

PingAccess Lab Guide

Protect WebApp using PingAccess

In this section, we protect a web application hosted on Tomcat.

1. PingFederate configuration for protected web app

1. Create a Simple Username Password Credential Validator

Goto System > Password Credential Validator > Create New Instance

Password Credential Validators | Create Credential Validator Instance

Type

Instance Configuration

Summary

Password Credential Validator configuration summary:

Create Credential Validator Instance

Type	
Instance Name	PCV
Instance ID	PCV
Type	Simple Username Password Credential Validator
Class Name	org.sourceid.saml20.domain.SimpleUsernamePasswordCredentialValidator
Parent Instance Name	None

Instance Configuration

Users	testuser 1, ***** false
-------	-------------------------

2. Create an IdP Adapter and attach this newly created PCV to the adapter

Goto Authentication > IdP Adapters > Create New Instance

In this lab a new IdP HTML adapter **PAHTMLAdapter** is created

IdP Adapters | Create Adapter Instance

Type

IdP Adapter

Extended Contract

Adapter Attributes

Adapter Contract Mapping

Summary

IdP adapter instance summary information

Create Adapter Instance

Type

Instance Name

Instance ID

Type

Class Name

Parent Instance Name

PAHTMLAdapter

PAHTMLAdapter

HTML Form IdP Adapter

com.pingidentity.adapters.htmlform.idp.htmlformIdpAuthAdapter

None

IdP Adapter

Credential Validators

Challenge Retries

Session State

Session Timeout

Session Max Timeout

Allow Password Changes

Password Management System

Enable 'Remember My Username'

Enable 'This Is My Device'

Change Password Policy Contract

Change Password Notification

Show Password Expiring Warning

Password Reset Type

Password Reset Policy Contract

Revoke Sessions After Password Change Or Reset

Account Unlock

Local Identity Profile

Notification Publisher

Enable Username Recovery

Login Template

Logout Path

Logout Redirect

Logout Template

PCV

3

None

60

480

false

false

false

false

false

None

false

false

None Selected

None Selected

false

html form login template.html

idp.logout.success.page.template.html

3. Create Access Token Management Instance

Access Token Management | Create Access Token Management Instance

Type

Instance Configuration

Session Validation

Access Token Attribute Contract

Resource URIs

Access Control

Summary

The values for the selected Access Token Management instance.

INSTANCE NAME

INSTANCE ID

TYPE

CLASS NAME

PARENT INSTANCE

Access Token for PingAv

paToken

JSON Web Tokens

com.pingidentity.pf.access.token.management.plugins.JwtBearerAccessTokenManagementPlugin

None

Access Token Management | Create Access Token Management Instance

Type

Instance Configuration

Session Validation

Access Token Attribute Contract

Resource URIs

Access Control

Summary

Complete the configuration necessary to issue and validate access tokens. This configuration was designed into, and is specific to, the selected Access Token Management plugin.

A JSON Web Token (JWT) Bearer Access Token Management Plug-in that enables PingFederate to issue (and optionally validate) cryptographically secure self-contained OAuth access tokens.

Symmetric Keys

Key ID	Key	Encoding	Action
Add a new row to 'Symmetric Keys'			

Certificates

Key ID	Certificate	Action
pkakey	CN=pingbootcampcert, O=Deloitte, L=, (01:8E:AF:00:7F:67 Exp: Apr 05, 2025)	Edit Delete
Add a new row to 'Certificates'		

Field Name	Field Value	Description
TOKEN LIFETIME	120	Defines how long, in minutes, an access token is valid.
USE CENTRALIZED SIGNING KEY	<input type="checkbox"/>	Select this option to use a centralized key when signing JWTs using an RSA-based or EC-based algorithm.
JWS ALGORITHM	RSA using SHA-256	The HMAC or signing algorithm used to protect the integrity of the token. For HMAC, the active symmetric key must be selected below. For RSA or EC, the active signing certificate must be selected. Integrity protection can also be achieved using symmetric encryption, in which case this field can be left unselected.
ACTIVE SYMMETRIC KEY ID	-- Select One --	The Key ID of the key to use when producing JWTs using an HMAC-based algorithm.
ACTIVE SIGNING CERTIFICATE KEY ID	pkakey	The Key ID of the key pair and certificate to use when producing JWTs using an RSA-based or EC-based algorithm.

