



PingIdentity Cyberark Authentication Integration Technical Documentation

Ping Identity

<https://www.pingidentity.com>

PingFederate (v9.1.4) and PingOne

September 2019

SOLUTION OVERVIEW

The following guide provides information for configuring a SAML connection to the Cyberark solution from both the PingFederate and PingOne Single Sign-On (SSO) solutions.

KEY BENEFITS

PingFederate Overview:

PingFederate enables outbound and inbound solutions for single sign-on (SSO), federated identity management, customer identity and access management, mobile identity security, API security, and social identity integration. Browser-based SSO extends employee, customer and partner identities across domains without passwords, using only standard identity protocols (Security Assertion Markup Language—SAML, WS-Federation, WS-Trust, OAuth and OpenID Connect, and SCIM).

PingFederate Documentation Reference:

<https://documentation.pingidentity.com/pingfederate/pf92/index.shtml#gettingStartedGuide/introductionGettingStarted.html>

PingOne Overview:

PingOne is a cloud-based identity as a service (IDaaS) framework for secure identity access management. You will use PingOne to give members of your organization secure single sign-on (SSO) to cloud applications.

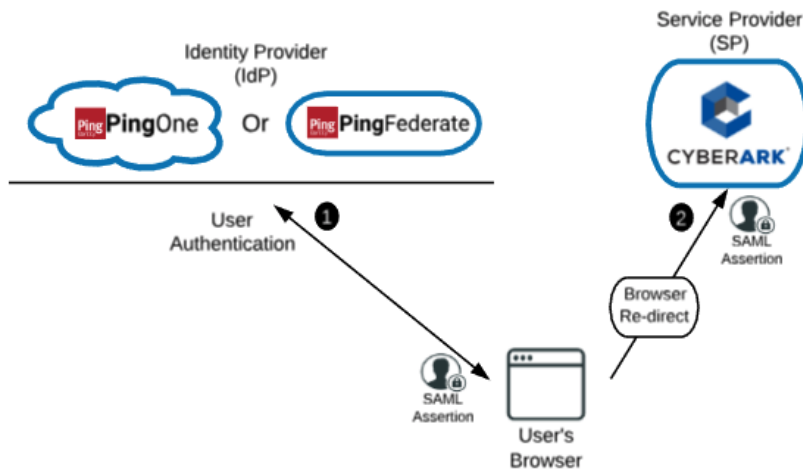
PingOne Documentation Reference:

<https://documentation.pingidentity.com/pingone/employeeSsoAdminGuide/index.shtml#adminOverview.html>

This integration was tested with CyberArk v9.x, v10.x, and Private Cloud.

Currently IDP initiated workflows are not supported.

DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



Process:

1. User initiates an Identity Provider (IdP) URL to access Cyberark. The IdP solution (PingOne or PingFederate) validates the user through the configured authentication flow.
 - a. (Not shown) Alternatively, the user could attempt to access Cyberark directly. Cyberark would re-direct the user to step 1, with a SAML request, to validate the user.
2. Upon user validation, the IdP solution re-directs the user's browser to Cyberark with a SAML assertion.
3. (Not shown) Cyberark validates the SAML assertion and grants access.

INSTALLATION & INTEGRATION CONFIGURATION

The following information will be needed from your Cyberark environment to configure a SAML connection in PingFederate or PingOne:

- Cyberark's SAML Entity ID (Audience Value). In the step-by-step SAML configuration, the value of '**PasswordVault**' will be used.
- Cyberark's Assertion Consumer Service (ACS) URL (POST Method). In this step-by-step SAML configuration example, the value of '**https://components.cyberark.local/PasswordVault/auth/saml/**' will be used

The following information will be provided to the Cyberark solution:

- PingFederate Signing Certificate used by the SAML connection settings. Certificate can be exported from the 'Server Configuration -> Certificate Management -> Signing & Decryption Keys & Certificates' section under the Action field.
- PingFederate's SAML Entity ID. Can be located under the 'Server Configuration -> System Settings -> Server Settings -> Federation Info' section

- PingFederate's IdP Url for SAML requests: https://<pingfederate base URL>/idp/SSO.saml2

Or,

- PingOne's Signing Certificate used by the SAML connection settings. Can be downloaded from the 'Application -> Cyberark SAML connection' section.
- PingOne's SAML Entity ID. Can be located from the 'Application -> Cyberark SAML connection -> entityId' section.
- PingOne's IdP Url for SAML Requests. Can be located from the 'Application -> Cyberark SAML connection -> Initiate Single Sign-On URL' section.

