PingAccess Lab Guide

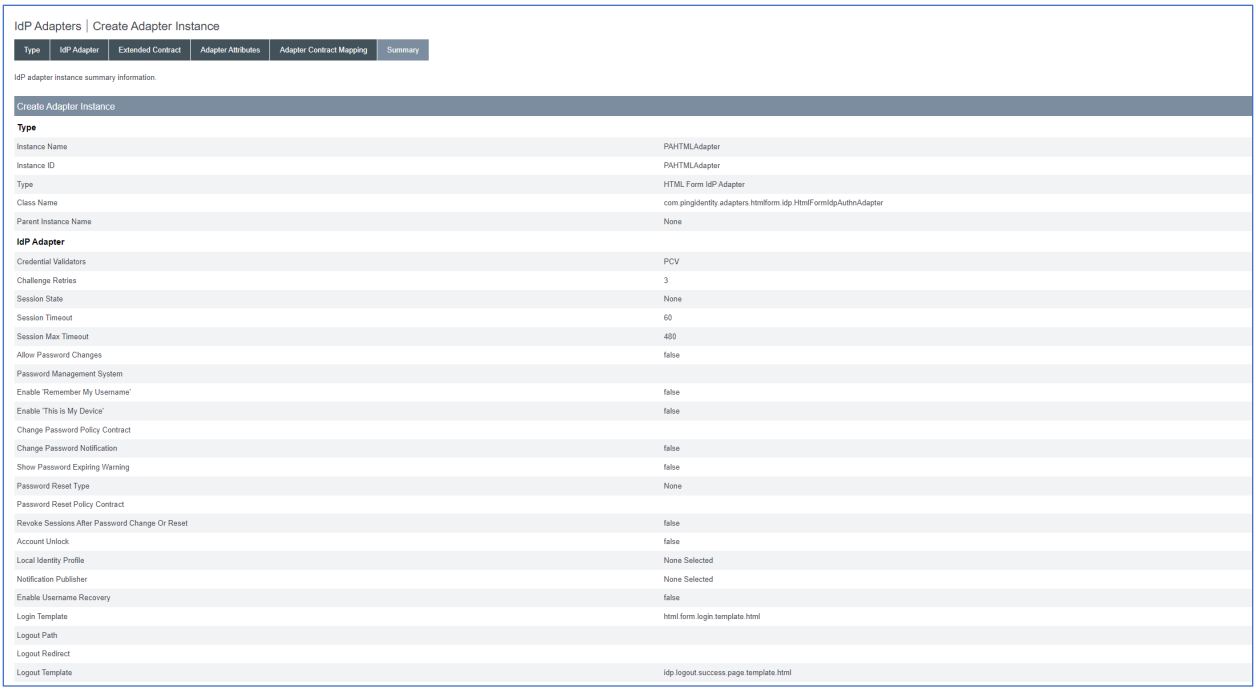
Protect WebApp using PingAccess

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

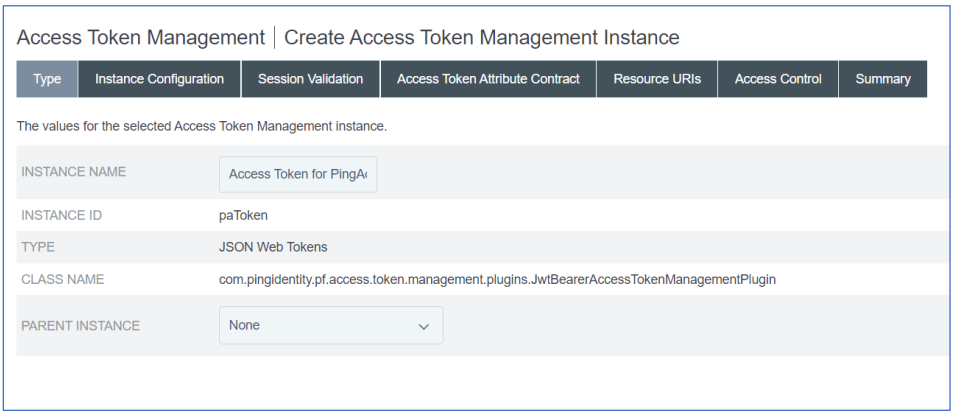
1. PingFederate configuration for protected web app