Access Token Management | Create Access Token Management Instance

Type

Instance Configuration

Session Validation

Access Token Attribute Contract

Resource URIs

Access Control

Summary

Provide the names of the attributes that will be carried in (or referenced by) the OAuth access token. For auditing purposes, an attribute may be chosen as the subject.

Subject Attribute Name

USER_KEY

Extend the Contract	Multi-Valued
uid	<input type="checkbox"/>
username	<input type="checkbox"/>
	<input type="checkbox"/>

4. Create OpenID connect Policy Management Instance

OpenID Connect Policy Management | Policy

- Manage Policy
- Attribute Contract
- Attribute Scopes
- Attribute Sources & User Lookup
- Contract Fulfillment
- Issuance Criteria
- Summary

Enter a Policy ID and Name. You may also change general settings for the ID Token.

POLICY ID	pa_OIDC		
NAME	<input type="text" value="pa_OIDC"/>		
ACCESS TOKEN MANAGER	<div>Access Token for PingAccess</div>		
ID TOKEN LIFETIME	<input type="text" value="5"/>	minutes	
INCLUDE SESSION IDENTIFIER IN ID TOKEN	<input type="checkbox"/>		
INCLUDE USER INFO IN ID TOKEN	<input type="checkbox"/>		
INCLUDE STATE HASH IN ID TOKEN	<input type="checkbox"/>		
INCLUDE X.509 THUMBPRINT HEADER IN ID TOKEN ?	<input type="checkbox"/>		
ID TOKEN TYPE (TYP) HEADER VALUE	<input type="text"/>		
RETURN ID TOKEN ON REFRESH GRANT	<input type="checkbox"/>		
REISSUE ID TOKEN IN HYBRID FLOW	<input type="checkbox"/>		
<div>Manage Access Token Managers</div>			

OpenID Connect Policy Management | Policy

- Manage Policy
- Attribute Contract
- Attribute Scopes
- Attribute Sources & User Lookup
- Contract Fulfillment
- Issuance Criteria
- Summary

The required Attribute Contract consists of a user identifier (sub). You may extend the contract to include additional attributes that will be returned to OAuth clients. The preset extended-contract list contains OpenID Connect attributes that are delivered to OAuth clients if INCLUDE USER INFO IN ID TOKEN is not enabled in the previous step. If the client doesn't receive an OAuth access token, which is required to access the UserInfo endpoint, all attributes

Attribute Contract				
sub				
Extend the Contract	Override Default Delivery	ID Token	UserInfo	Multi-Valued ?
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OpenID Connect Policy Management | Policy

Manage Policy	Attribute Contract	Attribute Scopes	Attribute Sources & User Lookup	Contract Fulfillment	Issuance Criteria	Summary
---------------	--------------------	------------------	---------------------------------	----------------------	-------------------	---------

Fulfill the Attribute Contract with values from the Access Token or from other sources listed.

Attribute Contract	Source	Value ?
sub	Access Token ▼	uid ▼

5. Create Access Token Mapping

- Goto Applications > Access Token Mappings
- Click on the dropdown list for context and select **IdPAdapter:PAHTMLAdapter**
- Click on the dropdown list for Access Token Manager and select **Access Token for PingAccess**
- Click Add Mapping

Access Token Mappings	
Manage the attribute mapping(s) used to fulfill the access token attribute contracts. This configuration maps from a persistent grant or other sources into the access token attribute contract. For mappings each access token manager. The default can be overridden based on the context of the authentication event of the original grant.	
Context	Access Token Manager
Authentication Policy Contract: API OAuth Policy Contract	Access Token Manager
Authentication Policy Contract: OAuth Policy Contract	Access Token Manager
Client Credentials	Access Token for PingAccess
IdP Adapter: PAHTMLAdapter	Access Token for PingAccess

6. Create an authorization code grant type client

Clients | Client

Manage the configuration and policy information about a client.