INTEGRATION STEPS

PINGONE SAML CONNECTION CONFIGURATION

In the PingOne Administration console go to 'APPLICATIONS -> My Applications -> Add Application -> New SAML Application'.

Section: (Application Details)

The screenshot shows the 'New Application' form in the PingOne Administration console, specifically the 'SAML' tab. The form is titled '1. Application Details'. It contains the following fields:

- Application Name:** A text input field containing 'CyberArk'.
- Application Description:** A text area containing the text: 'CyberArk is the global leader in privileged access security, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline.' Below the text area is a small note: 'Max 500 characters'.
- Category:** A dropdown menu with 'Other' selected.
- Application Icon:** A section for selecting an icon. It includes the text 'For use on the dock' and a preview of the CyberArk logo. Below the preview is a 'Change' button. A small note below the icon section says 'Max Size: 256px x 256px'.

At the bottom of the form, there is a 'NEXT: Application Configuration' label, a 'Cancel' button, and a 'Continue to Next Step' button.

Enter an 'Application Name', 'Application Description', 'Category' and a logo. Click 'Continue to Next Step'.

Section: (Application Configuration)

New Application SAML Incomplete No

2. Application Configuration

I have the SAML configuration I have the SSO URL

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

Signing Certificate PingOne Account Origination Certificate

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

Assertion Consumer Service (ACS)

Entity ID

Application URL

Single Logout Endpoint

Single Logout Response Endpoint

Single Logout Binding Type ☐ Redirect ☐ Post

Primary Verification Certificate No file selected.

Secondary Verification Certificate No file selected.

Encrypt Assertion ☐

Signing Algorithm

Force Re-authentication ☐

Force MFA ☐

Keep the following in mind when creating your connection:

1. Both SP- and IdP-initiated SSO are allowed
2. Map SAML_SUBJECT in your attribute contract, plus any attributes (configure them in PingOne later)
3. Allow outbound POST or redirect
4. Allow outbound POST

NEXT: SSO Attribute Mapping

In the 'I have the SAML configuration' section, enter the 'Assertion Consumer Service (ACS)' value. In this example, 'https://components.Cyberark.local/PasswordVault/auth/saml/' is used. Also, Enter the 'Entity ID'. In this example 'PasswordVault' is used. Click 'Continue to Next Step'.

Section: (SSO Attribute Mapping)

New Application SAML Incomplete No

3. SSO Attribute Mapping

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

	Application Attribute	Identity Bridge Attribute or Literal Value	As Literal	Advanced	Required	
1	SAML_SUBJECT	<Username Identifier>	☐	☐	☐	X

NEXT: Review Setup

Enter the 'Identity Bridge Attribute' from your configuration. This the user value to identify a Cyberark user. Click 'Save & Publish'.

PINGFEDERATE SAML CONNECTION CONFIGURATION

In the PingFederate administrative console go to, 'Identity Provider -> SP Connections -> Create New':

Section: (Connection Type)

The screenshot shows the PingFederate administrative console interface. On the left is a navigation menu with 'MAIN' (Identity Provider, Service Provider, OAuth Server) and 'SETTINGS' (Server Configuration). The main content area is titled 'SP Connection' and has tabs for 'Connection Type', 'Connection Options', 'Import Metadata', 'General Info', 'Browser SSO', and 'Credentials'. The 'Connection Type' tab is active, showing an 'Activation & Summary' section. It instructs the user to select a connection type for the SP. Below this, there are three options: 'No Template', 'BROWSER SSO PROFILES' (which is selected with a checkmark and shows 'PROTOCOL SAML 2.0'), 'WS-TRUST STS', and 'OUTBOUND PROVISIONING'. At the bottom right are 'Cancel' and 'Next' buttons.

Select 'BROWSER SSO PROFILES' AND SAML 2.0. Click 'Next'.

Section: (Connection Options)

The screenshot shows the same PingFederate administrative console, but now the 'Connection Options' tab is active. It instructs the user to 'Please select options that apply to this connection.' There are three options: 'BROWSER SSO' (checked with a checkmark), 'IDP DISCOVERY', and 'ATTRIBUTE QUERY' (unchecked). At the bottom right are 'Cancel', 'Previous', and 'Next' buttons.