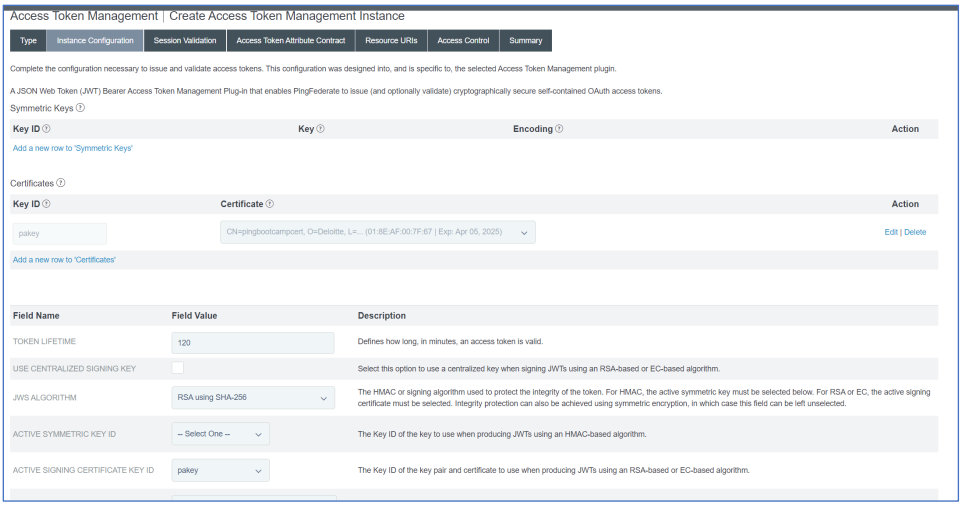
1. Create a Simple Username Password Credential Validator
   Goto System > Password Credential Validator > Create New Instance

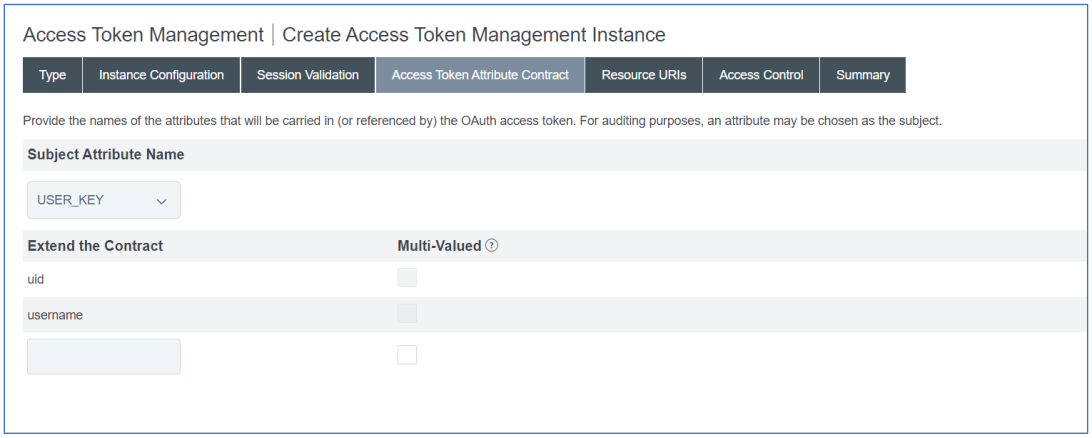
2. Create an IdP Adapter and attach this newly created PCV to the adapter
   Goto Authentication > IdP Adapters > Create New Instance
   In this lab a new IdP HTML adapter **PAHTMLAdapter** is created



