google account.		Configure
ි G	AML authentication et set up with Azure, (	<b>)</b> Okta, and OneLogin, or y	your custom SAML 2.0 solutior	Configure

- 5. If prompted, enter your password to continue.
- 6. In the SAML 2.0 Endpoint (HTTP) field, enter the PingFederate Location value.
- 7. In the Identity Provider Issuer field, enter the PingFederate entityID value.
- 8. In the **Public Certificate** field, paste in the contents of the PingFederate signing certificate.

Enter your SAML 2.0 Endpoint. This is where you go when you try to login.	https://
Custom SAML Instructions	
dentity Provider Issuer	
The IdP Entity ID for the service you use.	
Public Certificate	
darren.scragg@proofid.com (), expiri	ng January 21st, 2024 (edit)
Copy and paste your entire x 509	BEGIN CERTIFICATE

9. Expand the Advanced Options section, and clear the Assertions Signed check box.

Advanced Options	
Sign AuthnRequest	
AuthnContextClassRef	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransp
	The RequestedAuthncontext Slack will send in authentication requests to your identity provider.
Service Provider Issuer	https://slack.com
	The SP Entity ID you would like us to send. By default, this is https://slack.com.
Choose how the SAML respon	se from your IDP is signed. You must choose at least one option.
Assertions Signed	

10. In the Settings section, select the It's optional radio button for the authentication setting.



11. Click Save Configuration.

Sign In Button Label	Button Previ	ew
Custom Label	ଙ	Sign in with Ping
Do you have a nickname for your SSO system? Add it to the Sign In Button!	This is what yo	our Sign In Button will look like.
Save Co	nfiguration	

12. When you're redirected to PingFederate, authenticate with PingFederate.

Your selection is confirmed against PingFederate and saved if successful.

## For Slack Enterprise Grid, do the following

- 1. Sign on to your Slack Organization (not Workspace) as an administrator.
- 2. Go to Manage Organization  $\rightarrow$  Security  $\rightarrow$  SSO Settings  $\rightarrow$  Configure SSO.



- 3. In the SAML 2.0 Endpoint (HTTP) field, enter the PingFederate Location value from the metadata file.
- 4. In the Service Provider Issuer URL, use the default value of https://slack.com.
- 5. In the Public (X.509) Certificate field, enter the contents of your PingFederate signing certificate.
- 6. Enable authentication request signing.
  - 1. Select the Sign the AuthnRequest check box.
  - 2. Copy the certificate text.
  - 3. Create a new .crt file on your computer and paste the certificate text.
  - 4. In PingFederate, import the .crt file as a trusted certificate authority. For help, see Manage Trusted Certificate Authorities <sup>□</sup> in the PingFederate documentation.
- 7. Clear the Sign the Assertion check box.

SA	ML Response Signing
Ch	oose how the SAML response from your identity provider is signed (you must choose at
lea	ist one option).
	Sign the Response

Sign the Assertion

## 8. Click Test Configuration.

9. Sign out of Slack and then sign back on using SSO.

## Test the PingFederate IdP-initiated SSO integration

- 1. Go to the PingFederate SSO application endpoint for the Slack SP connection.
- 2. Complete the PingFederate authentication.

Damen Ters *	Ø	•   🗰	Ø	Details E-men.iz		
Get started Next: Assemble the team					-	
© Slack Connect	NEW				2	
* Channels				6	antas,	<b>F</b> •
e general e random					Add a title	
# sso-integration				EQ	0	
Add channels				Final	Edit	Mary

You're redirected to your Slack domain.

### Test the PingFederate SP-initiated SSO integration

- 1. Go to your Slack domain, <a href="https://your-domain.slack.com">https://your-domain.slack.com</a>.
- 2. Click Sign in with Ping.

Customize		
Sign In Button Label	Button Prev	iew
Custom Label	ୈ	Sign in with Ping
Do you have a nickname for your SSO system? Add it to the Sign In Button!	This is what y	our Sign In Button will look like.
Save Co	nfiguration	

3. After you're redirected, enter your PingFederate username and password.

After successful authentication, you're redirected back to Slack.





# Configuring SAML SSO with Slack and PingOne for Enterprise

Enable Slack sign-on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct Slack sign-on using PingOne for Enterprise (SP-initiated sign-on) with JIT provisioning.

### Before you begin

- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- You must have administrative access to PingOne for Enterprise and Slack.

### Set up the Slack application in PingOne for Enterprise

- 1. Sign on to PingOne for Enterprise and go to Applications  $\rightarrow$  Application Catalog.
- 2. Search for Slack.

Application Catalog				Applications / Application Catalog
owse for the ap	plication you want to add or searc	h for it by name.	Don't see the application you're looking for? Fill	out our Application Request Form.
slack		Search		
	Application Name	•	Туре	
÷L.	Slack		SAML with Provisioning (API)	

- 3. Expand the Slack entry and click the **Setup** icon.
- 4. Copy the Issuer and IdP ID values.
- 5. Download the signing certificate.

1. SSO Instructions	
Signing Certificate	PingOne Account Origination Certificate (2021) V
F	or reference, please note the following configuration parameters:
IdP ID	
Initiate Single Sign-On (SSO) URL @	
Issuer	

- 6. Click Continue to Next Step.
- 7. Set ACS URL to https://your-slack-domain.slack.com/sso/saml.
- 8. Click Continue to Next Step.
- 9. In the **Attribute Mapping** section, map the attributes to the corresponding attributes in your userstore.

Application Attribut	e Description	Identity Bridge Attribute or Literal Value
	Map your email attribute ('mail' in AD). The NameID format must be set to	SAML_SUBJECT
1 * SAML_SUBJECT	urn:oasis:names:tc:SAML:2.0 nameid-	LIAs Literal
	format persistent, in the Advanced attribute section.	Advanced
		Email (Work)
2 User.Email	Map your email attribute ('mail' in AD).	LAs Literal
		Advanced
	Map the appropriate attribute from	Username
3 User.Username	your user directory.	LJAs Literal
		Advanced
o miliano -	Map the appropriate attribute from	First Name
4 first_name	your user directory.	LAS Literal
		Advanced

10. In the **SAML\_SUBJECT** row, click **Advanced**.

11. In the NamelD Format to send to SP field, enter urn:oasis:names:tc:SAML:2.0:nameid-format:persistent.

### 12. Click Save.

dvanced Attri	bute Options					
dvanced Attrib	ute Options for SAM	L_SUBJECT				
dvanced Att	ribute Options					
ameldFormat O						
lame ID Format to	send to SP:	urn:oasis:names:tc:S	AML:2.0:nameid-for	mat.persistent		
Attribute Map	ping					
ou can build an a	attribute mapping using	multiple scurce attribu	tes, literals and tran	sformation function	s.	
or example, SAN	IL_SUBJECT can be (w	/here each attribute va	lue is a separate er	ntry):		
subject = firstNa	me + "." + lastName + "	@" + domainName				
SAML_SUBJEC	T = SAML_SUBJECT					
IDP Attrib	ute Name or Literal Valu	ue As Literal	Function			Ē
1 SAML	SUBJECT	As Literal			~ 0	
Add Attribute						

# 13. Click Continue to Next Step.

14. Click **Add** for each user group that should have access to Slack.

ee this application on their personal d	ock.	- <u>-</u>
Group1, Group2, etc	Search	
Group Name		
Users@directory		Remo
Domain Administrators@directory		Add

### 15. Click Continue to Next Step.

### 16. Click Finish.

# Add the PingOne for Enterprise IdP connection to Slack

- 1. Sign on to your Slack Admin account as an administrator.
- 2. Go to Settings & Administration  $\rightarrow$  Workspace Settings.

	#ss Add	o-integration ☆ a topic
DT		
Invite people to     <b>     </b>      : Create a channel		5-22 PM
Preferences		joined #sso-integration.
Settings & administration	>	Settings
Tools	>	Workspace settings Customize

3. Click the Authentication tab.

4. In the Configure an authentication method section, on the SAML authentication line, click Configure.

Settings	Permissions	Authentication	Attachments	Access Logs
Slack suppo below, or lea	rts a number of single arn more about using	e sign-on (SSO) services. single sign-on with Slac	. Get started with setting up yo	ur workspace's SSO
Configur	e an authentica	tion method		
G Go	oogle Apps authent	tication		Configure

- 5. If prompted, enter your password to continue.
- 6. In the SAML 2.0 Endpoint (HTTP) field, enter https://sso.connect.pingidentity.com/sso/idp/SSO.saml2? idpid=PingOne-IdP-ID-value.
- 7. In the Identity Provider Issuer field, enter PingOne-Issuer-value.
- 8. In the **Public Certificate** field, paste in the contents of the PingOne for Enterprise signing certificate.

SAML 2.0 Endpoint (HTTP)	
Enter your SAML 2.0 Endpoint. This is where you go when you try to login.	https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid
Custom SAML Instructions	
Identity Provider Issuer The IdP Entity ID for the service you use.	https://pingone.com/idp/cacocc_rozrozrozrozrozrozrozrozrozrozrozrozrozr
Public Certificate	
Copy and paste your entire x.509 Certificate here.	

9. Expand the Advanced Options section and clear the Responses Signed check box.

Advanced Options	
Sign AuthnRequest	
AuthnContextClassRef	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransp
	The RequestedAuthncontext Slack will send in authentication requests to your identity provider.
Service Provider Issuer	https://slack.com
	The SP Entity ID you would like us to send. By default, this is https://slack.com
Choose how the SAML respon	se from your IDP is signed. You must choose at least one option.
Responses Signed	
Assertions Signed	

10. In the Settings section, select the It's optional check box for the authentication setting.

(i) Note
You can change the authentication setting to your desired value after testing has been completed.
Authentication for your workspace must be used by:
<ul> <li>All workspace members</li> </ul>
<ul> <li>All workspace members, except guest accounts</li> </ul>
It's optional

11. Click Save Configuration.

Sign In Button Label	Button Preview	
Custom Label	ୈ	Sign in with PingOne
Do you have a nickname for your SSO system? Add it to the Sign In Button!	This is what	your Sign In Button will look like.

# Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to your Ping desktop as a user with Slack access.

## (i) Note

To find the Ping desktop URL in the Admin console, go to Setup  $\rightarrow$  Dock  $\rightarrow$  PingOne Dock URL.

2. Complete the PingOne for Enterprise authentication.

You're redirected to your Slack domain.



If the user doesn't exist in Slack, you are prompted to accept the Slack terms.

## Test the PingOne for Enterprise SP-initiated SSO integration

- 1. Go to your Slack domain, https://your-domain.slack.com.
- 2. Click Sign in with PingOne.


3. After you're redirected to PingOne for Enterprise, enter your PingOne for Enterprise username and password.

	Ping Sign On	
USERINAME		
музуюно		
	Wemeniber Me	
	Sign Cn	
	Forget Password	

After successful authentication, you're redirected back to Slack.

## (i) Note

If the user doesn't exist in Slack, you are prompted to accept the Slack terms.



#### Next steps

After successful testing, you can change the Slack **It's optional** authentication setting as necessary.

# Splunk

## Configuring SAML SSO with Splunk Cloud and PingFederate

Learn how to configure SAML SSO with Splunk Cloud and PingFederate.

About this task

## (i) Note

An error in configuration could cause users and administrators to be unable to sign on to Splunk Cloud. The following **Direct Login** link can be used for local authentication: https://tenant.splunkcloud.com/en-US/account/login?loginType=splunk.

The following table details the required and optional attributes to be configured in the assertion attribute contract.

Attribute Name	Description	Required / Optional
SAML_SUBJECT		Required
Role	User role as per SAML Groups. Attribute name is configurable in SAML configuration for application.	Required
Email	User Email address. Attribute name is configurable in SAML configuration for application.	Optional
RealName	User display name. Attribute name is configurable in SAML configuration for application.	Optional

The following table details the references that are used within this guide that are environment-specific. Replace these with the suitable value for your environment.

Reference	Description
tenant	The instance name for the Splunk Cloud tenant.

### i) Note

The following configuration is untested, and is provided as an example. Additional steps might be required.

#### **Create a PingFederate SP connection for Splunk Cloud**

1. Download the Splunk Cloud metadata from <a href="https://tenant.splunkcloud.com/en-US/saml/spmetadata">https://tenant.splunkcloud.com/en-US/saml/spmetadata</a>.

- 2. Sign on to the PingFederate administrative console.
- 3. Using the metadata that you downloaded, create an SP connection in PingFederate:
  - 1. Configure using Browser SSO profile SAML 2.0.
  - 2. Enable the following **SAML Profiles**:
    - IdP-Initiated SSO
    - SP-Initiated SSO
    - IdP-Initiated SLO
    - SP-Initiated SLO
  - 3. In Assertion Creation: Attribute Contract, set the Subject Name Format to urn:oasis:names:tc:SAML:1.1:nameidformat:emailAddress.
  - 4. Extend the contract:
    - Attribute: Role
    - Format: urn:oasis:names:tc:SAML:2.0:attrname-format-basic
  - 5. In the **Assertion Creation: Attribute Contract Fulfilment**, map attribute **SAML\_SUBJECT** to the attribute **mail** and map attribute **Role** to the LDAP attribute containing the Splunk role.
  - 6. In Protocol Settings: Allowable SAML Bindings, enable Redirect and POST.
- 4. Export the metadata for the newly-created SP connection.
- 5. Export the signing certificate public key.

Pr	PingFederate	× +	- 🗆 ×
÷	→ C ▲ Not secur	re   ping.localdomain:9999/pingfederate/app#/spConnections	☆ 🖰 ፤
Pinį	gFederaté	AUTHENTICATION APPLICATIONS SECURITY SYSTEM	오   🖲   🌒
	< Integration	SP Connections	
Ð	SP Connections	On this screen you can manage connections to your partner SPs.	
Æ	SP Adapters	Search Clear Narrow By V	
ψ	Target URL Mapping	Connection Name  Connection ID Virtual ID Protocol Enabled Activ	on
	SP Default URLs	SAME 20 Selection	ct Action 🗠
	Policy Contract Adapter Mappings Adapter-to- Adapter Mappings	Create Connection Import Connection	

## Configure the PingFederate IdP-connection for Splunk Cloud

- 1. Sign on to Splunk Cloud as an administrator.
- 2. In the top navigation bar, click **Settings**.
- 3. Click Authentication Methods.



4. Click SAML, and then click Configure Splunk to use SAML.

Settings   Splunk	x +	- 🗆 ×
← → C ■	splunkcloud.com/en-US/manager/launcher/authoverview	* 🖰 :
splunk>cloud Apps	Messages      Settings      Activity      Find	👤 Splunk Cloud Admin 🔹 🔞 🔹
Authentication M	lethods	
Select a	in authentication method. Splunk supports native authentication as well as the following external methods:	
	Internal 🖾 Splunk Authentication (always on)	
Relo	External O None O LDAP SAML Configure Splunk to use SAML	

- 5. On the **SAML Configuration** window, note the warning and save the **Direct Login** URL so that you can use it in the event of integration errors.
- 6. In the Metadata XML File field, click Select File, and select the PingFederate metadata file that you exported.



- 7. Review the configuration loaded from the metadata.
- 8. Set the **Entity ID** to the one that you configured in PingFederate when creating the SP configuration, such as **splunkEntityId**.
- 9. Set the Role alias to the value that you configured in PingFederate for the attribute contract, such as Role.
- 10. Set the Name ID Format to Email Address.

SAML Groups   Splunk 8.0.200	6 × +			- C	×
← → C ■	splunkcloud.com/en-US/m	anager/launcher/saml#		0v 🕁	<b>e</b> :
splunk>cloud Apps •	Messages • Settings •	Activity = Find Q	👤 Spå	unk Cloud Admin +	0.
SAML Groups	SAML Configuration	1	×		
Once mapped, SAML groups Click SAML Configuration to	Entity ID ?	splunkEntityld			
10100 0000	Sign AuthnRequest		- 18		
1 SAML Groups	Attribute Query Requests		- 18		
Name *	▼ Alias		- 11		
samluser	Role alias	Role			
	RealName alias				
	Mail alias				
	Advanced Settings		- 18		
	Name Id Format ?	Email Address *			
	Fully qualified domain name or IP of the load balancer ?	https://spluniccloud.com			
	Redirect port - load balan- cer port <sup>7</sup>	443	Ξ.		
		Cancel Sav	•		

11. Ensure the fully qualified domain name parameter and port parameter match that of your Splunk Cloud instance.

For example:

- Fully Qualified Domain Name: https://tenant.splunkcloud.com
- **Port**: 443
- 12. Click Save.
- 13. Go to Settings  $\rightarrow$  Authentication Methods  $\rightarrow$  SAML Settings.
- 14. Click **New Group** and configure the following settings.

Setting	Value
Name	<ul> <li>samluser</li> <li>Note         This value should match the role you are passing from PingFederate in the SSO Attribute Mapping.     </li> </ul>
Role	user

Splunk

SAML Groups   Splunk 8.0.200	6 × +				- 0	×
← → C ■	.splunkcloud.com/e	n-US/manager/launcher/sar	ml		* <b>0</b>	:
splunk>cloud Apps •	Messages • Si	ettings • Activity • F	ind Q,	👤 Splunk Clou	d Admin 🝷	0.
SAML Groups Map the groups from your SAN Once mapped, SAML groups p Click SAML Configuration to m	M, server to roles in Sp possess the abilities an lodify your existing SAI	iunk Enterprise. d permissions of the assigne ML setup. Click New Group to	id Splunk roles. o add a new SAML group. Learn more [2	SAML Configuration	New Group	,
1 SAML Groups	filter	q			20 per page	
Name *		Actions	Roles ≎	Status +		
samluser		Edit Delete	user	✓ Enabled		

#### 15. Click Save.

16. Create additional groups as required to meet requirements.



The configuration is complete.