Make sure 'BROWSER SSO' is checked. Click 'Next'

Section: (Import Metadata)

The screenshot shows the 'Import Metadata' tab selected in the 'SP Connection' configuration. The left sidebar contains a navigation menu with 'Identity Provider' highlighted under the 'MAIN' section. The main content area has a sub-header 'SP Connection' and a tabbed interface with 'Import Metadata' as the active tab. Below the tabs, there is a section titled 'Activation & Summary' with a text block explaining that metadata can be imported from a file or URL. A 'METADATA' section contains three radio buttons: 'NONE' (selected), 'FILE', and 'URL'. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

Select 'NONE' for 'METADATA'. Click 'Next'.

Section: (General Info)

The screenshot shows the 'General Info' tab selected in the 'SP Connection' configuration. The left sidebar is the same as the previous screenshot. The main content area has a sub-header 'SP Connection' and a tabbed interface with 'General Info' as the active tab. Below the tabs, there is a text block explaining the fields. The form contains several input fields: 'PARTNER'S ENTITY ID (CONNECTION ID)' with the value 'PasswordVault', 'CONNECTION NAME' with the value 'CyberArc', 'VIRTUAL SERVER IDS' with an 'Add' button, 'BASE URL', 'COMPANY', 'CONTACT NAME', 'CONTACT NUMBER', 'CONTACT EMAIL', 'APPLICATION NAME', and 'APPLICATION ICON URL'. At the bottom, there is a 'LOGGING MODE' section with four radio buttons: 'NONE', 'STANDARD' (selected), 'ENHANCED', and 'FULL'. At the bottom right, there are 'Cancel', 'Previous', 'Next', and 'Save' buttons.

Enter the '**PasswordVault**' for the 'PARTNER'S ENTITY ID' and provide a desired name for the 'Connection Name'. Click 'Next'.

Section: (Browser SSO)

The screenshot shows the 'SP Connection' configuration page in PingFederate. The left sidebar has a 'MAIN' section with 'Identity Provider' selected, and a 'SETTINGS' section with 'Server Configuration' selected. The main content area has tabs for 'Connection Type', 'Connection Options', 'Metadata URL', 'General Info', 'Browser SSO', and 'Credentials'. The 'Browser SSO' tab is active, showing a 'BROWSER SSO CONFIGURATION' section with a 'Configure Browser SSO' button. At the bottom right are 'Cancel', 'Previous', 'Next', and 'Save' buttons.

Click on 'Configure Browser SSO'.

Section: (SAML Profiles)

The screenshot shows the 'SP Connection | Browser SSO' page with the 'SAML Profiles' tab selected. It contains two columns of checkboxes: 'Single Sign-On (SSO) Profiles' and 'Single Logout (SLO) Profiles'. Under SSO, 'IDP-INITIATED SSO' and 'SP-INITIATED SSO' are checked. Under SLO, 'IDP-INITIATED SLO' and 'SP-INITIATED SLO' are unchecked. At the bottom right are 'Cancel', 'Next', 'Done', and 'Save' buttons.

Check both 'IDP-INITIATED SSO' and 'SP-INITIATED SSO'. Click 'Next'.

Section: (Assertion Lifetime)

The screenshot shows the 'SP Connection | Browser SSO' page with the 'Assertion Lifetime' tab selected. It contains two input fields: 'MINUTES BEFORE' and 'MINUTES AFTER', both with a value of '5'. At the bottom right are 'Cancel', 'Previous', 'Next', 'Done', and 'Save' buttons.

Leave the '5' minute defaults or adjust as needed. Click 'Next'.

Section: (Assertion Creation)

The screenshot shows the 'Assertion Creation' step in the PingFederate configuration interface. The left sidebar contains a 'MAIN' section with 'Identity Provider', 'Service Provider', and 'OAuth Server', and a 'SETTINGS' section with 'Server Configuration'. The main content area is titled 'SP Connection | Browser SSO' and has tabs for 'SAML Profiles', 'Assertion Lifetime', 'Assertion Creation' (selected), 'Protocol Settings', and 'Summary'. Below the tabs, a description states: 'This task provides the configuration for creating SAML assertions to enable SSO access to resources at your SP partner's site.' The 'Assertion Configuration' table shows: IDENTITY MAPPING: Standard, ATTRIBUTE CONTRACT: SAML_SUBJECT, ADAPTER INSTANCES: 1, and AUTHENTICATION POLICY MAPPINGS: 0. A 'Configure Assertion Creation' button is present. At the bottom right are 'Cancel', 'Previous', 'Next', 'Done', and 'Save' buttons.