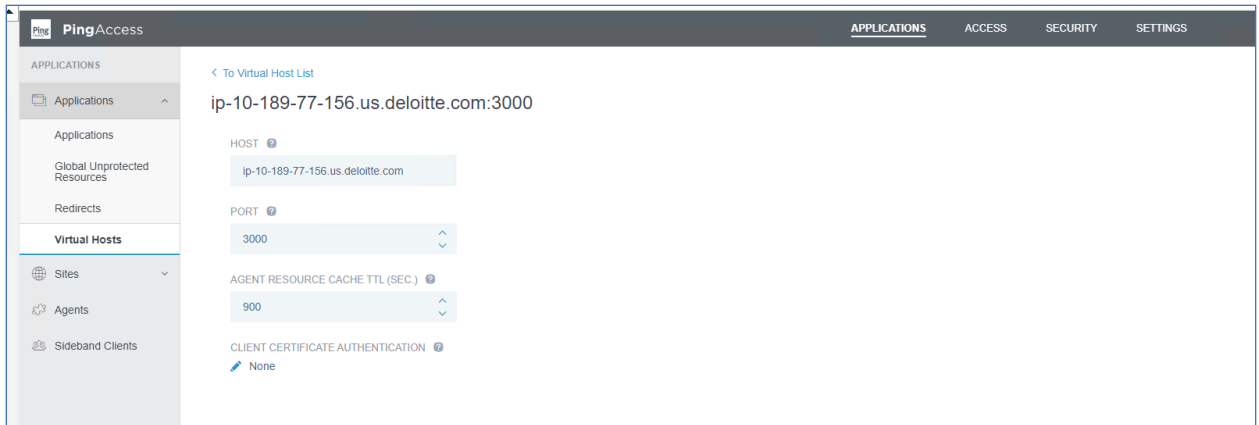
CLIENT ID	pa_wam
NAME	<div>PingAccess Web Manag</div>
DESCRIPTION	<div></div>
CLIENT AUTHENTICATION	<div><div><input type="radio"/></div> NONE</div> <div><div><input checked="" type="radio"/></div> CLIENT SECRET</div> <div><div><input type="radio"/></div> CLIENT SECRET JWT</div> <div><div><input type="radio"/></div> CLIENT TLS CERTIFICATE</div> <div><div><input type="radio"/></div> PRIVATE KEY JWT</div>

JWKS	<div></div>	
REDIRECT URIS	Redirection URIs <div>https://10.189.77.156:3000/pa/oidc/cb</div> <div></div> <div>Add</div>	Action Edit Delete
LOGO URL	<div></div>	
ALLOW AUTHENTICATION API REDIRECTLESS MODE	<input type="checkbox"/> Allow	
BYPASS AUTHORIZATION APPROVAL	<input checked="" type="checkbox"/> Bypass	
RESTRICT COMMON SCOPES	<input type="checkbox"/> Restrict	
EXCLUSIVE SCOPES	<input type="checkbox"/> Allow Exclusive Scopes	
AUTHORIZATION DETAIL TYPES	<input type="checkbox"/> Allow Authorization Details	
ALLOWED GRANT TYPES	<input checked="" type="checkbox"/> Authorization Code <input type="checkbox"/> Implicit <input type="checkbox"/> Refresh Token <input type="checkbox"/> Client Credentials <input type="checkbox"/> Device Authorization Grant <input type="checkbox"/> CIBA <input type="checkbox"/> Token Exchange <input type="checkbox"/> Resource Owner Password Credentials <input type="checkbox"/> Assertion Grants <input type="checkbox"/> Access Token Validation (Client is a Resource Server)	
RESTRICT RESPONSE TYPES	<input type="checkbox"/> Restrict	
DEFAULT ACCESS TOKEN MANAGER	<div>Access Token for PingAccess</div>	
RESTRICT TO DEFAULT ACCESS TOKEN MANAGER	<input type="checkbox"/> Restrict	
VALIDATE AGAINST ALL ELIGIBLE ACCESS TOKEN MANAGERS	<input type="checkbox"/>	
REQUIRE PROOF KEY FOR CODE EXCHANGE (PKCE)	<input type="checkbox"/>	
PERSISTENT GRANTS MAX LIFETIME	<input checked="" type="radio"/> Use Global Setting <input type="radio"/> Grants Do Not Expire	