## **Configuring SAML SSO with Splunk Cloud and PingOne for Enterprise**

Learn how to configure SAML SSO with Splunk Cloud and PingOne for Enterprise.

About this task

## **(i)** Note An error in configuration could cause users and administrators to be unable to sign on to Splunk Cloud. The following Direct Login link can be used for local authentication:

https://tenant.splunkcloud.com/en-US/account/login?loginType=splunk

The following table details the required and optional attributes to be configured in the assertion attribute contract.

Attribute Name	Description	Required / Optional
SAML_SUBJECT		Required
Role	User role as per SAML Groups. Attribute name is configurable in SAML configuration for application.	Required
Email	User email address. Attribute name is configurable in SAML configuration for application.	Optional

Attribute Name	Description	Required / Optional
RealName	User display name. Attribute name is configurable in SAML configuration for application.	Optional

The following table details the references that are used within this guide that are environment-specific. Replace these with the suitable value for your environment.

Reference	Description
tenant	The instance name for the Splunk Cloud tenant.

#### Create a PingOne for Enterprise Application for Splunk Cloud

- 1. Download the Splunk Cloud Metadata from https://tenant.splunkcloud.com/en-US/saml/spmetadata .
- 2. Sign on to PingOne for Enterprise and click Applications.
- 3. On the SAML tab, click Add Application.

	DASHBOARD APPLICATIONS				0	Sign O	đ
My Applications Application C	Catalog PingID SDK Applications (	OAuth Settings					
My Applications							
SAML OIDC							
-							
Applications you've added to your a	account are listed here. You can search	by application na	me, description or e	ntityid			
<ul> <li>Active applications are enabled</li> <li>Details displays the peopleation</li> </ul>	for single sign-on (SSO). details.						
<ul> <li>Details displays the application</li> </ul>							
Application Name	Type Status	Enab	led				
Devails displays the application     Application Name     Use the button below to add your fi	Type Status	Enab	led				
Details displays the application     Application Name     Use the button below to add your fi	Type Status	Enab	led				
Details displays the application     Application Name     Use the button below to add your fi     Add Application -	Type Status	Enab	led		Pause All SSO	•	
Details displays the application     Application Name     Use the button below to add your fi     Add Application      Search Application Catalog	Type Status	Enab	ied		Pause All SSO	]•	
Details clasplays the application     Application Name     Use the button below to add your fi     Add Application      Search Application Catalog     New SAML Application	Type Status	Enab	ied		Pause All SSO	0	
Details displays the application     Application Name Use the button below to add your fit     Add Application      Search Application Catalog     New SAML Application     Request Ping Identity add a new	Type Status irst application. w application to the application catalog	Enab	ied		Pause All SSO	o	

4. Click Search Application Catalog and search for Splunk.

The results should show Splunk Enterprise. This is suitable for both Splunk Cloud and Splunk Enterprise.

5. Click the **Splunk Enterprise** row.



- 6. Click Setup.
- 7. Select the appropriate signing certificate.
- 8. Review the steps, and note the PingOne SaaS ID, IdP ID, Initiate Single Sign-on (SSO) URL, and Issuer values.

Pi Ping

admin.pingone.com/		☆	9	9	,	9	9	,	9	Э	9
	Application Name		* Туре								
>	Splunk Enterpris	e	SAML	V	_						
1. SSO Instructions											
Signing Cer	tificate PingOne Acco	ount Origination Certificate (2021	Download								
s	For reference, plea aaS ID	ase note the following configurat	ion parameters:								
	IdP ID										
Initiate Single S (SSO)	ign-On https://sso.con	nect.pingidentity.com/sso/sp/ir	nitssoʻi								
	Issuer https://pingone	.com/idp/c									
	Splunk supports se	elf service SSO. Follow the instru-	uctions below to setup SSO.								
Settings > Access	Controls > Authentication	Method									
Labe	I	Description									
1 Spl Dov	unk Administrator: vnload Splunk Metadata	Choose "Download File" to s	save the Splunk metadata to your file :	system.							
2 Pin	gOne Setup Step 2:	Choose "Select File" to uplo	ad the Splunk metadata.								

Map the SAML attributes to the appropriate values for this application from your Identity

#### 9. Click Continue to Next Step.

10. In the Upload Metadata section, click Select File, and upload the Splunk Cloud metadata file that you downloaded.

11. Make sure the following values are set:

• ACS URL to https://tenant.splunkcloud.com/saml/acs

PingOne Setup Step 3: SSO

• Single Logout Endpoint to https://tenant.splunkcloud.com/saml/logout

Pt Pir	gOne -	Application Catalog × +		-		×
$\leftarrow \rightarrow$	C	admin.pingone.com/web-portal/cas/applicatio	ncatalog	☆	θ	÷
		2. Connection Configuration				^
		Assign the attribute values for single sig	in-on (SSO) to the application.			
		Upload Metadata	Uploaded file:splunkcloudSPMetadata.xml			
			Select File Or use URL			
		ACS URL	https:// splunkcloud.com/s * our configuration information.			
		Entity ID	splunkEntityId			
		Target Resource @				
		Single Logout Endpoint @	https://			
		Single Logout Response Endpoint @	example.com/sloresponse.endpoint			
		Primary Verification Certificate e	saml20metadata.cer			
			CN+SplunkServerDefaultCert			
			Expires: 2024/02/02			
			Download   Remove Certificate			
		Secondary Verification Certificate @	Choose File No file chosen			
		Force Re-authentication @	0			
		Encrypt Assertion @	0			

13. In the **Attribute Mapping** section, complete the attribute mapping for the Splunk role for the user.

## (i) Note

For this integration example, all PingOne for Enterprise authenticated users will be mapped to a role with the literal value of samluser, and the **Identity Bridge Attribute** or **Literal Value** check box is selected. However, this could also be retrieved from the user directory.

14. In the Attribute Mapping section, in the Identity Bridge Attribute or Literal Value column of the SAML\_SUBJECT row, select the attribute SAML\_SUBJECT.

3. Attri M	ibute Ma lap your	Application Attribute	tion Name k Enterprise ites to the attributes required by the ap	pplication.	SAML	1	7		
3. Attri M	ibute Ma lap your	Spluni apping r Identity bridge attribu Application Attribute	k Enterprise	pplication.	SAML				
3. Attri M	ibute Ma lap your	apping Identity bridge attribu Application Attribute	ites to the attributes required by the ap	pplication.					
M	lap your	r identity bridge attribu Application Attribute	ites to the attributes required by the ap	pplication.					
	lap your	Application Attribute	ites to the attributes required by the ap	pplication.					
		Application Attribute							
		Application Annoule	Description	Identity Bridge Att	tribute or Literal				
			Description	Value					
		SAML SUBJECT	Splunk username - map to	SAML_SUBJE	СТ				
	1		appropriate source attribute.	As Literal					
				Advanced					
	2 Dola *		Map to attribute group attribute (ex.	samiuser As Leval					
	-	14010	'memberOf' in Active Directory).	Advanced					
							- I		
	Add nev	w attribute							
-	Indicates	s a required attribute.							
	(T: PineO	ne App Customization - Sp	plunk Enterprise		Cancel Back	Continue to Next S	step		

16. Update the Name, Description, and Category fields as required.

P1 PingOne	- Application Catalog × +			- 🗆 ×
< → c	admin.pingone.com/web-portal/cas/application	catalog		<b>☆ ⊖</b> :
	> Splunk Enterpris	2	SAML	
	A. PingOne App Customization - Splunk Entern Icon @ Name @ Description @ Category @ NEXT: Group Access	Select image Splunk Cloud Splunk Enterprise is the leading platform for real-time operational intelligence. It's the easy, fast and secure way to search, analyze and visualize the massive streams of machine data generated by your IT Engineering	Cancel Back Continue to Next	Step

18. Add suitable user groups for the application.

PingOne - Applicatio	on Catalog X +	-		×
← → C ■ a	dmin.pingone.com/web-portal/cas/applicationcatalog	\$	θ	1
5.0	Group Access         Select all user groups that should have access to this application. Users that are members of the added groups will be able to SSO to the see this application on their personal dock.         Group1, Group2, etc       Search         Group Name       Domain Administrators@directory	is application and w	11	
	NEXT: Review Setup	ontinue to Next Ste	Ρ	

20. Review the settings.



21. Copy the Single Sign-On (SSO) URL value to a temporary location.

This is the IdP-initiated SSO URL that you can use for testing.

22. On the Signing Certificate row, click Download.

You will use this for the Splunk Cloud configuration.

23. On the SAML Metadata row, click Download.

You will use this for the Splunk Cloud configuration.

24. Click Finish.

#### Configure the PingOne for Enterprise IdP connection for Splunk Cloud

- 1. Sign on to Splunk Cloud as an administrator.
- 2. From the top navigation bar, click Settings.
- 3. Click Authentication Methods.



4. Click SAML, and then click Configure Splunk to use SAML.



5. Note the warning and save the **Direct Login URL** so that you can use it in the event of integration errors.

6. On the Metadata XML File row, click Select File, and select the PingOne for Enterprise metadata that you exported.

SAML Groups   Splunk 8.0.200	6 × +			-		×
← → C ■	splunkcloud.com/en-US/manager/launcher/saml			0v ☆	Θ	÷
splunk>cloud Apps •	Messages * Settings * Activity * Find Q	2	Splunk Clo	ud Admin	-	<b>0</b> -
SAML Groups Map the groups from your SA	SAML Configuration	×	Iguration			
Once mapped, SAML groups Click SAML Configuration to	WARNING: An error in configuring SAML could result in users and admins being locked out of Splunk Cloud. Use this lin to access the local login and revert back to None for authentication If you are locked out:	k Í				
0 SAML Groups	https://[name].splunkcloud.com/en-US/account/login?login?ype=splunk [replace (name) with your account name] Be sure to copy this information to a safe place before closing this window.					
Name *	Configure SAML for Splunk, Learn More 2					
No SAML Groups are of the second s	Download the SPMetadata from Splunk and add it to your SAML environment to connect to Splunk. SP Metadata File Download File Import Identity Provider (IdP) metadata by browsing to an XML file, or copy and paste the information into the Metadata Contents text box. Metadata XML File Select File Metadata Contents Apply Cancel Sev					

- 7. Review the configuration you loaded from the metadata.
- 8. Set the Entity ID to the one that you configured in PingOne for Enterprise when you created the SP configuration, such as splunkEntityId.
- 9. Set the **Role alias** to the value that you configured in PingOne for Enterprise for the **SSO Attribute Mapping**. For example, **Role**.

SAML Groups   Splunk 8.0.2006 × +	- 🗆 ×
← → C ■ splunkcloud.com/en-US/manager/launcher/saml#	∾ ☆ 😝 :
<b>splunk</b> >cloud Apps = Messages = Settings = Activity = Find Q	👤 Splunk Cloud Admin 👻 🚱 🕶
SAML Groups SAML Configuration	X Iguration New Group
Once mapped, SAML groups Entity ID * splunkEntityId	1
Sign AuthnRequest	
Attribute Query Requests	20 per page *
▼ Alias	_
Role alias Role	
RealName alias	
Mail alias	
Advanced Settings	
Name id Format <sup>*</sup> Email Address •	
Fully qualified domain name or IP of the load balancer 7	
Redirect port - load balan- cer port 7	□.
Cancel	Save

10. Set the Name ID Format to Email Address.

11. Ensure the fully qualified domain name parameter, and port parameter matches that of your Splunk Cloud instance.

For example:

- Fully Qualified Domain Name: https://tenant.splunkcloud.com
- **Port**: 443
- 12. Click Save.
- 13. Go to Settings  $\rightarrow$  Authentication Methods  $\rightarrow$  SAML Settings.
- 14. Click **New Group** and configure the following settings:

Setting	Value
Name	<ul> <li>samluser</li> <li>Note         This value should match the role you're passing from PingOne for Enterprise in the SSO Attribute Mapping.     </li> </ul>
Role	user

SAML Groups   Splunk 8.0.2	006 × +					- 0	×
← → C ■	.splunkcloud.com/	en-US/manager/launcher/sa	ml			\$	<b>e</b> :
splunk>cloud Apps	▼ Messages ▼ S	ettings • Activity •	Find Q,		👤 Splunk Clou	d Admin 🕶	0.
SAML Groups					SAML Configuration	New G	roup
Map the groups from your S Once mapped, SAML group Click SAML Configuration to	AML server to roles in S s possess the abilities ar modify your existing SA	plunk Enterprise. nd permissions of the assigne ML setup. Click New Group t	ed Splunk roles. o add a new SAML group. Learn more 🛤				_
1 SAML Groups	filter	Q				20 per pa	ge •
Name *		Actions	Roles ¢	Status ¢			
samluser		Edit Delete	user	✓ Enabled			

#### 15. Click Save.

16. Create additional groups as required to meet requirements.

SAML Groups   Splunk 8.0.200	5 × +					-		×
← → ♂ ■	.splunkcloud.com/en-US/n	anager/launcher/saml#				04	* <b>0</b>	:
splunk>cloud Apps •	Messages • Settings •	Activity * Find	٩			👤 Splunk Cloud /	idmin =	<b>0</b> -
SAML Groups Map the groups from your SA	Create New SAML	Group				× Iguration		
Click SAML Configuration to a	Group Name	samluser						
1 SAML Groups	Splunk Roles	Available item(s) epps can_delete	edd ell >	Selected item(s) user	< remov	re all p		
Nome *		sc_admin						
samluser		1264	-					
					Cancel			

The configuration is complete.

#### Test the PingOne for Enterprise IdP-Initiated SSO integration

1. Go to the **Single Sign-On (SSO) URL** in the PingOne for Enterprise application configuration and perform IDP initiated SSO.

https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=saasid&idpid=idpid

## Test the PingOne for Enterprise SP-initiated SSO integration

1. Go to the URL for your Splunk Cloud tenant, https://tenant.splunkcloud.com.

You're redirected to PingOne for Enterprise for authentication.

1 https://login.pingone.com/idp/d	+	×
← → C ■ login.pingone.com/ic	idp/directory/a/645baa9a-fd5f-4886-a4f9-52e8a97dc612/sso/?returnurl=https%3A%2F%2Fsso.connect.pingid 🕶 🗞 🏠 😔 Incognito	
		ĥ
	Ping	
	identity. <sup>20</sup>	
	Sign On	
	USERNAME	
	PASSWORD	
	Remember Me	
	Sign On	
		P
	Forgot Password	
		÷
Home   Splunk 8.0.2006 X +	+	×
← → C 🔹 🛃 splunks	kcloud.com/en-US/app/launcher/home	
splunk>cloud Messages • S	ettings • Activity • Find Q	•
Apps 🗘	Explore Splunk Cloud	1
Search & Reporting		
Universal Forwarder	Search Manual 12 Pivot Manual 12 Dashboards & Visualizations 12	
	Use the Splunk Search Processing Use Pivot to create tables and charts Create and edit dashboards using Language (SPL). with SPL. interactive editors or simple XML.	
	Ci	×
	(C) diat	
		ļ
	Choose a home dashboard	
	Choose a home dashboard	
	Choose a home dashboard	

## Test PingOne for Enterprise SP-initiated SLO

- 1. Click the username in the top right corner.
- 2. Click Logout.





## **SuccessFactors**

## **Configuring SAML SSO with SuccessFactors and PingFederate**

Learn how to enable SuccessFactors sign-on from a PingFederate URL (IdP-initiated sign-on) and direct SuccessFactors sign-on using PingFederate (SP-initiated sign-on).

#### Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users requiring application access.
- Populate SuccessFactors with at least one user to test access.
- You must have administrative access to PingFederate.
- You must have access to either SuccessFactors Customer Support or the SuccessFactors Provisioning tool.

#### Create a PingFederate SP connection for SuccessFactors

- 1. Sign on to the PingFederate administrative console.
- 2. Create an SP connection for SuccessFactors in PingFederate:
  - 1. Configure usingBrowser SSO profile SAML 2.0.
  - 2. Set Partner's Entity ID to https://www.successfactors.com.
  - 3. Enable the following SAML Profiles:
    - IdP-Initiated SSO
    - SP-Initiated SSO
  - 4. In Assertion Creation: Attribute Contract, extend the contract to add an attribute named SAML\_NAME\_FORMAT.
  - 5. In Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfillment, map SAML\_SUBJECT and map SAML\_NAME\_FORMAT to urn:oasis:names:tc:SAML:2.0:nameid-format:persistent.
  - 6. In Protocol Settings: Assertion Consumer Service URL, set binding to POST, and set Endpoint URL to http://placeholder.

You will update this value later.

- 7. In Protocol Settings: Allowable SAML Bindings, enable POST.
- 8. In Credentials: Digital Signature Settings, select the PingFederate signing certificate.
- 3. Save the configuration.

- 4. Export the signing certificate.
- 5. Export and then open the metadata file, and copy the following values:
  - The entityID
  - The Location entry ( https://your-value/idp/SSO.saml2 )

#### Add the PingFederate IdP Connection to SuccessFactors

1. Sign on to the SuccessFactors Provisioning application.

## (i) Note

If you do not have access to this application, you will need to contact SuccessFactors' Customer Support.