Assertion Configuration	
IDENTITY MAPPING	Standard
ATTRIBUTE CONTRACT	SAML_SUBJECT
ADAPTER INSTANCES	1
AUTHENTICATION POLICY MAPPINGS	0

Click on 'Configure Assertion Creation'.

Section: (Identity Mapping)

The screenshot shows the 'Identity Mapping' step in the PingFederate configuration interface. The left sidebar is identical to the previous screen. The main content area is titled 'SP Connection | Browser SSO | Assertion Creation' and has tabs for 'Identity Mapping' (selected), 'Attribute Contract', 'Authentication Source Mapping', and 'Summary'. A description states: 'Identity mapping is the process in which users authenticated by the IdP are associated with user accounts local to the SP. Your selection may affect the way that the SP will look up and associate the user to a specific local account.' Three options are listed: 'STANDARD' (selected with a radio button), 'PSEUDONYM' (radio button), and 'TRANSIENT' (radio button). Each option has a checkbox for 'INCLUDE ATTRIBUTES IN ADDITION TO THE PSEUDONYM/TRANSIENT IDENTIFIER'. At the bottom right are 'Cancel', 'Next', 'Done', and 'Save' buttons.

Make sure 'STANDARD' is selected. Click 'Next'

Section: (Attribute Contract)

Ping Identity

MAIN

IP

Identity Provider

SP

Service Provider

AM

OAuth Server

SETTINGS

Server Configuration

SP Connection | Browser SSO | Assertion Creation

Identity Mapping

Attribute Contract

Authentication Source Mapping

Summary

An Attribute Contract is a set of user attributes that this server will send in the assertion.

Attribute Contract

Subject Name Format

SAML_SUBJECT

urn:oasis:names

Extend the Contract

Attribute Name Format

Action

urn:oasis:names

Add

Cancel

Previous

Next

Done

Save

Copyright © 2003-2018
Ping Identity Corporation
All rights reserved.
Version 91.4.0

Only 'SAML_SUBJECT' is needed. No need to Extend the Contract. Click 'Next'.

Section: (Authentication Source Mapping)


PingFederate

MAIN

Identity Provider

Service Provider

OAuth Server

SETTINGS

Server Configuration

SP Connection | Browser SSO | Assertion Creation

Identity Mapping

Attribute Contract

Authentication Source Mapping

Summary

PingFederate uses IdP adapters, partner IdPs or Authentication Policies to authenticate users to your SP. Users may be authenticated by one of several different adapters or authentication policy contracts, so map an adapter instance for each IDP system or a authentication policy contract for each policy.

Adapter Instance Name	Virtual Server IDs	Action
HTMLForm		Delete

Authentication Policy Contract Name	Virtual Server IDs	Action
-------------------------------------	--------------------	--------

Map New Adapter Instance

Map New Authentication Policy

Cancel

Previous

Next

Done

Save

Copyright © 2003-2018
Ping Identity Corporation
All rights reserved
Version 38.4.0

Map the required authentication Adapter or Policy Contract from your environment. In this example, we will use the HTML Form adapter for authentication by clicking on 'Map New Adapter Instance'.

Section: (Attribute Contract Fulfillment)

Ping Federate

MAIN

Identity Provider

Service Provider

OAuth Server

SETTINGS

Server Configuration

SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping

Adapter Instance | Mapping Method | Attribute Contract | Issuance Criteria | Summary

Fulfill your Attribute Contract with values from the authentication adapter or with dynamic text values.

Attribute Contract	Source	Value	Actions
SAML_SUBJECT	Adapter	username	None available

Cancel Previous Next Done Save

Copyright © 2003-2018
Ping Identity Corporation
All rights reserved
Version 9.1.4.0

Map the user identifier value needed by Cyberark. In this example, Source is the 'Adapter' and the Value is the 'username'. Click 'Next'.