2. PingAccess configuration for protected web app

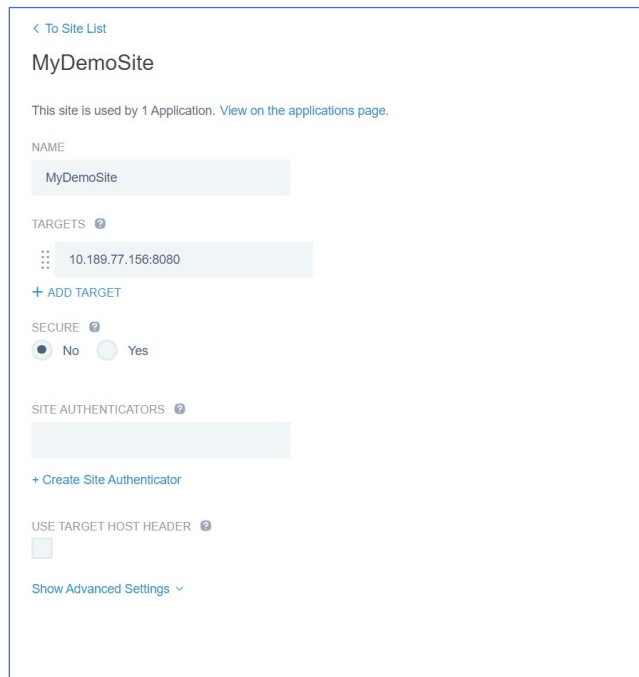
1. Virtual Host

- Goto Applications > Virtual Hosts
- In the host field, enter the public facing domain name of the web application, in this case it is PingAccess Hostname
- In the port field, enter the port number of the public facing domain name, , in this case it is PingAccess runtime port



2. Site

- Goto Applications > Sites
- In the name field enter the domain name
- In the target field, enter the target server webserver
- Select a Trusted Certificate Group



Hide Advanced Settings ^

SKIP HOSTNAME VERIFICATION ⓘ
☒

EXPECTED CERTIFICATE HOSTNAME ⓘ

AVAILABILITY PROFILE ⓘ
Default Availability Profile ▾
[Edit](#)

LOAD BALANCING STRATEGY ⓘ
None

SEND TOKEN ⓘ
☐

MAXIMUM CONNECTIONS ⓘ
-1 ▴ ▾

MAXIMUM WEBSOCKET CONNECTIONS ⓘ
-1 ▴ ▾

USE PROXY ⓘ
☐

KEEP ALIVE TIMEOUT ⓘ

3. Web Sessions

- a. Goto Access > Web Sessions
- b. In the Cookies Type list, select Encrypted JWT or Signed JWT
- c. In Audience field, enter the audience field to which PA token is applicable
- d. In the OpenID Connect Login Type select **Code**

[← To Web Session List](#)

PingAccess Web Management

NAME
PingAccess Web Management

COOKIE TYPE ⓘ
Encrypted JWT

AUDIENCE ⓘ
WebSession

OPENID CONNECT LOGIN TYPE ⓘ
Code

CLIENT ID ⓘ
pa_wam

CLIENT CREDENTIALS TYPE ⓘ
☒ Secret ☐ Mutual TLS ☐ Private Key JWT

CLIENT SECRET ⓘ

IDLE TIMEOUT (M) ⓘ
60

MAX TIMEOUT (M) ⓘ
240

[Hide Advanced Settings](#)

4. Applications

Go to Applications

In Context root, enter the common root of all web session endpoints

In the virtual host, select the virtual host

For application type select web

In the Web Session List, select a websession for the application

TomcatApp
10.189.77.156:3000

Properties	Resources	Web Policy
------------	-----------	------------

VIRTUAL HOSTS:	10.189.77.156:3000
CONTEXT ROOT:	/
DESTINATION:	Site
SITE:	MyDemoSite
WEB SESSION:	PingAccess Web Management
WEB IDENTITY MAPPING:	DemoidentityMapping
AUTHENTICATION CHALLENGE POLICY:	None
RISK POLICY:	None
SPA SUPPORT ENABLED:	true