2. Search for your company and click its name link.

Success	SuccessFactors Business Execution Suite™ P R O V I S I O N I N G												
Companies	Compan	ies											
	Company Details	New Company	Clone Company	Reports	Operations/I	Maintenance	SMB	Manage Provisioners	Manage WFA URLs	SAC configuration tool	SuccessStore	Upgrade Cent Content	ter Media
	List of Comp	oanies <u>o-</u>	ABCDEEG	HIJKL	MNOPO	RSTU	<u>v w x</u> y	<u>Z</u> Others show a	II				
	Show License info	rmation 🗆 🕓	how License										
- X													
SUCCESS	Company Nam	10	Company ID	0	Total Seats	None	Seat Enforce	ement Option	Expiration Date	Expiration E	Enforced	DB Pool ID	Active
FACTORS	Your Company			0		None							v

3. Click Single Sign-On (SSO) Settings.



4. In the For SAML based SSO section, click SAML v2 SSO.

5. In the SAML Asserting Parties (IdP) list, select Add a SAML Asserting Party, and enter the following values:

Field	Value
SAML Asserting Party Name	PingFederate
SAML Issuer	The PingFederate <b>Issuer</b> value
Require Mandatory Signature	Assertion
Enable SAML Flag	Enabled
Login Requested Signature (SF Generated/SP/RP)	Select <b>No</b> .
SAML Profile	Browser/Post Profile
SAML Verifying Certificate	Paste the PingFederate signing certificate contents.



6. In the SAML v2: SP-initiated login section, enter the following values:

Field	Value
Enable sp initiated login (AuthnRequest)	Select <b>Yes</b> .
Default issuer	Selected.

Field	Value
single sign on redirect service location (to be provided by idp)	https://sso.connect.pingidentity.com/sso/idp/ SSO.saml2?idpid=IdP-ID-value
Send request as Company-Wide issuer	Select <b>Yes</b> .
SAML v2: NameID Setting         Require sp must encrypt all NameID elements         NameID Format    persistent	
SAML v2 : SP-initiated login Enable sp initiated login (AuthnRequest) Default issuer single sign on redirect service location (to be provided by idp) Send request as Company-Wide issuer	Yes 🗘 /1 Yes 🗘

7. Click **Add an asserting party** to save the configuration.

For SAML based SSO: SAML v1.1 SSO	O SAML v2 SSO
SAML Asserting Parties(IdP)         Add a SAML Asserting Party           Add an asserting party	0

8. In the **SAML Asserting Parties (IdP)** list, select the asserting party that you created.

SAML Asserting Parties(IdF	✓ Add a SAML Asserting Party
Add an asserting party	test

- 9. Go to Single Sign On Features.
- 10. In the Single Sign On Features section, enter any text value in the Reset Token field.

A value is required only to switch on SSO.

11. Click Save Token.

Single Sign On Features	
Token-based login is Off.	
Reset Token : Show Token is required for all SSO	Save Token

12. Record the SuccessFactors Assertion Consumer Service URL value containing your SuccessFactors Hostname and Company ID.

(https://your-hostname.successfactors.com/saml2/SAMLAssertionConsumer?company=your-company-ID)

### Update the ACS URL values in PingFederate

1. Sign on to the PingFederate administrative console.

- 2. Edit the SP connection for SuccessFactors.
- 3. Set Assertion Consumer Service URL → Endpoint URL to the SuccessFactors Assertion Consumer Service URL value.

(https://your-hostname.successfactors.com/sam12/SAMLAssertionConsumer?company=your-company-ID)

4. Save the changes.

#### Test the PingFederate IdP-initiated SSO integration

- 1. Go to the PingFederate SSO Application Endpoint for the SuccessFactors SP connection.
- 2. Complete PingFederate authentication.

You're redirected to your SuccessFactors domain.

## Configuring SAML SSO with SuccessFactors and PingOne for Enterprise

Learn how to enable SuccessFactors sign-on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct SuccessFactors sign-on using PingOne for Enterprise (SP-initiated sign-on).

#### Before you begin

- · Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Populate SuccessFactors with at least one user to test access.
- You must have administrative access to PingOne for Enterprise.
- You must have access to either SuccessFactors Customer Support or the SuccessFactors Provisioning tool.

#### Obtain the PingOne for Enterprise values for the SuccessFactors application

- 1. Sign on to PingOne for Enterprise and go to **Applications**  $\rightarrow$  **Application Catalog**.
- 2. Search for SuccessFactors.

Application Ca	italog			Applications / Applications / Applications / Applications	plication Catalog
Browse for the application	n you want to add or search for i	it by name. Don't see the applica	tion you're looking for? Fill out o	ur Application Request For	m.
	-				
successfactors		Search			
	Application Nan	ne	↑ Туре		
$\heartsuit$	SuccessFacto	rs	SAML		

- 3. Expand the SuccessFactors entry and click the Setup icon.
- 4. Copy the Issuer and IdP ID values.

5. Download the signing certificate.



#### Add the PingOne for Enterprise IdP connection to SuccessFactors

1. Sign on to the SuccessFactors Provisioning application.

**Note** If you do not have access to this application, you will need to contact SuccessFactors' Customer Support.

2. Search for your company and click its name link.

Success	Factors Busin	iess Execu	tion Suite™ I	PROVI	SIONII	N G							
Companies	Compan	ies											
	Company Details	New Company	Clone Company	<u>Reports</u>	Operations/	Maintenance	SMB	Manage Provisioners	Manage WFA URLs	SAC configuration tool	SuccessStore	Upgrade Cer Content	nter Media
	List of Comp	oanies <u>0-9</u>		HIJKL	MNOP		<u>w x y</u>	<u>Z</u> Others show a	<u>all</u>				
•	Show License info	ormation 🗌 Sh	low License										
×.	Company Nam	-	Company ID		Total Seate		ant Enforce	ament Option	Expiration Date	Expiration	oforced	DB Real ID	Activo
SUCCESS FACTORS	Your Company		Company ID	0	Iotal Seats	None	eat Eniorce	Sment Option	Expiration Date	Expiration of		DB POOLD	~

3. Click Single Sign-On (SSO) Settings.



4. In the For SAML based SSO section, click SAML v2 SSO.

5. In the SAML Asserting Parties (IdP) list, select Add a SAML Asserting Party, and enter the following.

Field	Value
SAML Asserting Party Name	PingOne for Enterprise
SAML Issuer	The PingOne for Enterprise <b>Issuer</b> value.
Require Mandatory Signature	Assertion
Enable SAML Flag	Enabled
Login Request Signature (SF Generated/SP/RP)	Select No.
SAML Profile	Browser/Post Profile
SAML Verifying Certificate	Paste the PingOne for Enterprise signing certificate contents.



6. In the SAML v2: SP-initiated login section, enter the following.

Field	Value			
Enable sp initiated login (AuthnRequest)	Select <b>Yes</b> .			
Default Issuer	Selected.			
single sign on redirect service location (to be provided by idp)	https://sso.connect.pingidentity.com/sso/idp/ SSO.saml2?idpid= <sup>[2]</sup> IdP-ID-value			
Send request as Company-Wide issuer	Select <b>Yes</b> .			
SAML v2: NameID Setting         Require sp must encrypt all NameID elements         NameID Format				
SAML v2 : SP-initiated login Enable sp initiated login (AuthnRequest) Default issuer single sign on redirect service location (to be provided by idp) Send request as Company-Wide issuer	Yes 🗘			

7. Click Add an asserting party to save the configuration.

For SAML based SSO: SAML v1.1 SSO		SAML v2 SSO
SAML Asserting Parties(IdP)	Add a SAML Asserting Party	0
Add an asserting party		

8. In the SAML Asserting Parties (IdP) list, select the asserting party that you created.

SAML Asserting Parties(IdF	✓ Add a SAML Asserting Party
Add an asserting party	test

9. In the **Single Sign On Features** section, enter any text value in the **Reset Token** field.

A value is required only to switch on SSO.

10. Click Save Token.

Single Sign On Features Tratenhamed Incinis IDII	
Reset Token : Show Token Token is required for all SSO	Save Token

11. Record the SuccessFactors Assertion Consumer Service URL value containing your SuccessFactors Hostname and Company ID.

(`https://your-hostname.successfactors.com/saml2/SAMLAssertionConsumer?company=your-company-ID)

#### Complete the SuccessFactors setup in PingOne for Enterprise

1. Continue editing the SuccessFactors entry in PingOne for Enterprise for Enterprise.



If the session has timed out, complete the initial steps to the point of clicking **Setup**.

- 2. Click Continue to Next Step.
- 3. Set the ACS URL to be the SuccessFactors Assertion Consumer Service URL value.

(https://your-hostname.successfactors.com/saml2/SAMLAssertionConsumer?company=your-company-ID)

4. Leave the preset Entity ID.

5. In the Target Resource field, replace \${sfdatacenter} with the hostname from the ACS URL value.
| Assign the attribute values for single sig | n-on (SSO) to the application.   |
|--|--|
|  | . ,  |
|  |  |
| Linioad Metadata                           |  |
| Opload Metadata                            | Select File Or use URL   |
|  |  |
|  | https://filefdatacepter) aucocosfactors (  |
| ACS UNL                                    | https://with your configuration information  |
|  | Repace the parameter(s) #(stotatacenter), #(company)of above with your comiguration mormation. |
| Entity ID                                  | https://www.successfactors.com   |
|  |  |
| Target Resource                            | https://\${sfdatacenter} successfactors (  |
| Target Resource @                          | Replace the parameter(s) () above with your contiduration information.                         |
|  |  |

- 6. Click Continue to Next Step.
- 7. Map the **SAML\_SUBJECT** attribute to the similar attribute names in your environment and click **Advanced**.

Map your	identity bridge attributes	s to the attributes required by the applicat	ion.	
	Application Attribute	Description	Identity Bridge Attribute or Literal Value	
:		Please map the appropriate	SAML_SUBJECT	:
1	*	values for your Successfactors userids	As Literal	

8. Set the Name ID Format to send to SP to urn:oasis:names:tc:SAML:2.0:nameid-format:persistent. Click Save.

-	
Advanced Attribute Options	×
Advanced Attribute Options for SAML_SUBJECT	<b>^</b>
Advanced Attribute Options	
NameldFormat @	
Name ID Format to send to SP: urn:oasis:names:tc:SAML:2.0:nameid-format:persistent	- 1
Attribute Mapping	- 1
You can build an attribute mapping using multiple source attributes, literals and transformation functions.	
For example, SAML_SUBJECT can be (where each attribute value is a separate entry):	
subject = firstName + "." + lastName + "@" + domainName	
SAML_SUBJECT = SAML_SUBJECT	
IDP Attribute Name or Literal Value As Literal Function	
1 SAML_SUBJECT	
Add Attribute	-
Close	Save

# 9. Click Continue to Next Step twice.

10. Click **Add** for all user groups that should have access to SuccessFactors.

5. Group Access
Select all user groups that should have access to this application. Users that are members of the added groups will be able to SSO to this application and wi see this application on their personal dock.
Group1, Group2, etc Search
Group Name
Users@directory Remove
Domain Administrators@directory Add

#### 11. Click Continue to Next Step.

12. Click Finish.

### Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to your Ping desktop as a user with SuccessFactors access.

# (i) Note

To find the Ping desktop URL in the Admin console, go to Setup  $\rightarrow$  Dock  $\rightarrow$  PingOne Dock URL.

2. Complete the PingOne for Enterprise authentication.

You're redirected to your SuccessFactors account.

	Ping Keetity Sign On	
USERNAME		
PASSWORD		
	Remember Me	
	Forgot Password	

## Test the PingOne SP-initiated SSO integration

- 1. Go to your SuccessFactors URL.
- 2. When you're redirected to PingOne for Enterprise, enter your PingOne username and password.



You're redirected back to SuccessFactors.

# SumoLogic

# Configuring SAML SSO with SumoLogic and PingFederate

Learn how to enable SumoLogic sign-on from a PingFederate URL (IdP-initiated sign-on) and direct SumoLogic sign-on using PingFederate (SP-initiated sign-on).

#### Before you begin

- Configure PingFederate to authenticate against an identity provider (IdP) or datastore containing the users requiring application access.
- PingFederate's X.509 certificate should be exchanged to verify the signature in SAML assertions.
- An email attribute is required in the assertion, either the SAML Subject or another SAML attribute per the SAML configuration. The value of the email attribute must be a valid email address. It is used to uniquely identify the user in the organization.
- Populate SumoLogic with at least one user to test access.

#### Create a PingFederate service provider (SP) connection for SumoLogic

- 1. Sign on to the PingFederate admin console.
- 2. Configure using Browser SSO profile SAML 2.0.
- 3. Set Partner's Entity ID to https://service.eu.sumologic.com/.
- 4. Enable the following SAML Profiles:
  - IdP-Initiated SSO
  - SP-Initiated SSO
- 5. In Assertion Creation: Attribute Contract, select urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified.
- 6. In Assertion Creation: Authentication Source Mapping: Authentication Source Mapping, map a new Adapter Instance → HTML Form.
- 7. In Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfilment, map SAML\_SUBJECT.
- 8. In Protocol Settings: Assertion Consumer Service URL, set Binding to POST and set Endpoint URL to https:// service.eu.sumologic.com/sumo/saml/consume/596910108. This value is received and updated from SumoLogic.
- 9. In Protocol Settings: Allowable SAML Bindings, enable POST.
- 10. In Credentials: Digital Signature Settings, select the PingFederate Signing Certificate.
- 11. Save the configuration.

- 12. Export the signing certificate.
- 13. Export and then open the metadata file and copy the value of:
  - The entityID
  - The Location entry(https://your-value/idp/SS0.saml2)

# Add the PingFederate IdP Connection to SumoLogic

1. Sign on to the SumoLogic application.

(i) Note		
In this	example, we have registered and logged in us	ing trial mode.
Home   Sumo Logic X	+	• - 6 ×
Sumo logic ←	Security     Security     Susers and Roles     Account	+ New
0 + 1 =	Home Learn Certification	
Recently Opened By Me	Log Search Metrics Traces Live Tail Explore Root Cause Setup Wizard	o
	Recently Opened Dashboards	Recently Run Searches
No Recent Items	No Recent Dashboards When you open your first dashboard, it will appear here.	No Recent Searches When you open your first search, it will appear here.
dashboards, they'll appear here.	Recommended Dashboards 📀	Pinned Searches
	No Recommended Dashboards When your team starts using dashboards, they will appear here.	No Pinned Searches When you pin a search, it will appear here. In order to pin a search, right click a search tab and select pin.
App Catalog		
Se Manage Data		
Administration		
<ul> <li>Help</li> <li>Seshadri Vasu Addanki (ProofID)</li> </ul>		•

2. Go to Administration  $\rightarrow$  Security  $\rightarrow$  SAML.

🐰 Security   Sumo Logic						
← → C 🗎 service.eu.	sumologi	c.com/ui/#/security/saml				🖈 😸 Incognito 🛛 Update 🔋
sumo logic	÷	🕈 🖿 🛢 Security	Users and Roles	Secount	+ New	i
0 \star 🖻		Password Policy Service Allowlist Settings	Access Keys Policies	SAML Installation Tokens		
Recently Opened By Me	~	Configuration List				+ Add Configuration
		NAME	DEBUG SP	INITIATED LOGIN	ISSUER	

3. Click Add Configuration.



4. Add the following values:

- Configuration Name : pingfed
- $^\circ\,$  Select the Debug Mode check box
- **Issuer**: The PingFederate Issuer value
- X.509 Certificate: Copy PingFederate's X.509 certificate here for verifying the signature
- Attribute Mapping: Select Use SAML Subject
- Optional Settings: Leave the default settings
- Click Add
- Enable Require SAML Sign In.

Security   Sumo Logic ×						• - • ×
$oldsymbol{\epsilon}  ightarrow \mathbf{C}$ $igacharrow$ service.eu.sumologi	c.com/ui/#/security/saml					🖈 🁼 Incognito 🛛 Update 🚦
sumo logic $\leftarrow$	🗰 🖹 Security	Subsers and Roles	Se Account	+ New		1
0 * E 🖢	Password Policy Service Allowlist Setting:	s Access Keys Policies	SAML Installation Tokens			
Recently Opened By Me 🗸 🗸	Configuration List					+ Add Configuration
	NAME	DEBUG SP IN	NITIATED LOGIN	ISSUER		
No Recent Items When you run searches and open dashboards, they'll appear here.	pingfed  Require SAML Sign In All users to sign in using	Tust log in using one of the SAML integration	ns unless they are allowed to bypass SAML an	vasu-þing d use password-based sign-in.		+ add Allowiist User
	NOME	STATUS E	EMAIL	CAN MANAGE SAML	LASI LOGIN	
App Catalog						
😂 Manage Data						
Administration						
Account	Seshadri Vasu Addanki	✓ s	seshadri.vasuaddanki@proofid.com	Yes	8/24/21 10:04 AM	
Users and Roles						
Security						
🕢 Help						•
2 Seshadri Vasu Addanki (ProofID)						

5. Select the **pingfed** configuration you have just created and copy the **Assertion Consumer Service URL**.

👪 Security   Sumo Logic 🛛 🗙					•	
$\leftrightarrow$ $\rightarrow$ $\mathbf{C}$ $\hat{\mathbf{e}}$ service.eu.sumologi	c.com/ui/#/security/saml				🖈 😁 Inc	ognito Update
sumo logic	🕈 🔚 🛢 Security	Users and Roles	Se Account	+ New		
0 ★ 🖻 🔚	Password Policy Service All	owlist Settings Access Keys Policies	SAML Installation Tokens			
Recently Opened By Me 🛛 🗸	Configuration List			+ Add Configuration	pingfed	×
	NAME	DEBUG SP INITIATED LOGIN	ISSUER		1 1	
					Assertion Consumer	
					https://service.eu.sumologic.com/sumo/saml/consume/59691	Сору
O						
<u>1</u>	pingfed		vasu-ping			
No Decent Items						
When you run searches and open						
dashboards, they'll appear here.						
	Require SAML Sign In	All users must log in using one of the SAML integra	ations unless they are allowed to bypass SAML	and use password-based sign-in.		