The following steps navigates you to the next configuration screen:

- Click 'Next' on the following 'Issuance Criteria' screen.
- Click 'Done' on the IdP Adapter Mapping 'Summary' screen.
- Click 'Next' on the Assertion Creation 'Authentication Source Mapping' screen.
- Click 'Done' on the Assertion Creation 'Summary' screen.

Section: (Assertion Creation)

Ping Federate

MAIN

Identity Provider

Service Provider

OAuth Server

SETTINGS

Server Configuration

SP Connection | Browser SSO

SAML Profiles | Assertion Lifetime | Assertion Creation | Protocol Settings | Summary

This task provides the configuration for creating SAML assertions to enable SSO access to resources at your SP partner's site.

Assertion Configuration

IDENTITY MAPPING Standard

ATTRIBUTE CONTRACT SAML_SUBJECT

ADAPTER INSTANCES 1

AUTHENTICATION POLICY MAPPINGS 0

Configure Assertion Creation

Cancel Previous Next Done Save

Click 'Next'.

Click 'Configure Protocol Settings' on the 'Protocol Settings' screen.

Section: (Assertion Consumer Service URL)

The screenshot shows the 'Protocol Settings' page for an 'SP Connection | Browser SSO'. The left sidebar has 'Identity Provider' selected under 'MAIN'. The main content area has tabs for 'Assertion Consumer Service URL', 'Allowable SAML Bindings', 'Signature Policy', 'Encryption Policy', and 'Summary'. The 'Assertion Consumer Service URL' tab is active. It contains a text area with the following text: 'As the IdP, you send SAML assertions to the SP's Assertion Consumer Service. The SP may request that the SAML assertion be sent to one of several URLs, via different bindings. Please provide the possible assertion consumer URLs below and select one to be the default.'

Default	Index	Binding	Endpoint URL	Action
default	0	POST	https://components.cyberark.local/PasswordVault/auth/saml/	Edit Delete

Below the table is an 'Add' button and a form with a checkbox, an input field, a binding dropdown (currently showing '- SELECT -'), another input field, and an 'Add' button.

At the bottom right are buttons: 'Cancel', 'Next', 'Done', and 'Save'.

Enter the following values:

- Index -> 0
- Binding -> POST
- Endpoint -> <https://<Your PVWA ADDRESS>/PasswordVault/auth/saml/>

Click 'Add' and then 'Next'

Section: (Allowable SAML Bindings)

The screenshot shows the 'Protocol Settings' page for an 'SP Connection | Browser SSO'. The left sidebar has 'Identity Provider' selected under 'MAIN'. The main content area has tabs for 'Assertion Consumer Service URL', 'Allowable SAML Bindings', 'Signature Policy', 'Encryption Policy', and 'Summary'. The 'Allowable SAML Bindings' tab is active. It contains a text area with the following text: 'When the SP sends messages, what SAML bindings do you want to allow?'

Below the text area are four checkboxes:

- ☐ ARTIFACT
- ☒ POST
- ☒ REDIRECT
- ☐ SOAP

At the bottom right are buttons: 'Cancel', 'Previous', 'Next', 'Done', and 'Save'.

Uncheck 'Artifact' and 'Soap'. These bindings are not used. Click 'Next'.

Section: (Signature Policy)

The screenshot shows the PingFederate web interface. On the left is a navigation menu with 'MAIN' and 'SETTINGS' sections. Under 'MAIN', 'Identity Provider' is selected. Under 'SETTINGS', 'Server Configuration' is selected. The main content area is titled 'SP Connection | Browser SSO | Protocol Settings'. It has four tabs: 'Assertion Consumer Service URL', 'Allowable SAML Bindings', 'Signature Policy' (which is active), and 'Encryption Policy'. Below the tabs is a 'Summary' section with a paragraph of text: 'Additional guarantees of authenticity may be agreed upon between you and your partner. For SP-initiated SSO, you can choose to require signed authentication requests sent via the POST or redirect bindings. You can also choose to sign assertions sent to your partner, regardless of the binding used.' Below this text are three checkboxes: 'REQUIRE AUTHN REQUESTS TO BE SIGNED WHEN RECEIVED VIA THE POST OR REDIRECT BINDINGS' (unchecked), 'ALWAYS SIGN ASSERTION' (unchecked), and 'SIGN RESPONSE AS REQUIRED' (checked). At the bottom right are buttons for 'Cancel', 'Previous', 'Next', 'Done', and 'Save'.