- 6. To enable SP-initiated SSO, select the **pingfed** configuration and click the **Pencil** icon above the **ACS URL**.
- 7. Select the SP Initiated Login Configuration check box and enter the following values:
  - Login Path: enter a unique identifier for your organization. You can specify any alphanumeric string (with no embedded spaces), provided that it is unique to your organization. (You can't configure a Login Path that another Sumo customer has already configured).

- Authn Request URL: enter the URL that the IdP has assigned for SumoLogic to submit SAML authentication requests to the IdP. For example, https://idp-server-hostname:9031/sso/idp/SS0.saml2
- Select Binding Type: Post.

👪 Security   Sumo Logic 🛛 🗙						• - • ×
← → C 🗎 service.eu.sumolog	ic.com/ui/#/security/saml/edit/000000002394201C					🖈 😸 Incognito 🛛 Update 🔋
sumo logic $\leftarrow$	🕈 🖿 🛢 Security	SUsers and Roles	Se Account	+ New		:
0 ★ 🖻 늘	Password Policy Service Allowlist Settings	Access Keys Policies	SAML Installation Tokens			
Recently Opened By Me V	← Edit pingfed					
	b2NhbGhvc3QwggEiMA0GCSqGSIb3DQ aQjm759ht9oJ2L216qq3hvr6b+DIwj	EBAQUAA4IBDwAwggEKAoIBAQC+ /WvbYAiTRzBqDmX59hao7rwXqh	jxrSrXHnAyQArkbzilWw 0wvtUdMNbP39xapFYEgE		-	
	Attribute Mapping *					
	Use SAML Subject     Use SAML Attribute					
۰ <sub>بل</sub>	Optional Settings					- L
	SP Initiated Login Configuration Login Path * pingfed					
When you run searches and open dashboards, they'll appear here.	Authn Request URL * https://192.168.1.192.9031/idp/SS0.sar	nl2				- 11
	Disable Requested Authentication (	Context				- 11
	Select Binding Type					
	Post     Redirect					
	Roles Attribute					
App Catalog	On Demand Provisioning					
S Manage Data	Logout Page					
슈 Administration						×
Help						Cancel Save
💄 Seshadri Vasu Addanki (ProofID)						

- 8. Click Save.
- 9. Click the saved **pingfed** configuration again and make a note of the **Authentication Request** and **EntityID** URLs.

👪 Security   Sumo Logic 🛛 🗙	+				• - Ø
← → C 🔒 service.eu.sumologie	c.com/ui/#/security/saml				🖈 👼 Incognito 🛛 Update
sumo logic	A 🖿 Security	SUsers and Roles	Se Account	+ New	
o \star 🖻 🖿	Password Policy Service Allow	vlist Settings Access Keys Policies	SAML Installation Tokens		
Recently Opened By Me 🗸 🗸	Configuration List			+ Add Configuration	pingfed
	NAME	DEBUG SP INITIATED LOGIN	ISSUER		/ <u>=</u>
					Authentication Request
					https://service.eu.sumologic.com/sumo/sami/login/59691010E Copy
					Assertion Consumer
					https://service.eu.sumologic.com/sumo/sami/consume/59691 Copy
					Entity ID
0	pingfed	pingfed	vasu-ping		https://service.eu.sumologic.com/sumo/sami/596910108 Copy
No Recent Items					
When you run searches and open dashboards, they'll appear here.					
	Require SAML Sign In	All users must log in using one of the SAML integratio	ins unless they are allowed to bypass SAML ar	id use password-based sign-in.	
	- Require SAME Sign III	An above making in using the of the dame integrate	and another to bypass dame at	to dee provincial adoct align in.	

The SumoLogic connection configuration is now complete.

#### Update the ACS URL values in PingFederate

- 1. Sign on to the PingFederate administrative console.
- 2. Edit the SP connection for SumoLogic.
- 3. Set the Partner's Entity ID (Connection ID) value to SumoLogic's Entity ID that you copied previously.
- 4. Set Assertion Consumer Service URL : Endpoint URL to SumoLogic's Assertion Consumer Service URL value.
- 5. Click Save.

#### Test the PingFederate IdP-initiated SSO integration

- 1. Go to the **PingFederate SSO Application Endpoint** for the SumoLogic SP connection.
- 2. Authenticate with PingFederate.

You're redirected to your SumoLogic domain.

#### Test the PingFederate SP-initiated SSO integration

- 1. Go to your SumoLogic Authentication Request URL.
- 2. After you're redirected to PingFederate, enter your PingFederate username and password.

After successful authentication, you're redirected back to SumoLogic.

# Tableau

# Configuring SAML SSO with Tableau and PingOne

Learn how to enable Tableau SSO in PingOne (IdP and SP-initiated).

#### Before you begin

- Configure PingOne to authenticate against an identity repository containing the users requiring application access.
- An Email Attribute is required in the assertion, either the SAML Subject or another SAML attribute per the SAML configuration. The value of the Email Attribute must be a valid email address. This attribute is used to uniquely identify the user in the organization.

#### Export the metadata from Tableau

- 1. Sign on to Tableau with an administration account.
- 2. Go to Settings  $\rightarrow$  Authentication.
- 3. Select the Enable an additional authentication method check box.
- 4. Select the SAML authentication method.
- 5. Expand the Edit Connection section.
- 6. Click Export Metadata.



#### **Create the Tableau SP connection**

- 1. In the PingOne admin portal, go to **Connections**  $\rightarrow$  **Applications**.
- 2. Create an SP connection for Tableau by selecting Add application.
- 3. When you're prompted to select an application type, select **WEB APP** and then click **Configure** next to **SAML** for the chosen connection type.
- 4. Enter a unique name for the application.
- 5. Import the Tableau metadata.
- 6. Select the signing certificate.
- 7. Confirm that the EntityID and endpoints are correct.
- 8. Enter a suitable value for Assertion Validity Duration (in seconds). A value of 300 seconds is typical.
- 9. Click Save and Continue.
- 10. Define the Tableau assertion requirements.

🔁 saml_subject	$\leftarrow$	Email Address	REQUIRED	Test Output
🔁 FirstName	←	Given Name		Test Output
🔁 LastName	$\leftarrow$	Mame Family Name		Test Output

- 11. Click the toggle to enable the application.
- 12. On the **Configuration** tab for the Tableau application, on the **Download Metadata** line, click **Download**.

Profile	Configuration	Attribute Mappings	Policies	Access
CON		~		
^ CON	INECTION DETAIL	-5		
DOW	NLOAD METADATA	Download	$\supset$	

# Import the metadata in Tableau

- 1. Upload the PingOne metadata file and click **Apply**.
- 2. Confirm that the IdP, entityID, and SSO service URL are correct.
- 3. Test the connection.
- 4. Match the Tableau attributes to the assertion attributes and click Apply.

5	Mato	ch attributes			
	Mai cor ava	tch the attribute names (assert responding attribute names on ilable attributes.	tions) in the IdP's 1 Tableau Online. 1	SAML configur Click Test Conn	ation to the action to fetch
	Tal	bleau Online Attribute	Identity Pr	ovider (IdP)	Assertion Name
	1	Email			
		Enter the name of the IdP asset contains the email address sen IdP to Tableau Online during the authentication process. The us authenticated if the IdP email a an exact match for the user's e address as stored in Tableau.	rtion that t from the e er is Na vddress is mail	imelD	
		Enter an assertion name for eit name, depending on how the lo these attributes to set the disp	her the first nam IP stores this info lay name.	e and last name rmation. Tablea	, or for the full au Online uses
		<ul> <li>First and last name</li> </ul>	O Full name		
			First name	FirstName	
			Last name	LastName	
			Full name	FullName	
					Apply

#### Test the IdP-initiated SSO integration

1. Go to the PingOne Application Portal and sign on with a user account.

## (i) Note

In the Admin console, go to **Dashboard** → **Environment Properties** to find the **PingOne Application Portal URL**.

2. Click the Tableau icon.

You're redirected to the Tableau website and logged in with SSO.

#### **Test the SP-initiated SSO integration**

- 1. Go to the Tableau sign on page and enter the email address that will redirect to PingOne.
- 2. In the PingOne sign-on prompt, enter your PingOne username and password.

You're redirected back to Tableau and signed on with SSO.

# **Configuring SAML SSO with Tableau and PingFederate**

Learn how to enable Tableau SSO in PingFederate (IdP and SP-initiated).

#### Before you begin

- Configure PingFederate to authenticate against an identity repository containing the users requiring application access.
- An Email Attribute is required in the assertion, either the SAML Subject or another SAML attribute per the SAML configuration. The value of the Email Attribute must be a valid email address. This attribute is used to uniquely identify the user in the organization.

#### Export the metadata from Tableau

- 1. Sign on to Tableau with an administration account.
- 2. Go to Settings  $\rightarrow$  Authentication.
- 3. Select the Enable an additional authentication method check box.
- 4. Select the SAML authentication method.
- 5. Expand the Edit Connection section.
- 6. Click Export Metadata.



#### **Create a Tableau SP Connection**

- 1. In PingFederate, create a service provider (SP) connection for Tableau.
- 2. Configure using Browser SSO profile SAML 2.0.
- 3. Upload the metadata file from Tableau.
- 4. Enable the following SAML profiles.
  - IdP-Initiated SSO
  - SP-Initiated SSO
- 5. Configure the assertion:
  - Select the source mappings.
  - Define the contract fulfillment.

Mapping Method	
Adapter	HTML Form IdP Adapter
Mapping Method	Use only the Adapter Contract values in the mapping
Attribute Contract Fulfillment	
FirstName	givenname (Adapter)
LastName	sn (Adapter)
SAML_SUBJECT	mail (Adapter)

- 6. In protocol settings: Allowable SAML Bindings, enable POST.
- 7. Go to https://PingFederate-url/pf/federation\_metadata.ping?PartnerSpId=Tableau-EntityId and download the metadata file from PingFederate.

#### Import the metadata in Tableau

- 1. Upload the PingFederate metadata file and click Apply.
- 2. Confirm that the IdP entityID and SSO service URL are correct.
- 3. Test the connection.
- 4. Match the Tableau attributes to the assertion attributes and click **Apply**.

5	Ма	tch attributes			
	N ci ai	latch the attribute names (assert orresponding attribute names or vailable attributes.	tions) in the Idl 1 Tableau Onlin	P's SAML configur e. Click Test Conn	ation to the ection to fetch
	Т	ableau Online Attribute	Identity	Provider (IdP)	Assertion Name
		Email			
		Enter the name of the IdP asset contains the email address sen	rtion that It from the		
		authentication process. The us	eris	NameID	
		authenticated if the IdP email a an exact match for the user's e	iddress is mail		
		address as stored in Tableau.			
		Display Name			
		Enter an assertion name for eit name, depending on how the lo these attributes to set the disp	her the first na IP stores this ir lay name.	me and last name nformation. Tablea	e, or for the full au Online uses
		• First and last name	O Full nam	e	
			First name	FirstName	
			Last name	LastName	
			Full name	FullName	
					Apply

#### Test the IdP-initiated SSO integration

Go to the PingFederate SSO application endpoint for Tableau, https://PingFederate-url/idp/startSSO.ping?
 PartnerSpId=Tableau-EntityId.

https://127.0.0.1:9031/idp/startSS0.ping?PartnerSpId=https://sso.online.tableau.com/public/sp/metadata/ 5c142f94-8889-491a-816c-e61ae6dc84cb

2. Authenticate with PingFederate.

You're redirected to Tableau.

#### **Test the SP-initiated SSO integration**

- 1. Go to the Tableau sign on page.
- 2. Enter the email address that will redirect to PingFederate.
- 3. Authenticate with PingFederate.

You're redirected back to Tableau.

# Configuring SCIM 2.0 provisioning with Tableau and PingFederate

Learn how to enable Tableau SCIM 2.0 Provisioning in PingFederate.

#### Before you begin

- Configure PingFederate to authenticate against an LDAP identity repository containing the users requiring application access.
- Configure PingFederate with the SCIM provisioning connector to support the SCIM 2.0 protocol.
- Configure PingFederate with the Tableau SP connection.
- Configure the PingFederate run.properties file to support provisioning.

#### Enable SCIM provisioning in Tableau

- 1. Sign on to Tableau with an administration account.
- 2. Go to Settings  $\rightarrow$  Authentication.
- 3. In the Automatic Provisioning and Group Synchronisation (SCIM) section, select the Enable SCIM check box.
- 4. Click Generate New Secret.

This will generate a new API secret that PingFederate will use to authenticate to the Tableau SCIM endpoint.

Automatic Provi	sioning and Group Synchronisation (SCIM)
Allow a third-party	y identity provider to manage users on this site. Learn more
✓ Enable SCIM	
Base URL	https://scim.online.tableau.com/pods/prod-uk-a/s
Generate Ne	w Secret

# Enable SCIM provisioning in the SP connection

- 1. In the PingFederate administrative console, select the Tableau SP connector.
- 2. On the **Connection Type** tab, select the **Outbound Provisioning** check box and in the **Type** list, select **SCIM Connector**.

SP Connectior	ns   SP Connecti	on				
Connection Type	Connection Options	Metadata URL	General Info	Browser SSO	Credentials	Outbound Provisioning
Select the type of conr	nection needed for this SP:	Browser SSO Profil	es (for Browser SS	O), WS-Trust STS (	(for access to ider	ntity-enabled Web Services),
CONNECTION TEMP	PLATE				No Template	
BROWSER SSC	PROFILES				PROTOCOL SAML 2.0	
WS-TRUST STS	3					
	ROVISIONING				TYPE	
					SCIM Con	nector v

- 3. On the **Outbound Provisioning** tab, select **Configure Provisioning**.
- 4. On the **Target** tab, in the **SCIM Version** list, select 2.0 and enter the **SCIM URL** and **OAuth 2 Bearer Token** obtained from Tableau.

SP Connections   SP	Connection   Configure Channels
Target Manage Channels	
Specify credentials and/or other co	onnection details that PingFederate will use to access the target service provider for outbound provisioning.
Provisioning Target	SCIM Connector
SCIM URL	https://scim.online.tableau.com/pods/prod-uł
SCIM VERSION	2.0 ~
AUTHENTICATION METHOD	OAuth 2 Bearer Token 🗸
BASIC AUTHENTICATION	
USERNAME	
PASSWORD	
OAUTH 2 BEARER TOKEN	
ACCESS TOKEN	

- 5. Define a channel to obtain the user details:
  - 1. Add the LDAP source and source location according to your user data source.

SP Connect	tions   SI	P Connection	Configure C	hannels   Chanı	nel	
Channel Info	Source	Source Settings	Source Location	Attribute Mapping	Activation & Summary	
Choose the data s	tore that serve	es as the local reposite	ory for user accounts	requiring provisioning.		
ACTIVE DATA ST	ORE	PingDirectory	~			
DATA STORE TY	PE	LDAP				
Manage Data S	Stores					

SP Connections   SP Connection   Configure Channels   Channel	
Channel Info         Source         Source Settings         Source Location         Attribute Mapping         Activation & Summary	
Enter or modify LDAP settings that apply to the source user-data store, as needed. Note that these fields are preconfigured wit settings can be used.	h default settings based on the LDAP Type, when specified (
Data Source	
DATA SOURCE	127.0.0.1
DATA SOURCE DESCRIPTION	PingDirectory
LDAP TYPE	PingDirectory
Identity	
ENTRY GUID ATTRIBUTE	entryUUID
GUID TYPE	Text ~
Group Membership Detection	
MEMBER OF GROUP ATTRIBUTE	
GROUP MEMBER ATTRIBUTE	uniqueMember
Change Detection	
USER OBJECTCLASS	inetOrgPerson
GROUP OBJECTCLASS	groupOfUniqueNames
CHANGED USERS/GROUPS ALGORITHM	Timestamp No Negation 🗸 🗸
USN ATTRIBUTE	
TIMESTAMP ATTRIBUTE	modifyTimestamp

# SP Connections | SP Connection | Configure Channels | Channel

Channel Info	Source	Source Settings	Source Location	Attribute Mapping	Activation & Summary
Enter the Base DN	l where user r	ecords are located in	the data store, and spe	ecify either an LDAP Filt	er or Group DN.
BASE DN		ou=SSO,ou=Peo	ople,dc=example,dc=c	om	
Users					
GROUP DN					
FILTER		objectClass=inet	tOrgPerson		
Groups					
GROUP DN					
FILTER		objectClass=gro	up		

2. Configure attribute mappings.



3. Enable the channel.

# Terraform

# Configuring SAML SSO with Terraform and PingOne

Learn how to enable Terraform sign-on from the PingOne SSO console (IdP-initiated sign-on) and direct Terraform login using PingOne SSO (SP-initiated sign-on).

#### Before you begin

- Link PingOne to an identity repository containing the users requiring application access.
- Populate Terraform with at least one user to test access.
- You must have administrative access to PingOne and an administrative account with site-admin permission on Terraform.

# (i) Note

Whenever *TFE-HOSTNAME* is specified throughout this document, replace it with the actual value of your Terraform instance hostname.

### Add the Terraform application to PingOne

1. In PingOne, go to **Connections** → **Applications** and click + to add a new application.

P	ingldentity.		
Enviro Sandt Sandto	nments box - Phil v	Applications	
		Q Search	Filter
*	Applications	3 Applications by Application Name	
u	IDENTITY PROVIDERS	Ping One Admin Console Client ID	
٢	PINC PRODUCTS	Ping PingOne Application Portal	
¢	PingFederate	Directors Salf Condes Medasount	
	PingIntelligence	PingOne Seit-Service - MyAccount Client ID: c	

2. In Select an Application Type, click Web App.

3. In Choose Connection Type, click Configure next to SAML.



- 4. Enter Terraform as the application name.
- 5. **Optional:** Enter a suitable description.
- 6. Optional: Upload an icon.
- 7. Click Next.
- 8. For Provide App Metadata, select Manually Enter.
- 9. For ACS URLs, enter https://TFE-HOSTNAME/users/saml/auth
- 10. Choose the Signing Key to use and then click Download Signing Certificate to download it as X509 PEM ( .crt ).
- 11. For Entity ID, enter https://TFE-HOSTNAME/users/saml/metadata
- 12. Leave SLO Endpoint and SLO Response Endpoint blank. Terraform does not support single logout (SLO).
- 13. In the Subject NameID Format list, select urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress.
- 14. Set a suitable value for Assertion Validity Duration (in seconds). A value of 300 seconds is typical.
- 15. Click Save and Continue.

### (i) Note

By default, Terraform generates a **Username** when an account is first created upon initial SSO. This is based on the user email address.

16. **Optional:** If you want to dictate the **Username** created for a user, you can include the **Username** attribute in the security assertion.

You can include the **MemberOF** attribute to automatically add users to specific **Teams** in the Terraform platform. Configure which **PingOne User Attribute** to map to each of these Terraform attributes.

APPLICATION NAME				TYPE	
Terraform				Web App	
Attribute Mapping Map your PingOne user defined attributes t	to the corr	espon	ding Application attribute for acce	essibility between users and this app.	
SAML ATTRIBUTES					
PINGONE USER ATTRIBUTE			APPLICATION ATTRIBUTE		
Email Address	~	=	saml_subject	<ul> <li>Required</li> </ul>	
PINGONE USER ATTRIBUTE			APPLICATION ATTRIBUTE		
Email Address	~	=	Username	Required	
			APPLICATION ATTRIBUTE		
PINGONE USER ATTRIBUTE					

#### 17. Click Save and Close.

- 18. Enable user access to this new application by moving the toggle to the right.
- 19. On the **Configuration** tab of the newly created Terraform application, copy and save the **Issuer ID** and **Initiate Single Sign-On URL** values. You will use these for configuring SAML on Terraform.

^	CONNECTION DETAILS	
	DOWNLOAD METADATA:	Download
	ISSUER ID:	https://auth.pingone.eu/
	SINGLE LOGOUT SERVICE:	https://auth.pingone.eu
	SINGLE SIGNON SERVICE:	https://auth.pingone.eu/2000.pin/_2001_1200_0201_120000011_56/saml20/idp/sso
	IDP METADATA URL:	https://auth.pingone.eu/
	INITIATE SINGLE SIGN-ON URL:	https://auth.pingone.eu/ <b>GEESSEESEESEESEESEESEESEESEESEESEESEESEE</b>

### Add PingOne as an identity provider (IdP) to Terraform

- 1. Go to https://TFE-HOSTNAME/app/admin/saml and sign on with an administrator account that has site-admin permissions.
- 2. Paste the Initiate Single Sign-On URL value that you saved previously into the Single Sign-On URL field.
- 3. Open the .crt file that downloaded previously in a text editor and copy and paste the entire contents into the IDP Certificate field.
- 4. Click Save SAML settings.

#### Test the PingOne IdP integration

1. Go to the PingOne application portal and sign on with a user account.

# (i) Note

You can find the PingOne Application Portal URL in **Dashboard** → **Environment Properties**.

2. Click the Terraform icon.

You're redirected and presented with a PingOne sign on prompt.

3. Enter your PingOne username and password.

Ping Sign On		
USERNAME		
PASSWORD		
	Hemember Me	
	Sign On	
	Forgot Password	

After successful authentication, you're redirected back to Terraform as a signed-on user.

# UltiPro

# Configuring SAML SSO with UltiPro and PingFederate

Learn how to enable UltiPro sign-on from the PingFederate console (IdP-initiated sign-on) and direct UltiPro sign-on using PingFederate (SP-initiated sign-on).

#### Before you begin

- Configure PingFederate to authenticate against an IdP or datastore containing the users requiring application access.
- Populate UltiPro with at least one user to test access.
- You must have administrative access to PingFederate.

#### Create a PingFederate SP connection for UltiPro

- 1. Sign on to the PingFederate administrative console.
- 2. Create an SP connection for UltiPro in Ping Federate:
  - 1. Configure using Browser SSO profile SAML 2.0.
  - 2. Set Partner's Entity ID to placeholder .

You'll change this later.

- 3. Enable the following SAML Profiles:
  - IdP-Initiated SSO
  - SP Initiated SSO
- 4. In Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfillment, map the SAML\_SUBJECT.
- 5. In Protocol Settings: Assertion Consumer Service URL, set Binding to POST, and set Endpoint URL to https://placeholder.

You'll change the **Endpoint URL** later.

- 6. In Protocol Settings: Allowable SAML Bindings, enable POST.
- 7. In Credentials: Digital Signature Settings, select the PingFederate signing certificate.
- 3. Export the metadata for the newly created UltiPro SP connection.
- 4. Export the signing certificate.

#### Add the PingFederate connection to UltiPro

- 1. Contact UltiPro Customer Support and request that SAML 2 be enabled for your organization.
- 2. Provide them with the downloaded PingFederate signing certificate and metadata.
- 3. Request their ACS URL and EntityID values.

#### Update the ACS URL values in PingFederate

- 1. Sign on to the PingFederate administrative console.
- 2. Edit the SP connection for UltiPro.
- 3. Set Partner's Entity ID to the UltiPro Entity ID value.
- 4. In Protocol Settings: Assertion Consumer Service URL, set Endpoint URL to the UltiPro Assertion Consumer Service URL value.
- 5. Save the changes.

#### Test the PingFederate IdP-initiated SSO integration

- 1. Go to the PingFederate SSO application endpoint for the UltiPro SP connection.
- 2. Complete the PingFederate authentication.

You're redirected to your UltiPro domain.

#### Test the PingFederate SP-initiated SSO integration

- 1. Go to your UltiPro application.
- 2. After you're redirected to PingFederate, enter your PingFederate username and password.

You're redirected back to UltiPro.

# Configuring SAML SSO with UltiPro and PingOne for Enterprise

Learn how to enable UltiPro sign-on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct UltiPro sign-on using PingOne for Enterprise (SP-initiated sign-on).

#### Before you begin

- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Populate UltiPro with at least one user to test access.
- You must have administrative access to PingOne for Enterprise.

## Add the UltiPro application to PingOne for Enterprise

- 1. Sign on to PingOne for Enterprise and go to **Applications**  $\rightarrow$  **My Applications**.
- 2. On the SAML tab, click Add Application.

	DASHBOARD APPLICATIONS	users setup	ACCOUNT	0	Sign Of
My Applications Application Catalo	g PingiD SDK Applications	OAuth Settings			
My Applications					
SAML OIDC					
Applications you've added to your accou	int are listed here. You can searc	h by application na	me, description or entity	ld	
<ul> <li>Active applications are enabled for s</li> <li>Details displays the application detail</li> </ul>	ils.				
<ul> <li>Details displays the application detail</li> </ul>					
Application Name	Type Status	Enab	led		
Application Name	Type Status	Enab	led		
Application Name	Type Status	Enab	led	Pause All SSO	0
Application Name Add Application  Search Application Catalog	Type Status	Enab	led	Pause All SSO	0
Application Name Add Application  Search Application Catalog New SAML Application	Type Status	Enab	led	Pause All SSO	Θ

- 3. Enter **UltiPro** as the application name.
- 4. Enter a suitable description.
- 5. For the category, select Human Resources.
- 6. Click Continue to Next Step.
- 7. Set Assertion Consumer Service (ACS) to https://placeholder and set Entity ID to placeholder.

You'll update these values later.

- 8. Click Continue to Next Step.
- 9. Click Add new attribute.

3. SSO Attribute Mapping		
Map the necessary application	provider (AP) attributes to attributes used by your i	dentity provider (IdP).
Application Attribute	Identity Bridge Attribute or Literal Value	Required
Add new attribute		

10. Add the **SAML\_SUBJECT** attribute and map it to the value required by UltiPro.

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

	Application Attribute	Identity Bridge Attribute or Literal Value	Required
		SAML_SUBJECT	
1	SAML_SUBJECT	As Literal	- *
		Advanced	

#### 11. Click Continue to Next Step.

12. Click **Add** for all user groups that should have access to UltiPro.

5. Group Access	
Select all user groups that should have access to this application. Users that are member see this application on their personal dock.	ers of the added groups will be able to SSO to this application and will
Group1, Group2, etc Search	
Group Name	
Users@directory	Remove
Domain Administrators@directory	Add

#### 13. Click Continue to Next Step.

14. Download the PingOne for Enterprise signing certificate and metadata.

Signing Certificate	Download
SAML Metadata	Download

15. Click Finish.

### Add the PingOne for Enterprise connection to UltiPro

- 1. Contact UltiPro Customer Support and request that SAML 2 be enabled for your organization.
- 2. Provide them with the downloaded PingOne for Enterprise signing certificate and metadata.
- 3. Request their ACS URL and EntityID values.

# Complete the UltiPro PingOne for Enterprise setup in UltiPro

1. Continue editing the UltiPro entry in PingOne for Enterprise for Enterprise.

# i) Note

If the session has timed out, complete the initial steps to the point of clicking Setup.

- 2. Click Continue to Next Step.
- 3. Set the ACS URL to the UltiPro ACS URL value.
- 4. Set the Entity ID to the UltiPro Entity ID value.
- 5. Click **Continue to Next Step** until you reach the final page, then click **Finish**.

#### Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to your Ping desktop as a user with UltiPro access.

### ) Νote

To find the Ping desktop URL in the Admin console, go to Setup  $\rightarrow$  Dock  $\rightarrow$  PingOne Dock URL.

2. Complete the PingOne for Enterprise authentication.

You're redirected to your UltiPro application.



#### Test the PingOne for Enterprise SP-initiated SSO integration

- 1. Go to your UltiPro application.
- 2. After you're redirected to PingOne for Enterprise, enter your PingOne for Enterprise username and password.



You're redirected back to UltiPro.

# Workato

# **Configuring SAML SSO with Workato and PingFederate**

Learn how to enable Workato sign-on from the PingFederate console (IdP-initiated sign-on) and direct Workato sign-on using PingFederate (SP-initiated sign-on).

#### Before you begin

- Configure PingFederate to authenticate against an identity provider (IdP) or datastore containing the users requiring application access.
- · Populate Workato with at least one user to test access.
- You must have administrative access to PingFederate.

### Create the Workato metadata

- 1. In PingFederate, create a service provider (SP) connection for Workato:
  - 1. Configure using Browser SSO profile SAML 2.0.
  - 2. Set Partner's Entity ID to https://www.workato.com/saml/metadata?id=Workato ID.

#### (i) Note

This value is provided by Workato on the **Tools**  $\rightarrow$  **Team**  $\rightarrow$  **Settings** tab.

- 3. Enable the following SAML profiles.
  - IdP-Initiated SSO
  - SP-Initiated SSO
- 4. In Assertion Creation: Authentication Source Mapping: Attribute Contract Fulfilment, map the SAML\_SUBJECT to your email attribute.
- 5. In Protocol Settings: Assertion Consumer Service URL, set Binding to POST and set Endpoint URL to https:// www.workato.com/saml/consume/.
- 6. In Protocol Settings: Allowable SAML Bindings, enable POST.
- 7. In Credentials: Digital Signature Settings, select the PingFederate Signing Certificate.

### i) Note

Note the metadata URL for the newly-created Workato SP connection.

# Add the PingFederate connection to Workato

- 1. Sign on to the Workato console as an administrator.
- 2. Select **Tools** in the left navigation pane.
- 3. Click the **Members** tab.
- 4. Select Team.
- 5. Select the **Settings** tab.

Team
Enables multiple users to collaborate on recipes in a shared workspace. Learn more $\ensuremath{\mathcal{C}}$
Collaborators Pending Invitations Settings Roles
Team name (Required)
Authentication method (Required)
SAML based SSO
Members accessing the team will have to re-authenticate using this method.
Team ID (Required)
Maximum 20 characters
SAML provider (Required)
·
Select your identity provider. If you don't see it, contact support.
Do you have your identity provider metadata URL? (Required)
No
Not sure how to get it, learn more here
Metadata URL (Required)
We will import your SAML settings from this file
Do you want to enable SAMI_IIT provisioning? (Required)
Yes
New users will be automatically added to the team after identity provider authentication. New users are assigned
the Operator role by default.
Validate settings

- 6. Enter a **Team name** for the team or company.
- 7. In the Authentication method list, select SAML based SSO.
- 8. In the SAML\_provider list, select Other.
- 9. Enter the Metadata URL value for the Workato SP connector in PingFederate.

## Test the PingFederate IdP-initiated SSO integration

1. Go to the PingFederate SSO Application Endpoint for the Workato SP connection.

2. Authenticate with PingFederate.

You're redirected to your Workato domain.

#### Test the PingFederate SP-initiated SSO integration

- 1. Go to https://app.workato.com/users/sign\_in  $\square$ .
- 2. After you're redirected to PingFederate, enter your PingFederate username and password.

You're redirected back to Workato.

# Configuring SAML SSO with Workato and PingOne

Learn how to enable Workato sign-on from the PingOne console (IdP-initiated sign-on) and direct Workato sign-on using PingOne (SP-initiated sign-on).

#### Before you begin

- Link PingOne to an identity repository containing the users requiring application access.
- Populate Workato with at least one user to test access.
- You must have administrative access to PingOne and an Admin account on Workato.

#### Add the Workato application to PingOne

1. In PingOne, go to **Connections**  $\rightarrow$  **Applications** and click the + icon.

Pingldentity.			
Environments Sandbox - Phil ~ Sandbox		Applications 🔸	
::	< Connections	Q Search 3 Applications by Application Name	Filter
<b>M</b>	IDENTITY PROVIDERS	PingOne Admin Console Client ID	
© @	PING PRODUCTS PingFederate	PingOne Application Portal Client ID: 1	
	PingIntelligence	PingOne Self-Service - MyAccount           Client ID: d	

2. When you're prompted to select an application type, select **WEB APP** and then click **Configure** next to **SAML** for the chosen connection type.

- 3. Enter Workato as the application name.
- 4. Enter a suitable description.
- 5. Optional: Upload an icon.
- 6. For Provide App Metadata, select Enter from URL.
- 7. In the Import URL field, enter https://www.workato.com/saml/metadata?id=your-Workato-ID.

# (i) Note

your-Workato-ID is a unique value to your Workato account and can be found in the Workato Portal.

- 8. In the ACS URLS field, enter https://www.workato.com/saml/consume.
- 9. Select the Signing Key to use and then click Download Signing Certificate to download as X509 PEM (.crt).
- 10. Leave SLO Endpoint and SLO Response Endpoint blank.
- 11. In the Subject NameID Format list, select urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress.
- 12. Enter a suitable value for Assertion Validity Duration (in seconds). A value of 300 seconds is typical.
- 13. Click Save and Continue.
- 14. Workato expects an email address to identify a user in the SSO security assertion:
  - If you use an email address to sign on through PingOne, click **Save and Close**.
  - If you sign on with a username, in the **PingOne User Attribute** list, select **Email Address** to map that to the **SAML\_SUBJECT**, then click **Save and Close**.
- 15. Click the toggle to enable the application.
- 16. On the **Configuration** tab of the newly-created Workato application, copy and save the **IDP Metadata URL** value.

You'll need this when configuring SAML on Workato.

^	CONNECTION DETAILS		
	DOWNLOAD METADATA:	Download	
	ISSUER ID :	https://auth.pingone.eu/f	
	SINGLE LOGOUT SERVICE :	https://auth.pingone.eu/f	saml20/idp/slo
	SINGLE SIGNON SERVICE:	https://auth.pingone.eu/f	saml20/idp/sso
	IDP METADATA URL:	https://auth.pingone.eu/f	saml20/metadata/c6c91962-45a9-4379-84bf-77576fa582f7
	INITIATE SINGLE SIGN-ON URL:	https://auth.pingone.eu/i	saml20/idp/startsso?spEntityId=https://xx-api.mimecast.com/login/saml

## Add PingOne as an identity provider (IdP) to Workato

- 1. Sign on to the Workato console as an administrator.
- 2. In the left navigation pane, click Tools.
- 3. Click the **Members** tab.
#### 4. Select Team.

5. Click the **Settings** tab.

Team	
Enables multiple users to collaborate on recipes in a shared workspace. Learn more 🗷	
Collaborators Pending Invitations Settings Roles	
Team name (Required)	
Authentication method (Required)	
SAML based SSO	*
Members accessing the team will have to re-authenticate using this method.	
Team ID (Required)	
Maximum 20 characters	
SAM provider (new sect)	
SAML provider (Required)	
Select your identity provider. If you don't see it, contact support	Ť
ocices your recently providen in you don't doe in contact support.	
Do you have your identity provider metadata URL? (Required)	
Yes     No	
Not sure how to get it, learn more here	
Mandata URI (200 to 0	
We will import your SAML settings from this file	
Do you want to enable SAML JIT provisioning? (Required)	
Yes	*
New users will be automatically added to the team after identity provider authentication. New users are assigne the <b>Operator</b> role by default.	ned
Validate settings	

- 6. Enter a **Team name** for the team or company.
- 7. In the Authentication method list, select SAML based SSO.
- 8. In the SAML\_provider list, select Other.
- 9. Enter the Metadata URL for the Workato SP Connector in PingOne.