Leave default settings (None checked). Click 'Next'.

Section: (Encryption Policy)

The screenshot shows the PingFederate web interface, similar to the previous one, but with the 'Encryption Policy' tab selected. The 'Summary' section contains a paragraph: 'Encryption may be applied to SAML messages for an added layer of protection in transport. If enabled, SAML Response messages may always be signed, regardless of the signature policy.' Below this are three radio button options: 'NONE' (selected), 'THE ENTIRE ASSERTION' (unchecked), and 'ONE OR MORE ATTRIBUTES' (unchecked). There is also a checkbox for 'SAML_SUBJECT' which is unchecked. At the bottom right are buttons for 'Cancel', 'Previous', 'Next', 'Done', and 'Save'.

Leave default settings 'None'. Click 'Next'.

The following steps navigates to the 'Credentials' screen:

- Click 'Done' on the 'Protocol Settings -> Summary' screen.
- Click 'Next' on the 'Browser SSO -> Protocol Settings' screen.
- Click 'Done' on the 'Browser SSO -> Summary' screen.
- Click 'Next' on the 'Browser SSO' screen

Section: (Credentials)

The screenshot shows the 'SP Connection' configuration page in PingFederate, specifically the 'Credentials' tab. The left sidebar contains a navigation menu with 'MAIN' (Identity Provider, Service Provider, OAuth Server) and 'SETTINGS' (Server Configuration). The main content area has tabs for 'Connection Type', 'Connection Options', 'Metadata URL', 'General Info', 'Browser SSO', and 'Credentials'. The 'Credentials' tab is active, showing an 'Activation & Summary' section. Below this, a 'Credential Requirement' table lists a 'DIGITAL SIGNATURE' requirement with a value of '01:67:66:CD:3F:0F (CN=CyberArk, O=Ping, C=US)'. A 'Configure Credentials' button is present. At the bottom right, there are 'Cancel', 'Previous', 'Next', and 'Save' buttons.

Click on 'Configure Credentials'.

Section: (Digital Signature Settings)

The screenshot shows the 'SP Connection | Credentials' configuration page in PingFederate, specifically the 'Digital Signature Settings' tab. The left sidebar is the same as the previous screenshot. The main content area has tabs for 'Digital Signature Settings' and 'Summary'. The 'Digital Signature Settings' tab is active, showing instructions: 'You may need to digitally sign SAML messages or security tokens to protect against tampering. Please select a key/certificate to use from the list below.' Below this, there is a 'SIGNING CERTIFICATE' dropdown menu with the selected value '01:67:66:CD:3F:0F (CN=CyberArk, O=Ping, C=US)'. A checkbox labeled 'INCLUDE THE CERTIFICATE IN THE SIGNATURE <KEYINFO> ELEMENT.' is unchecked. Below that, there is a 'SIGNING ALGORITHM' dropdown menu with the selected value 'RSA SHA256'. A 'Manage Certificates' button is at the bottom left. At the bottom right, there are 'Cancel', 'Next', 'Done', and 'Save' buttons.

Select the 'Signing Certificate' that will be used for Cyberark (RSA SHA256). This certificate will be provided to Cyberark needed for SAML validation. Click 'Next' and then 'Done' on the Summary Screen.

Click 'Next' on the 'Credentials' screen.

In the 'Activation and Summary' screen, the IdP initiated URL can be copied from the 'SSO Application Endpoint' field. Click 'Save'

CYBERARK SAML CONFIGURATION

- 1) Start by login as Administrator then go to Administration -> Options. Find the **Authentication Methods** section and expanded. Click on **SAML** and fill in the following parameters:

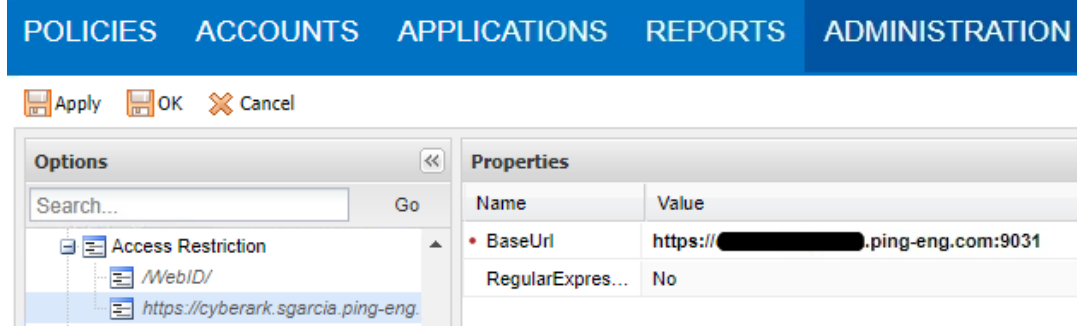
The screenshot shows the CyberArk Administration console with the 'ADMINISTRATION' tab selected. Below the navigation bar, there are buttons for 'Apply', 'OK', and 'Cancel'. The main window is divided into two panes. The left pane, titled 'Options', shows a tree view under 'Authentication Methods' with 'saml' selected. The right pane, titled 'Properties', shows a table of configuration parameters for the selected 'saml' method. The 'DisplayName' and 'Enabled' rows are highlighted with a red rectangle.

Name	Value
Id	saml
DisplayName	Ping Identity SAML
Enabled	Yes
MobileEnabled	No
LogoffUrl	
UseVaultAuthentication	No
UseRadius	No
UseLDAP	No

DisplayName: Choose a name that will clearly identify Ping Identity. It will be displayed in the PVWA logon screen.

Enabled: Must be set to **Yes**.

- 2) Scroll down to find the **Access Restriction**. Right click on it and select **Add Allowed Referrer**. Then enter the URL of your Ping Identity tenant host:



Also make sure that **RegularExpression** is set to **No**.

Note: Make sure to click on **Apply** and that the “Your changes have been saved successfully” dialog appears on the screen.

- 3) Find the PVWA **web.config** file and locate the **<appSettings>** section:

```
<appSettings>
  <add key="VaultFile" value="C:\CyberArk\Password Vault Web Access\VaultInfo\Vault.ini" />
  <add key="GWFile" value="C:\CyberArk\Password Vault Web Access\CredFiles\gwuser.ini" />
  <add key="HomePage" value="default.aspx" />
  <add key="CustomerLogoURL" value="..\images/header_cobrand.gif" />
  <add key="ConfigurationCredentialFile" value="C:\CyberArk\Password Vault Web Access\CredFiles\appuser.ini" />
  <add key="ConfigurationSafeName" value="PVWAConfig" />
  <add key="LogFolder" value="c:\windows\temp\PVWA" />
  <!-- Valid values: "" - use temp folder -->
  <add key="ApplicationID" value="" />
  <add key="MultilingualSupport" value="No" />
  <add key="InternalUsersPasswordChangeInterval" value="3600" />
  <add key="MobileVersionEnabled" value="yes" />
  <add key="FullVersionEnabled" value="yes" />
  <add key="RSADecodeUserName" value="yes" />
  <add key="IdentityProviderLoginURL" value="https://[redacted].ping-eng.com:9031/ldp/SSO.saml2" />
  <add key="IdentityProviderCertificate" value="" />
  <add key="Issuer" value="PasswordVault" />
</appSettings>
```

You'll need the **IdentityProviderLoginURL** and **IdentityProviderCertificate** from Ping. Make sure to get an ASCII export of the certificate and remove all CR's (should be a single line). Set the **Issuer** to the default value of PasswordVault.

Save the file and then restart IIS.

TROUBLESHOOTING

If you're having trouble login in, be aware that:

- Currently CyberArk doesn't support native IDP initiated login flows
- We support only specific configurations of the SAML response
- We must have the audience configured

Detailed information is provided [here](#). Please make sure the instructions to configure the IDP are followed, before contacting CyberArk Technical Support.

PINGIDENTITY CONTACT INFO

Business Contacts	Name	Matt Martin
	Email	mattmartin@pingidentity.com
	Tel	303.396.6236
	Name	Matt Bates
	Email	mattbates@pingidentity.com
Technical Contact	Name	Peter Holko
	Email	peterholko@pingidentity.com
Support Contact	Name	Ping Identity Support
	Email	support@pingidentity.com
	Tel	303.468.2857