## Test the PingOne IdP integration

1. Go to the PingOne Application Portal and sign on with a user account.

## (i) Note

In the Admin console, go to **Dashboard** → **Environment Properties** to find the **PingOne Application Portal URL**.

2. Click the Workato icon.

You're redirected to Workato and signed on with SSO.

## Test the PingOne SP integration

- 1. Go to https://app.workato.com/users/sign\_in<sup>□</sup> and enter your email address only.
- 2. In the PingOne sign-on prompt, enter your PingOne username and password.

	Ping Kently	
USERNAME		
PASSWORD		
	Hemember Me	
	Forgot Password	

You're redirected back to Workato and signed on.

# Workday

## Configuring SAML SSO with Workday and PingFederate

Enable Workday sign-on from a PingFederate URL (IdP-initiated sign-on) and direct Workday sign-on using PingFederate (SP-initiated sign-on), with single logout (SLO).

#### Before you begin

- Configure PingFederate to authenticate against an identity provider (IdP) or datastore containing the users requiring application access.
- Populate Workday with at least one user to test access.
- You must have administrative access to PingFederate and Workday.

#### Create a PingFederate service provider (SP) connection for Workday

- 1. Sign on to the PingFederate administrative console.
- 2. Create an SP connection for Workday in PingFederate.
- 3. Set Partner's Entity ID to http://www.workday.com
- 4. Enable the IdP-Initiated SSO and SP Initiated SSO SAML profiles.
- 5. In Assertion Creation  $\rightarrow$  Authentication Source Mapping  $\rightarrow$  Attribute Contract Fulfillment, map SAML\_SUBJECT.
- 6. In Protocol Settings → Assertion Consumer Service URL:
  - 1. Set Binding to POST.
  - 2. In the Endpoint URL field, enter https://your-environment.workday.com/your-tenant-name/login-saml.flex
  - 3. In Protocol Settings → Allowable SAML Bindings, enable POST.
  - 4. In Credentials → Digital Signature Settings, select the PingFederate Signing Certificate.

#### 7. Click Save.

- 8. Export the signing certificate.
- 9. Export the metadata file, open it in a text editor, and copy:
  - The entityID
  - The SSO Location entry https://your value/idp/SS0.saml2
  - $\circ$  The SLO Location entry <code>https://your value/idp/SLO.saml2</code>

## Add the PingFederate IdP Connection to Workday

1. Sign on to Workday as an administrator and click Account Administration.

Welcome, Ping				٩
Difference O Herris	 Application 7 items	15	Deployment	Business
Go to Inibox	Analytics	Utilities	Security & Audit	Processes

## 2. Click Edit Tenant Setup – Security.

Audit	View
Signons and Attempted Signons	All Workday Accounts
Workday Accounts Currently Locked Out By Exces	Workday Accounts
Workday Accounts with Expired Passwords	View Security Groups for User
	View Implementers
Actions Edit Tenant Setur	View Implementers
Actions Edit Tenant Setur	View Implementers
Actions Edit Tenant Setu Disable Workday	View Implementers p - Security v Accounts
Actions Edit Tenant Setu Disable Workday Enable/Disable Accou	view Implementers p - Security v Accounts nt Data Masking

- 3. In the **Single Sign On** section, click the **+** icon under **Redirection URLs**.
- 4. Configure the redirection URLs:

Redirect Type	Single URL
Login Redirect URL	https://your-environment.workday.com/your-tenant-name/login- saml2.flex
Logout Redirect URL	Single logout (SLO) location from previous procedure <pre>https://your value/ idp/SLO.saml2</pre>
Mobile App Login Redirect URL	https://your-environment.workday.com/your-tenant-name/login- saml2.flex
Mobile Browser Login Redirect URL	https://your-environment.workday.com/your-tenant-name/login- saml2.flex
Environment	Select environment

5. In the SAML Setup section, select the Enable SAML Authentication check box.

SAML Setup
Enable SAML Authentication *
Enable Native Multi-Factor Authentication
SAML Identity Providers

6. Click the + icon.

SAML Identity Providers					
(+)	Identity Provider	Disabled	*Identity Provider Name	*Issuer	*x509 Certificate

- 7. Set the **Identity Provider Name** to PingFederate, and in the **Issuer** field, enter the entity ID value that you copied from PingFederate.
- 8. For SLO, in the  $x509\ certificate$  section, click Create  $x509\ Public\ Key.$

x509 Certificate	
Search	:=
Ву Туре	>
	~

9. In the **Name** field, enter a name for your PingFederate signing certificate, such as **PingFederateCert**.

10. Open the PingFederate signing certificate in a text editor, copy the contents, and paste them into the **Certificate** field.

Create	x509 Public Key
Name *	PingOneCert
Valid From	01/21/2021
Valid To	01/21/2024
Certificate 🔸	

#### 11. Click **OK**.

12. Use the following configuration.

Enable IdP Initiated Logout	Selected
Logout Response URL	Enter the SLO location that you copied from PingFederate. For example, https://your value/idp/ SLO.saml2.
Enable Workday Initiated Logout	Selected
Logout Request URL	Enter the SLO location that you copied from PingFederate. For example, https://your value/idp/ SL0.saml2.
Service Provider ID	<pre>Enter http://www.workday.com.</pre>
SP Initiated	Selected
Do Not Deflate SP-initiated Authentication Request	Selected
IdP SSO Service URL	Enter the SLO location you copied from PingFederate. For example, <a href="https://your-value/idp/SL0.saml2">https://your-value/idp/SL0.saml2</a> .

13. Click **OK**.

14. For SLO, in the x509 Private Key Pair menu, select Create x509 Private Key Pair.

x509 Private Key Pair	*	
	Search	
Enable Mobile Browser SSO for Native Apps	All	
	Create x50	09 Private Key Pair

15. In the **Name** field, enter a name for the key pair.

Create x50	9 Private Key Pai	r -	
Name	* workday		
Description			
Do Not Allow Regene	eration		el]

#### 16. Click **OK**.

17. Hover next to the key pair name and click the ... icon.

x509 Private Key Pair	workday 🚥
Enable Mobile Browser SSO for Native Apps	

### 18. In **x509 Private Key Pair**, select **View Key Pair**.

	>	× _
x509 Private Key Pair	•<	View Key Pair
Audits	>	Edit Key Pair
Integration IDs	>	Regenerate Key Pair

19. Copy the contents of the public key and save them in a text editor.

Description	(empty)
Valid From	11/30/2018
Valid To	11/30/2021
Public Key	-BEGIN CERTIFICATE-
	-END CERTIFICATE-

20. Set the Authentication Request Signature Method to SHA-256.



Leave all the other values in this section blank.

21. Click Done.

#### Update the PingFederate Workday IdP for SLO

- 1. Sign on to the PingFederate administrative console.
- 2. Edit the SP connection for Workday and add the following extra SAML profiles:
  - IDP-Initiated SLO
  - SP Initiated SLO
- 3. In Protocol Settings → SLO Service URL:
  - 1. Set Binding to POST
  - 2. Set Endpoint URL to https://your-environment.workday.com/your-tenant-name/logout-saml.htmld.
  - 3. Set Response URL to https://your-environment.workday.com/your-tenant-name/logout-saml.htmld.
- 4. In **Credentials** → **Signature Verification Settings**, select the saved Workday public key.

#### Test the PingFederate IdP-initiated SSO

- 1. Go to the PingFederate SSO Application Endpoint for the Workday SP connection.
- 2. Complete the PingFederate authentication.

	Ping Sign On
USERNAME	
PASSWORD	
	Hemember Mc
	Sign On
	Forgot Password

You are redirected to your Workday domain.



3. Click Sign Out.



## Test the PingFederate SP-initiated SSO integration

- 1. Go to your Workday URL.
- 2. After you're redirected to PingFederate, enter your PingFederate username and password.

After successful authentication, you are redirected back to Workday.



#### 3. Click Sign Out.



You are signed out.

## Configuring SAML SSO with Workday and PingOne for Enterprise

Enable Workday sign-on from the PingOne for Enterprise console (IdP-initiated sign-on) and direct WorkDay sign-on using PingOne for Enterprise (SP-initiated sign-on), with single logout (SLO).

#### Before you begin

- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Populate Workday with at least one user to test access.
- You must have administrative access to PingOne for Enterprise and Workday.

## Setup the Workday application in PingOne for Enterprise

- 1. Sign on to PingOne for Enterprise and go to **Applications**  $\rightarrow$  **Application Catalog**.
- 2. In the Application Catalog, search for Workday.

pplication Catalog		Applications / Application	Catalo
owse for the application you wan	to add or search for it by name. Don't see the applica	tion you're looking for? Fill out our Application Request Form.	
workday	Search		
Арр	lication Name	* Туре	
W	orkdav	SAML	

- 3. Expand the Workday entry and click **Setup**.
- 4. Copy the **Issuer** and **IdP ID** values.
- 5. Download the signing certificate.

1. SSO Instructions	
Signing Certificate	PingOne Account Origination Certificate (2021) V
F	or reference, please note the following configuration parameters:
SaaS ID	
IdP ID	
Initiate Single Sign-On (SSO) URL @	
Issuer	

- 6. Click Continue to Next Step.
- 7. Enter the following values.

Field	Entry
ACS URL	https://your-environment.workday.com/your-tenant-name/login-saml.flex
Entity ID	http://www.workday.com
Target Resource	https://your-tenant-name/fx/home.flex
Single Logout Endpoint	https://your-environment.workday.com/your-tenant-name/logout-saml.htmld
Single Logout Response Endpoint	https://your-environment.workday.com/your-tenant-name/logout-saml.htmld

#### 8. Click Continue to Next Step.

#### 9. Map the **SAML\_SUBJECT** attribute.

your identity bridge attrib	utes to the attributes require	ed by the application.
Application Attribute	Description	Identity Bridge Attribute or Literal Value
		SAML_SUBJECT
1 * SAME_SUBJECT	Click to Edit	UAs Literal
		Advanced

## 10. Click Continue to Next Step twice.

11. Click **Add** for each user group that should have access to Workday.

ee this application on their personal do	ck.	
Group1, Group2, etc	Search	
Group Name		
Users@directory		Remov
Domain Administrators@directory		Add

#### 12. Click Continue to Next Step.

13. Click Finish.

## Add the PingOne for Enterprise identity provider (IdP) connection to Workday

1. Sign on to Workday as an administrator and click **Account Administration**.

Welcome, Ping				٢
inbox 6 itema	 Application 7 items	15		Ē,
Ge to Inbox	Reporting & Analytics Account Administration	Integrations Willities	Deployment	Business Processes

#### 2. Click Edit Tenant Setup – Security.

Audit	view
Signons and Attempted Signons	All Workday Accounts
Workday Accounts Currently Locked Out By Exces	Workday Accounts
Workday Accounts with Expired Passwords	View Security Groups for User
Actions	View Implementers
Actions Edit Tenant Setu	View Implementers
Actions Edit Tenant Setu Disable Workday	view Implementers p - Security v Accounts
Actions Edit Tenant Setu Disable Workday Enable/Disable Accou	view Implementers p - Security v Accounts nt Data Masking

- 3. In the **Single Sign On** section, click the **+** icon under **Redirection URLs**.
- 4. Set the following properties:

Field	Entry
*Redirect Type	Single URL
Login Redirect URL	https://your-environment.workday.com/your-tenant- name/login-saml2.flex
Logout Redirect URL	<pre>https://sso.connect.pingidentity.com/sso/ SL0.saml2.workday.com/your-tenant-name/login- saml2.flex</pre>
Mobile App Login Redirect URL	https://your-environment.workday.com/your-tenant- name/logout-saml.htmld
Mobile Browser Login Redirect URL	https://your-environment.workday.com/your-tenant- name/logout-saml.htmld
Environment	Select your environment.

5. In the SAML Setup section, select the Enable SAML Authentication check box.

SAML Setup	
Enable SAML Authentication	* 🔽
Enable Native Multi-Factor Authentication	
SAML Identity Providers	

6. Click the + icon.

SAML Iden	tity Provide	ers				
Œ	Identity Provider	Disabled	*Identity Provider Name	*lssuer	*x509 Certificate	

7. Set the Identity Provider Name to PingOne and enter the Issuer value you copied previously.

8. In the x509 Certificate section, click Create x509 Public Key.

509 Certificate	
ßearch	:=
Ву Туре	>
A 11	、 、

- 9. Enter a name for your PingOne for Enterprise signing certificate, such as PingOneCert.
- 10. Open the PingOne for Enterprise signing certificate in a text editor and paste the contents of the certificate into the **Certificate** field.

Name *	PingOneCert		
Valid From	01/21/2021		
Valid To	01/21/2024		

- 11. Click **OK**.
- 12. Set the following properties.

Property	Value
Enable IdP Initiated Logout	Selected
Logout Response URL	https://sso.connect.pingidentity.com/sso/ SLO.saml2
Enable Workday Initiated Logout	Selected
Logout Request URL	<pre>https://sso.connect.pingidentity.com/sso/ SL0.saml2</pre>
Service Provider ID	http://www.workday.com
SP Initiated	Selected
Do Not Deflate SP-initiated Authentication Request	Selected
IdP SSO Service URL	<pre>https://sso.connect.pingidentity.com/sso/idp/ SSO.saml2?idpid=IdP-ID-value-from-PingOne</pre>

## 13. Click **OK**.

14. For SLO, in the x509 Private Key Pair menu, select Create x509 Private Key Pair.

x509 Private Key Pair	*	
	Search	
Fnable Mobile Browser SSO for Native Anns	All	>
Enable Configure Bound CCO	Create x50	09 Private Key Pair

15. Enter a name for the key pair.

Create x509	Private Key Pair	
Name	* workday	
Description		
Do Not Allow Regeneratio	un []	

#### 16. Click **OK**.

17. Hover next to the key pair name and click the **Menu** icon.

x509 Private Key Pair	workday 🔤
Enable Mobile Browser SSO for Native Apps	

#### 18. Click View Key Pair.

000	>	×
x509 Private Key Pair	> <	View Key Pair
Audits	>	Edit Key Pair
Integration IDs	>	Regenerate Key Pair

19. Copy the contents of the public key and save them in a text editor.

Description	(empty)
Valid From	11/30/2018
Valid To	11/30/2021
Public Key	-BEGIN CERTIFICATE-

#### 20. Set Authentication Request Signature Method to SHA-256.



21. Click Done.

## Complete the Workday SLO setup in PingOne

1. Go to PingOne for Enterprise and continue editing the Workday entry.

# (i) Note

If the session has timed out, complete the initial steps to the point of clicking Setup.

- 2. Click Continue to Next Step.
- 3. Click Choose File, and select the saved Workday public key file.



4. Click Continue to Next Step until the final screen. Click Finish.

## Test the PingOne for Enterprise IdP-initiated SSO integration

1. Go to your Ping desktop as a user with Workday access.



To find the Ping desktop URL in the admin console, go to Setup  $\rightarrow$  Dock  $\rightarrow$  PingOne Dock URL.

2. Complete the PingOne authentication.

	Ping Sign On	
USERNAME		
PASSWORD		
	Remember Mc	
	Sign On	
	Forgot Pessword	

You are redirected to your Workday environment.

Q Seen						. 53	٥	62	0
	Welcome, Ping				٥				
	Enterna Sector	 Application 2 dama Reporting & Analytics Account Account Account	S Vergenders Viller	Depiryment Estavity & Audit	Resident Processes				

## 3. Click Sign Out.

You are signed out.



## Test the PingOne for Enterprise SP-initiated SSO integration

1. Go to your Workday URL.

For example:

#### https://your-environment.workday.com/Your tenant/login-saml2.flex

2. After you're redirected to PingOne for Enterprise, enter your PingOne for Enterprise username and password.

	Ping Sign On	
USERNAME		
PASSWORD		
	Remember Mc	
	Sign On	
0	Forgot Pessword	

After successful authentication, you are redirected back to Workday.

Q Seen						23	٥	ß	0
	Welcome, Ping				ø				
	Enter State	 Applications 2 dama Paperting & Accept Accept Accept	a Maryana Mary	Depiryment Security & Apple	Reciperation				

3. Click Sign Out.



You are signed out.



# Workplace by Facebook

## Configuring SAML SSO with Workplace by Facebook and PingOne for Enterprise

Learn how to enable Workplace by Facebook sign-on from the PingOne for Enterprise console (IdP initiated sign-on) and direct Workplace by Facebook sign-on using PingOne for Enterprise (SP-initiated sign-on).

#### Before you begin

- Link PingOne for Enterprise to an identity repository containing the users requiring application access.
- Populate Workplace by Facebook with at least one user to test access.
- You must have administrative access to PingOne for Enterprise and Workplace by Facebook.

#### Set up the supplied Workplace by Facebook Application in PingOne for Enterprise

- 1. Make a note of your Workplace by Facebook Organization ID and subdomain, for example, https://myorg.workplace.com.
- 2. Sign on to PingOne for Enterprise and go to Applications → Application Catalog.
- 3. Search for Workplace by Facebook.
- 4. Expand the Workplace by Facebook entry and click the **Setup** icon.

Application	Catalog	Applications / Application Catalog
Browse for the applic	cation you want to add or search for it by	me. Don't see the application you're looking for? Fill out our Application Request Form.
workplace by	Se	ch
	Application Name	^ Туре
3	Workplace by Facebook	SAML

- 5. Copy the **Issuer** and **IdP ID** values.
- 6. Download the signing certificate.

1. SSO Instructions	
Signing Certificate	PingOne Account Origination Certificate (2021) V
Fo SaaS ID	r reference, please note the following configuration parameters:
IdP ID	
Initiate Single Sign-On (SSO) URL @	n de la complete de la constante de la constant
Issuer	

- 7. Click Continue to Next Step.
- 8. Set ACS URL to https://your-subdomain.facebook.com/work/saml.php.

Set EntityID to https://www.facebook.com/company/your-organization-ID.

Assign the attribute values for single sig	n-on (SSO) to the application.
Upload Metadata 🛛 💿	Select File Or use URL
ACS URL	https://myorg.facebook.com/work/saml.
Entity ID	//www.facebook.com/company/123456

- 9. Click Continue to Next Step.
- 10. Map SAML\_SUBJECT to the attribute containing the Facebook username value (an email address).

3. Attril	ibute Mapping			
Ma	ap your identity bridge attributes	s to the attributes required by the application	1.	
	Application Attribute	Description	Identity Bridge Attribute or Literal Value	
	1 SAML_SUBJECT	Identifies the authenticated principal. This value must match the userName value of the user being signed in. For this attribute make sure to click on the 'Advanced' button and change the 'Name ID Format to send to SP' to 'urn:oasis:names:tc:SAML:1.1:nameid- format:emailAddress'.	Email (Work)	

- 11. Click Advanced.
- 12. Set Name ID Format to urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress.

Advanced Attribute Options	×
Advanced Attribute Options for SAML_SUBJECT	
Advanced Attribute Options	
NameldFormat @	
Name ID Format to send to SP: urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress	
Attribute Mapping	
You can build an attribute mapping using multiple source attributes, literals and transformation functions.	
For example, SAML_SUBJECT can be (where each attribute value is a separate entry):	
subject = firstName + "." + lastName + "@" + domainName	
SAML_SUBJECT = Email (Work)	
IDP Attribute Name or Literal Value As Literal Function	1
1 Email (Work)	
Add Attribute	-
Close	Save

#### 13. Click Save.

#### 14. Click Continue to Next Step twice.

15. Click **Add** for all user groups that should have access to Workplace by Facebook.

Group Access		
Select all user groups that should have access to see this application on their personal dock.	his application. Users that are members of the added groups will be able to SSO to this	application and v
Group1, Group2, etc	Search	
Course Name		
		Demour
		Remove
Domain Administrators@directory		Add

#### 16. Click Continue to Next Step.

17. Download the signing certificate.



18. Click Finish.

## Add the PingOne for Enterprise IdP connection to Workplace by Facebook

- 1. Sign on to your Workplace by Facebook console as an administrator.
- 2. Go to Admin Panel  $\rightarrow$  Security.
- 3. Click the Authentication tab.
- 4. For Log in, select Single Sign-On (SSO).

#### 5. Click Add New SSO Provider.

6. Set the following field values:

Field	Setting
Allow users to login via	SSO only
SAML URL	<pre>https://sso.connect.pingidentity.com/sso/idp/ SSO.saml2?idpid=IdP-ID-value (from Set up the supplied Workplace by Facebook Application in PingOne for Enterprise)</pre>
SAML Issuer URL	Issuer-value (from Set up the supplied Workplace by Facebook Application in PingOne for Enterprise)
SAML Certificate	Paste in the contents of the signing certificate that you downloaded.



#### 7. Click Test SSO.

- 8. After a successful test, save the changes.
- 9. Go to Admin panel  $\rightarrow$  People and search for the user to use SSO.
- 10. Edit the user and select SSO for Log in with.

## (i) Note

See Workplace documentation for setting this value on users in bulk.

## Test the PingOne for Enterprise IdP-Initiated SSO integration

1. Go to your Ping desktop as a user with Workplace by Facebook access.

## (i) Note

To find the Ping desktop URL in the Admin console, go to Setup  $\rightarrow$  Dock  $\rightarrow$  PingOne Dock URL.

2. Complete PingOne for Enterprise authentication.

You are redirected to your Workplace by Facebook domain.

	<b>Ping</b> Kently,	
USERNAME		
PASSWORD		
	Remember Me	
	Forgot Password	

## Test the PingOne for Enterprise SP-initiated SSO integration

- 1. Go to https://your subdomain.workplace.com.
- 2. Enter your email address.
- 3. When you are redirected to PingOne for Enterprise, enter your PingOne for Enterprise username and password.

	Ping Keetity Sign On	
USERNAME		
PASSWORD		
	Hemember Me	
	Sign On	
	Forgot Password	

After successful authentication, you're redirected back to Workplace by Facebook.

# Wrike

## Configuring SAML SSO with Wrike and PingOne

Learn how to configure SAML SSO with Wrike and PingOne.

#### Before you begin

You must have Business Level permissions to configure SAML.

#### About this task

Learn more about Wrike and SSO in the SAML SSO: Implementation Guide C in the Wrike documentation.

i Note

This is a tested integration

#### Download the Wrike metadata

- 1. Sign on to your Wrike admin account and in the upper right-hand corner, select your name and then Settings.
- 2. Go to Security  $\rightarrow$  Setup SAML SSO.
- 3. In the Set up your identity provider list, select Other.
- 4. Download the service provider (SP) metadata:

Choose from:

- Click Download XML file.
- Copy the metadata link.
- 5. Click Next.

#### Import the metadata into PingOne

- 1. In a new tab, sign on to your PingOne SSO admin account and go to **Connections**  $\rightarrow$  **Applications** and click the **+** icon.
- 2. On the New Application page, click Advanced Configuration, and on the SAML line, click Configure.
- 3. On the Create App Profile page, enter the following information:
  - Application Name
  - Optional: Description

Wrike

• Optional: Icon

#### 4. Click Save and Continue.

5. The **Configure SAML Connection** page allows for a few options to configure the SP metadata in PingOne. Only one of the following is required to import the metadata:

Choose from:

- Click Import Metadata to import the metadata file that you downloaded in the previous procedure.
- Click Import from URL to upload the copied link from the previous procedure.
- If you know the Wrike SP metadata details, manually enter the required information.

### 🏠 Important

All required information is filled out if you choose **Import Metadata** or **Import From URL** except for the **SUBJECT NAMEID FORMAT**.

You must update the **SUBJECT NAMEID FORMAT** to urn:oasis:nams:tc:SAML:1.1:nameid-format:emailAddress . If you set this to something else, you'll get a connection error.

#### 6. Click Save and Continue.

- 7. On the Attribute mapping page, add the following attributes and mark all as Required.
  - firstName
  - lastName
  - NamelD

## (i) Note

The PingOne User Attribute for the saml\_subject must be updated to Email Address and not User ID.

- 8. Click Save and Close.
- 9. On the Applications page, click the Configuration tab and copy the URL on the IDP METADATA URL line.
- 10. On your Wrike tab, paste the URL that you copied in the previous step into the **Use URL to provide XML** field and click **Next**.
- 11. Click Enable SAML settings to finalize the configuration of the SAML connection.

You'll receive a verification email providing you with a 6-digit code.

12. Copy and paste the 6-digit code into the confirmation box to verify the connection and then click **Confirm** to finalize set up.

A page with information on testing opens.

## (i) Note

Although this page provides you with information on testing the SAML SSO set up, follow Test the integration to test your integration.

#### 13. Click Save.

## Create and assign identities in PingOne

## i) Note

If you've already assigned identities and groups in PingOne, go to Test the integration.

- 1. In PingOne, go to **Identities**  $\rightarrow$  **Groups** and click the + icon next to **Groups**.
- 2. On the Create New Group page, enter values for the following:
  - Group Name (Required)
  - Description (Optional)
  - Population (Optional)
- 3. Click Finish & Save.
- 4. To add identities to the group, on the **Identities** tab, go to **Users**  $\rightarrow$  + Add User.
- 5. On the Add User page, enter the necessary information for a user.

## 🏠 Important

Verify the first name, last name, and email address are correct, as these are values passed in the SAML assertion.

- 6. Click Save.
- 7. Assign the user that you created to the group that you created previously.

Locate the user you created and:

- 1. Expand the section for the user.
- 2. Select the **Groups** tab.
- 3. Click **+ Add**.
- 8. In the Available Groups section, select the group that you created and click the + icon to add it to the user's group memberships. Click Save.
- 9. On the **Connections** tab, for the Wrike application:
  - Click the Access tab
  - Click the Pencil icon to edit the configuration
- 10. Select the group that you created and add it to the Applied Groups section. Click Save.

You're now ready to test the integration.

## Test the integration

- 1. In the PingOne admin console, go to **Dashboard**  $\rightarrow$  **Environment Properties**.
- 2. Right-click on the Application Portal URL and open it in a private browser session.
- 3. Sign on as the test user that you created and click the Wrike tile.

You're signed on to the user's Wrike account using SSO and testing is complete.

# Zendesk

## **Configuring SAML SSO with Zendesk and PingFederate**

Learn how to configure SAML SSO with Zendesk and PingFederate.

#### About this task

The following table details the required and optional attributes to be configured in the assertion attribute contract.

Attribute Name	Description	Required / Optional
SAML-SUBJECT	Email Address	Required

The following table details the references that are used within this guide that are environment specific. Replace these with the suitable value for your environment.

Reference	Description
tenant	Zendesk Tenant name

## Create the PingFederate service provider (SP) connection for Zendesk

- 1. Sign on to the PingFederate administrative console.
- 2. Using the following information, create an SP connection in PingFederate:
  - 1. Set Partner's Entity ID to https://tenant.zendesk.com.
  - 2. Configure using Browser SSO profile SAML 2.0.
  - 3. Enable the following SAML Profiles.
    - IdP-Initiated SSO
    - SP-Initiated SSO
  - 4. In Assertion Creation → Attribute Contract Fulfillment, set the Subject Name Format to urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress.
  - 5. In Assertion Creation → Attribute Contract Fulfillment, map the attribute SAML\_SUBJECT to the attribute mail.
  - 6. In Protocol Settings → Assertion Consumer Service URL, enter https://tenant.zendesk.com/access/saml.
  - 7. In Protocol Settings → Allowable SAML Bindings, enable Redirect.

- 8. In **Credentials**, choose a suitable signing certificate and make sure the **Include the certificate in the signature <KEYINFO> element** check box is selected.
- 3. Export the metadata for the newly-created SP connection.
- 4. Export the signing certificate public key.

<b>Ping</b> Federate	AUTH	IENTICATION	APPLICATIONS	SECURITY	SYSTEM	M		Q	1	2
<ul> <li>Integration</li> <li>SP Connections</li> <li>SP Adapters</li> <li>Target URL Mapping</li> <li>SP Default URLs</li> <li>Policy Contract Adapter Mappings</li> <li>Adapter-to Adapter Mappings</li> </ul>	SP Connections On this screen you can mar Connection Name  Connection Name  Create Connection	age connections to Connection ID https://	zendesk.com	Search Virtual ID	Clear N Protocol	arrow By Enabled	✓ Action Select Action ✓			

## Configure the PingFederate IdP connection for Zendesk

- 1. Sign on to Zendesk as an administrator.
- 2. Click on the **Products** icon.
- 3. Click Admin Centre.



- 4. Click the **Security** icon.
- 5. Click Single sign-on.
| X Zen                           | idesk Admin Centre × + |  | 7  | [  | 2   | ×   |
|---------------------------------|------------------------|--|----|----|-----|-----|
| $\leftrightarrow$ $\rightarrow$ | C 🔒 cendesk.com/a      | dmin/security/sso  | \$ | *  | θ   | :   |
| ж                               | Staff members          |  |    | 88 | 2.2 | *   |
| A                               | End users              |  |    |    |     | Î   |
| B                               | Single sign-on         | Single sign-on   |    |    |     |     |
| -                               | Advanced               | Configure your single sign-on (SSO) method using information from your identity provider. Please note<br>you will need to enable SSO in the "Staff members" or "End users" sections. The same SSO<br>configuration is applied to both staff members and end users. |    |    |     |     |
| 0                               |                        | A When using SSD into up to up its up for upper identifies including their appli   |    |    |     |     |
| #                               |                        | Za when using 550 it's up to you to verify users identifies, including their entails   |    |    |     |     |
| •                               |                        | SAML   |    |    |     |     |
| ₽                               |                        |  |    |    |     |     |
|                                 |                        | JSON Web Token Configure   |    |    |     |     |
|                                 |                        |  |    |    |     |     |
|                                 |                        |  |    |    |     |     |
|                                 |                        |  |    |    |     |     |
|                                 |                        |  |    |    |     |     |
|                                 |                        |  |    |    |     | 200 |

6. In the SAML SSO URL field, enter the SSO URL for your PingFederate environment configuration.

For example:

#### https://pinghostname/idp/SSO.saml2

7. Open the **Signing** certificate you downloaded in the PingFederate SP configuration and copy the thumbprint to the **Certificate** fingerprint.

eneral	Certification P	am	
<u>S</u> how:	<all></all>	~	
Field		Value	^
Is	suer		
Va	alid from	21 January 2021 11:15:20	
Va	alid to	21 January 2024 11:15:20	_
E SU	ibject Iblic kev	RSA (2048 Bits)	- 1
Pu	blic key parameters	05 00	
Th	umbprint		
			_

8. Select the **Enabled** check box.



#### 9. Click Save.

10. Enable external authentication for **Staff members** or **End users** as required.

(j) Note
The following example enables it for <b>Staff members</b> only.
∘ Click the <b>Security</b> icon.
<ul> <li>Click Staff members.</li> </ul>

- Select the External Authentication check box.
- Click Single sign-on.
- Click Save.



## Test the integration

## For PingFederate IdP-initiated SSO

Go to the SSO Application Endpoint from the PingFederate application configuration to perform IdP-initiated SSO.

 $\label{eq:product} For example, \ \texttt{https://PingFederateHostname:PingFederatePort/idp/startSS0.ping?PartnerSpId=Zendesk} \ .$ 



# For PingOne SP-initiated SSO

1. Go to the URL for your Zendesk tenant. For example, <a href="https://tenant.zendesk.com">https://tenant.zendesk.com</a>.



2. Click I am an Agent to initiate SSO.



# Configuring SAML SSO with Zendesk and PingOne

Learn how to configure SAML SSO with ZenDesk and PingOne.

#### About this task

The following table details the required and optional attributes to be configured in the assertion attribute contract.

Attribute Name	Description	Required / Optional
SAML-SUBJECT	Email Address	Required

The following table details the references that are used within this guide that are environment specific. Replace these with the suitable value for your environment.

Reference	Description
tenant	Zendesk Tenant name

## **Create a PingOne Application for Zendesk**

- 1. Sign on to PingOne for Enterprise and go to **Applications**  $\rightarrow$  **Application Catalog**.
- 2. Search for Zendesk .
- 3. Click the **Zendesk** row.



#### 4. Click Setup.

5. In the **Signing Certificate** list, select the appropriate signing certificate.

 ← → C	admin.pingone.com/web-po	/cas/applicationcatalog		☆	* 6	3 :
	1. SSO Instructions					
	Signing Certificate	PingOne Account Origination Certificate (2021) V Download				
	Fc	eference, please note the following configuration parameters:				
	SaaS ID					
	IdP ID					
	Initiate Single Sign-On (SSO) URL ❷	tps://sso.connect.pingidentity.com/sso/sp/initsso?saasid=				1
	Issuer	tps://pingone.com/idp				
	In	der to set up SSO to Zendesk, please follow the instructions below:				
	SETTINGS > SECURITY > /	hentication				
	Label	Description				
	1 Configure SSC	arameters Check Single Sign On				
	2 Configure SSC	arameters Mode: SAML				
	3 Configure SSC	arameters SAML SSO URL: https://sso.connect.pingidentity.com/sso/idp/S IDP ID}	SO.saml2?idpid={Enter your			
	4 Configure SSC	arameters https://sso.connect.pingidentity.com/sso/terminatesession?page redirect users to}	e=https://{enter a URL to			
	5 Configure SSC	arameters IP ranges (optional): Leave blank for all IPs to use SSO.				

6. Review the steps, and make a note of the PingOne SaaS ID, IdP ID, Single Sign-On URL, and Issuer values shown.

#### 7. Click Continue to Next Step.

- 8. Make sure that ACS URL is set to https://tenant.zendesk.com/access/saml.
- 9. Make sure that Entity ID is set to https://tenant.zendesk.com.

P1 PingOne - Application Catalog × +		<u></u>		>	<
← → C	tioncatalog	☆	* 6	Э :	:
2. Connection Configuration					*
Assign the attribute values for single sig	n-on (SSO) to the application.				
Upload Metadata	Select File Or use URL				
ACS URL	https://zendesk.com/access. * Replace the parameter(s) '\$(accountname)' above with your configuration information.				1
Entity ID	Replace the parameter(s) '\$(accountname)' above with your configuration information.				
Target Resource @					
Single Logout Endpoint @	example.com/slo.endpoint				
Single Logout Response Endpoint @	example.com/sloresponse.endpoint				
Primary Verification Certificate @	Choose File No file chosen				
Secondary Verification Certificate @	Choose File No file chosen				
Force Re-authentication @					
Encrypt Assertion @					
Signing @	● Sign Assertion ) Sign Response				

- 10. Click Continue to Next Step.
- 11. In the Attribute Mapping section, in the Identity Bridge Attribute or Literal Value column of the SAML\_SUBJECTrow, enter SAML\_SUBJECT.

PingOne - Applicat	tion Catalo	y × +			-	C	3	×
← → C 🔋	admin.pi	ingone.com/web-portal/c	as/applicationcatalog		☆	*	Θ	:
		Application Name	* Type					
2		Zendesk	SAML with Pr	rovisioning (API)				
3. A1	ttribute I Map yo	Mapping ur identity bridge attribu	utes to the attributes required by the	application.				
		Application Attribute	Description	Identity Bridge Atribute or Literal Value				
	1	SAML_SUBJECT	mail	SAML_SUBJECT				
	5.55			Advanced				
			The second second for	Name or Literal				
	2	displayName	display purposes.	As Literal				
				Advanced				
			A phone number conciled as a	Name or Literal				
	з	phone	string.	C As Literal				
				Advanced				
				Name or Liferal				
	4	email	The user's primary email address	As Literal				
				Advanced				
				Name or Literal				
	5	name	The user's formatted name	As Literal				
				Advanced				+

12. Enter the values for the other attributes as required.

- 13. Click Continue to Next Step.
- 14. Update the Name, Description, and Category fields as required.

	Application Name	* Туре			
2	Zendesk	SAML with Provisioning (API)	1	×	
4. PingOne	App Customization - Zendesk				
	Icon @	2			
	Name @	Select image Zendesk			
	Description ⊕	Zendesk simplifies your support team's workflow with custom automatic actions, meaningful organization, and streamlined systems for managing support content.			

# 15. Click Continue to Next Step.

16. Add the user groups for the application.

$\rightarrow$ G	admin.pingone.com/web-portal/cas/applicationcatalog	☆	*	0	
	5. Group Access Select all user groups that should have access to this application. Users that are members of the added groups will be able to SSC see this application on their personal dock.	to this application	n and	will	
	Group1, Group2, etc Search				
	Group Name	5 ×			
	Domain Administrators@directory	Rem	ove		
	Users@directory	Rem	ove		
	NEWE Devices Solar	Continue to t	lext St	ten	
	NEX1: Keview Setup	Continue to		сp	l

# 17. Click Continue to Next Step.

18. Review the settings.

P1 Ping	One - Application Catalog × +		-		×
<b>←</b> →	C admin.pingone.com/web-portal/cas/applicatio	incatalog	\$	* 0	) =
	Application Name	* Туре			
	Zendesk	SAML with Provisioning (API)		_	
	6. Review Setup				
	Test your connection to the application				
	lcon ⊕				
	Name @	Zendesk			
	Description @	Zendesk simplifies your support team's workflow with custom automatic actions, meaningful organization, and streamlined systems for managing support content.			
	Category @	CRM			
	Connection ID				
	You may need to configure these conne	ction parameters as well.			
	saasid				
	idpid				
					+

#### 19. Copy the Single Sign-On (SSO) URL value to a temporary location.

This is the IdP-initiated SSO URL that you can use for testing.

#### 1. On the Signing Certificate line, click Download.

You'll use this in the Zendesk configuration.

#### 20. On the SAML Metadata line, click Download.

You'll use this in the Zendesk configuration.

#### 21. Click Finish.

<b>ng</b> One <sup>-</sup>		DASHBOARD	PPLICATIONS	USERS SETUP	ACCOUNT		•		Sign Off
My Application	ns Application Catalog	PingID SDK Ap	plications (	OAuth Settings					
My Applica	ations								
SAML OID	C.								
Applications you	ve added to your account	are listed here. Yo	u can search l	by application na	me, description or	entityId			
Applications you • Active applic • Details displ	I've added to your account cations are enabled for sin lays the application details	are listed here. Yo gle sign-on (SSO).	u can search I	by ap <mark>plicatio</mark> n na	me, description or	entity <mark>id</mark>			
Applications you • Active applix • Details displ	I've added to your account cations are enabled for sin lays the application details	are listed here. Yo gle sign-on (SSO).	u can search l	by application na	ne, description or	entityld			
Applications you • Active applix • Details displ	I've added to your account cations are enabled for sin ays the application details	are listed here. Yo gle sign-on (SSO). Search	u can search l	by application na	ne, description or	entityld			
Applications you <ul> <li>Active applic</li> <li>Details displ</li> </ul>	I've added to your account cations are enabled for sin lays the application details	are listed here. Yo gle sign-on (SSO). Search	u can search l	by application na	ne, description or	entityld			
Applications you • Active applix • Details displ	Ive added to your account cations are enabled for sin lays the application details Application Name	are listed here. Yo gle sign-on (SSO). Search	u can search l	by application na	ne, description or e	entityld			
Applications you <ul> <li>Active applix</li> <li>Details displ</li> </ul>	Ive added to your account cations are enabled for sin lays the application details Application Name Zendesk	are listed here. Yo gle sign-on (SSO). Search	u can search l	by application na Status Active	ne, description or d Er	antityld Iabled	Remove		
Applications you    Active applia	I've added to your account cations are enabled for sin lays the application details Application Name Zendesk	are listed here. Yo gle sign-on (SSO). Search	u can search l ype SAML	Status Active	ne, description or d Ef	abled	Remove	•	

# Configure the PingOne IdP connection for Zendesk

- 1. Sign on to Zendesk as an administrator.
- 2. Click the **Products** icon.
- 3. Click Admin Centre.



4. Click the **Security** icon.

esk Admin Centre X +			8.94	-	×
C 🔒zendesk.com/a	dmin/security/sso	☆	*	0	:
Staff members			88	2	*
End users					Ĩ
Single sign-on	Single sign-on				
Advanced	Configure your single sign-on (SSO) method using information from your identity provider. Please note you will need to enable SSO in the "Staff members" or "End users" sections. The same SSO configuration is applied to both staff members and end users.				
	22. When using 550 it's up to you to very users identifies, including their entail.				
	SAML				
	ICOM Web Token				
					-
	C Endusers Endusers Single sign-on Advanced	C               endesk.com/admin/security/sso           Staff members             Single sign-on             Advanced <t< th=""><th>C  endesk.com/sdmin/security/sso</th><th>C implementation   Staff members Find users Find u</th><th>C       •</th></t<>	C  endesk.com/sdmin/security/sso	C implementation   Staff members Find users Find u	C       •

- 5. Click Single sign-on.
- 6. In the **SSO Login URL** field, enter the URL Location for the **SingleSignOnService Location** from the PingOne SP metadata that you downloaded from the Zendesk configuration.

For example:

#### https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=idpid

7. Open the signing certificate that you downloaded in the PingOne SP configuration and paste the thumbprint into the **Certificate fingerprint** section.

	Details	Certification P	ath	
<u>S</u> how:	<all></all>		~	
Field			Value	^
Iss Va	uer lid from lid to		21 January 2021 11:15:20 21 January 2024 11:15:20	
Pu	bject blic key blic key p	arameters	RSA (2048 Bits) 05 00	
Th	umbprint			~

#### 8. Click Enabled.



#### 9. Click Save.

10. Enable external authentication for **Staff members** or **End users** as required.

i Note
The following example enables it for <b>Staff members</b> only.
∘ Click the <b>Security</b> icon.
<ul> <li>Click Staff members.</li> </ul>

- Select the External Authentication check box.
- Click Single sign-on. + Click Save.



#### Test the integration

#### Choose from:

# For PingFederate IdP-Initiated SSO

Go to the Single Sign-On (SSO) URL in the PingOne Application configuration to perform IdP initiated SSO.

For example, https://PingFederateHostname:PingFederatePort\_\_/idp/startSS0.ping?PartnerSpId=Zendesk .



# For PingOne SP Initiated SSO

1. Go to the URL for your Zendesk tenant. For example, https://tenant.zendesk.com.



2. Click I am an Agent to initiate SSO.

* * +		- o x
← → C 🕯 sendesk.com	/access/unauthenticated	🕁 🔒 Incognito 🚦
zendesk		
	Sign in to	

# Zoho

# Configuring SAML SSO with Zoho and PingOne

Learn how to configure SAML SSO using Zoho and PingOne.

#### **Configue SAML in PingOne**

1. In PingOne, go to **Connections**  $\rightarrow$  **Applications** and click the + icon.



- 2. On the New Application page, click Advanced Configuration.
- 3. On the SAML line, click Configure.

Zoho

Web applications that are accessed within a bapications that are stored and run from a. between r desktop.         A front-end application that uses an API.         Management API integrations that can performacions that can the growthere or desktop.         Apps cr	티
	nfigured by advanced users fro nd up.
+ IOS and Android apps     + Non-Interactive service integrations       • .NET web apps     • Desktop apps     • Angular       • Java apps     • Push Authentication     • Node, is	Your choice     No barriers     Complete flexibility
WEB APP NATIVE APP SINGLE PAGE APP WORKER	VANCED CONFIGURATION
CHOOSE CONNECTION TYPE	Confidure

- 4. On the Create App Profile page, enter the following details:
  - Application Name (Required)
  - Description (Optional)
  - Icon (Optional)

Cre Persor	ate App Profile nalize your application by creating a unique profile. The description
	APPLICATION NAME
	Zoho Directory
	DESCRIPTION
	Zoho SSO Configuration
	ICON
	ZOHO
	Remove Image

- 5. Click Save and Continue.
- 6. On the **Configure SAML Connection** page, in the **Provide App Metadata** section, select **Manually Enter**.

Configure SAML Connection	
SAML is an authentication protocol that acts as a service provider (SP) to PingOne (the identity provider,	or IdP).
PROVIDE APP METADATA	

# Set up SAML in Zoho

- 1. In a separate browser tab, sign on to your Zoho Directory admin account (directory.zoho.com).
- 2. Go to **Security** → **Custom Authentication**, select **Setup Now**, and note the **ACS URL** value.



- 3. Copy the ACS URL value from the previous step.
- 4. Go to your PingOne SSO browser tab and paste this value into the ACS URLS field.



#### Input the service provider (SP) data

1. Enter the **ENTITY ID** in PingOne.

# (i) Note

This configuration example uses https://directory.zoho.com. Refer to the following table for instructions on which Entity ID to use, based on your location.

Zoho Directory account DC	Identifier (Entity ID)	Relay state
US	zoho.com	https://directory.zoho.com
EU	zoho.eu	https://directory.zoho.eu
IN	zoho.in	https://directory.zoho.in
AU	zoho.com.au	https://directory.zoho.com.au
CN	zoho.com.cn	https://directory.zoho.com.cn

2. Update the SUBJECT NAMEID FORMAT to urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress.

3. In the Assertion Validity Duration (In Seconds) field, enter a value, for example 3600.

ENTITY ID	9
https://directory.zoho.com	
SLO ENDPOINT	
SLO RESPONSE ENDPOINT	
SLO BINDING HTTP POST HTTP Redirect	
urn:oasis:names:tc:SAML:1.1:nameid-format:ema	ailAddress 🗸
ASSERTION VALIDITY DURATION (IN SECONDS)	
3600	
TARGET APPLICATION URL	

4. In the Signing Key, click Download Signing Certificate and select X509 PEM (.crt)for the format.

You'll need the signing certificate later.

PingOne SSO Certificate f	or Administrators er	nvironme 🗸
Download Signing Certific	ate	
Solact format	ign Response	Sign Assertion & Response
Select IOIIIat		
IGN X509 PEM (.crt)		

5. On the Attribute Mapping tab, in the SAML Attributes section, map the Outgoing Value for saml\_subject to Email Address.



- 6. Click Save and Close.
- 7. On the **Applications** page, next to **Zoho Directory**, click the toggle to enable the connection.

19 <mark>1 (</mark> 10	Zoho Directory Client ID:			<b>(</b> : ×
Profile	Configuration	Attribute Mappings	Policies Access	
4.00	a Tuna			1
Ad	vanced Configuratio	n (SAML)		
De	scription			
Zol	ho SSO Configuration	n		
Clie	ent ID			
Ho	me Page URL			
No	Home Page Config	ured		
Sig	non URL			
Dei	fault Signon Page			

8. On the **Configuration** tab, in the **Configuration Details** section, note the **Single Logout Service** and **Single SignOn Service** values.

You'll need these to complete the next procedure.

Client ID:		💽 : ×
Profile Configuration A	ribute Mappings Policies Access	
		/
CONNECTION DETAILS		
DOWNLOAD METADATA:	Download	
ISSUER ID :	https://auth.pingone.com/	
SINGLE LOGOUT SERVICE:	https://auth.pingone.com/	
SINGLE SIGNON SERVICE:	https://auth.pingone.com/	
IDP METADATA URL:	https://auth.pingone.com/	F
INITIATE SINGLE SIGN-ON URL	https://auth.pingone.com/	
SAML SETTINGS		

# **Configure Zoho for SSO**

- 1. In Zoho, on the Custom Authentication page, paste the Single SignOn Service value from PingOne into the Sign-in URL.
- 2. Optional: Paste the Single Logout Service value from PingOne into the Sign-out URL field.

Use this value to set up SAML at your IdP Sign-in URL *
Sign-in URL *
ttps://auth.pipgapa.com/
https://autn.pingone.com/
URL to sign in to Zoho account
Sign-out URL
https://auth.pingone.com/
URL to redirect when users sign out.

- 3. Optional: If required, enter your site's password change URL in the Change Password URL field.
- 4. In the Verification Certificate section, click Browse and upload the X509 certificate that you downloaded previously.

Browse	bc2c88bd-e619-46fc-a60c-0bf2
e certificate	file must contain the public key for Zoho to
e certificate rify sign-in re	file must contain the public key for Zoho to equest.
e certificate rify sign-in re	file must contain the public key for Zoho to equest.

5. Click **Save** to save the connection and complete the setup.

## Create and assign identities in PingOne

If you've already assigned identities and groups in PingOne, move on to Test the integration.

- 1. In PingOne, go to **Identities Groups** and click the **+** icon next to **Groups**.
- 2. On the Create New Group page, enter values for the following:
  - Group Name (Required)
  - Description (Optional)
  - Population (Optional)
- 3. Click Finish & Save.

Groups     Administrators can manage their groups including creating groups, updating group membership manually or dynamically and more. Learn     Search Groups	Create New Group Groups provide application access for users.
Name	Enter Profile Data
Apps Administrators Population	Group Name
Admin	Description
	Provideling
	Administrators Population
	Finish & Save

4. To add identities to the group, on the **Identities** tab, go to **Users**  $\rightarrow$  + Add User.

Pi	ngldentity.		⑦ - ⑤ Explore - La Ryan Schafer -
Enviror Admin Product	ments strators •	Users	
<b>#</b>	< Identities	Q Search or SCIM Query Filters >	+ Add User
	Users	Example SCIM Queries	
	Groups	4 users by Family Name ~	
-	Populations		
Ð	Attributes		
U	Roles		
ø		Test, Adam	
•			
		Test, Joe joetisst	

5. On the **Add User** page, enter the required information for a user.



6. Click Save.

Add User			$\otimes$
COUNTRY CODE	LOCALITY	REGION	
ZIP CODE			
COMPANY INFORMATION			-
ACCOUNT ID		POPULATION @	
		Administrators Population	
USERNAME			
1			
TYPE			
TITLE			
PREFERENCES			
PREFERRED LANGUAGE		LOCALE	
None	~	None	
TIMEZONE Select a timezone V			
Save			
			_

7. Assign the user that you created to the group that you created previously. Locate the user and do the following:

1. Expand their section.

- 2. Select the **Groups** tab.
- 3. Click **+ Add**.

Test, Adam adamtest								Reset Password	Ī
Profile	Roles	Authentication	Groups	Consent	API	Sync Status	Credentials		
Group Me	mberships 1	+ Add							
									1

8. In the **Available Groups** section, select the group you created and click the + icon to add it to the user's group memberships. Click **Save**.

< Back to Users Adam Test		
Profile         Roles         Authentication         Groups           0         Groups define a collection of unany units membership of builded reliants filesing ordering ordering ordering filesing ordering ordering ordering ordering		
Groups denne a Conectori or daels dang menutersing or by opienisc mening chemic droups can be deed to assign approach acce     Q. Search Available Groups	53 UU USETS.	
AVAILABLE GROUPS	GROUP MEMBERSHIPS	
# Admin	Apps     Administrators Population	$\bigcirc$

- 9. On the **Connections** tab, for the Zoho Directory application, do the following:
  - 1. Click the **Access** tab.
  - 2. Click the **Pencil** icon to edit the configuration.

<b>e/ 11</b> 0	Zoho Directory Client ID: c			<b>()</b> : >
Profile	e Configuration	Attribute Mappings	Policies Access	
GR	OUP MEMBERSHIP PO	ICY		1

3. Select the group that you created and add it to the **Applied Groups** section. Click **Save**.

Zoho Directory > Edit Access		×
Admin Only Access		
Must have admin role		
Group Membership Policy		
Groups can be added to control user access to the The following selections determine groups that h	ne application. All users have access when no groups are listed. ave access to the application.	
Q Search Groups		
ALL GROUPS	APPLIED GROUPS	
ii Admin	+ Apps Administrators Population	-
5		

# Test the integration

- 1. In the PingOne admin console, go to **Dashboard**  $\rightarrow$  **Environment Properties**.
- 2. Right-click on the **Application Portal URL** and open it in a private browser session.





3. Sign on as the test user that you created and click the **Zoho Directory** tile.

All Applications	Applications				Q Find applications			Ryan S		
	ALL APPLICATIONS									
	Aha!	DATADOG	freshworks	٢	PagerDuty	Ping	् quickbase	🗸 wrike	2600	
	Aha Labs	Datadog	Freshworks	Неар	PagerDuty	Ping Identity	QuickBase	Wrike	Zoho Directory	

You're signed on to the user's Zoho Directory account.