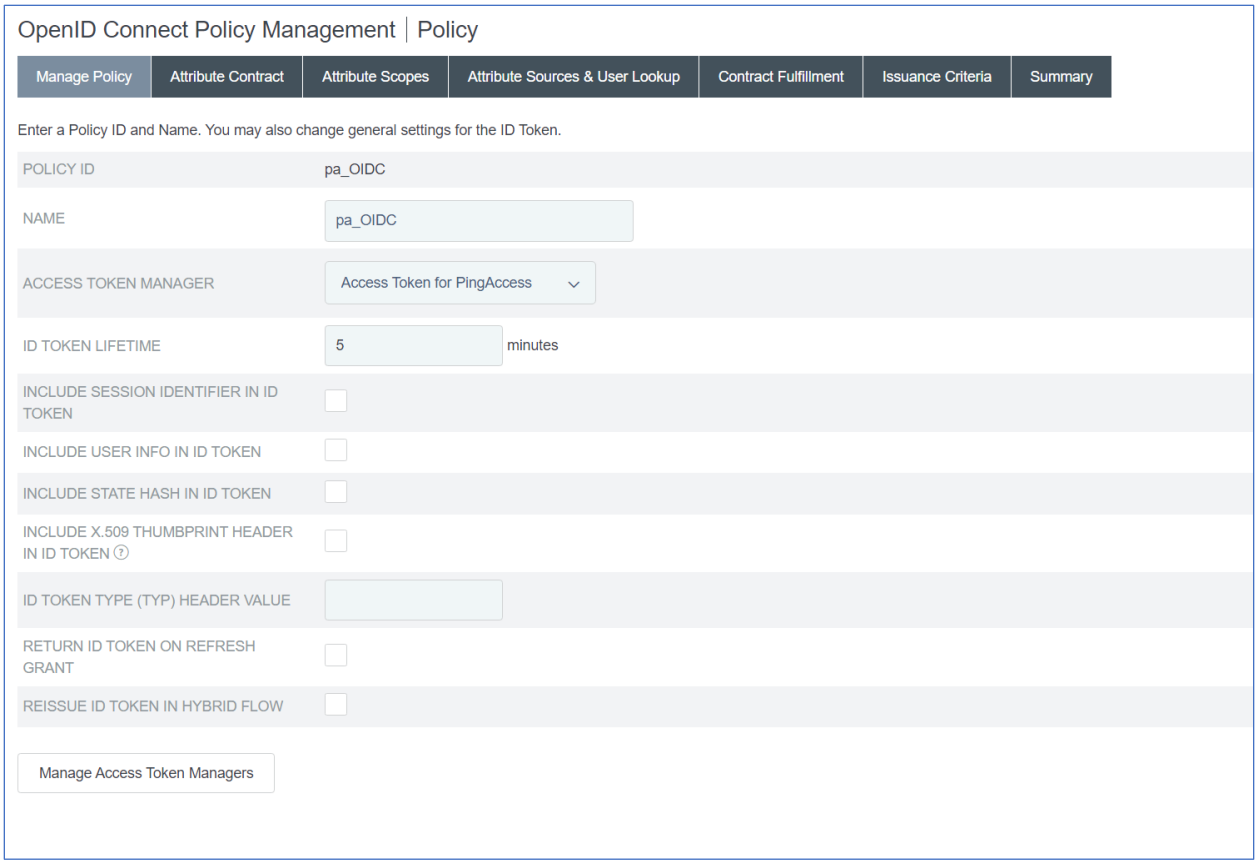
3. Create Access Token Management Instance

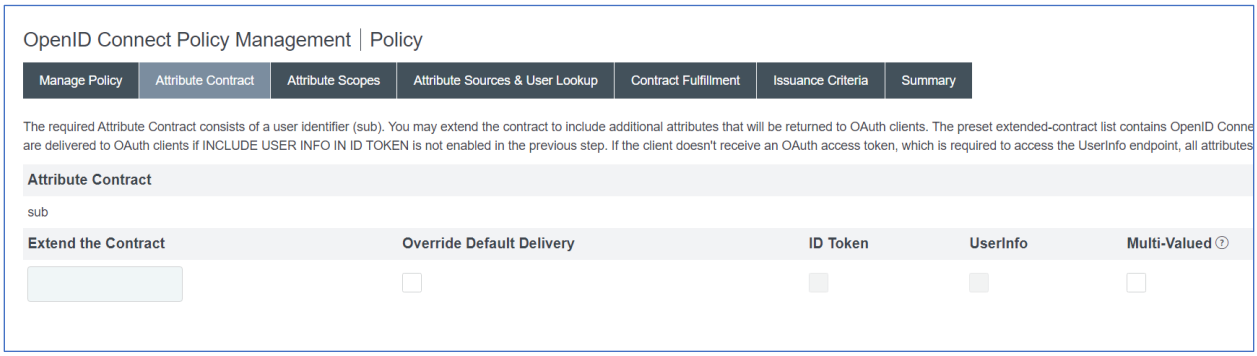


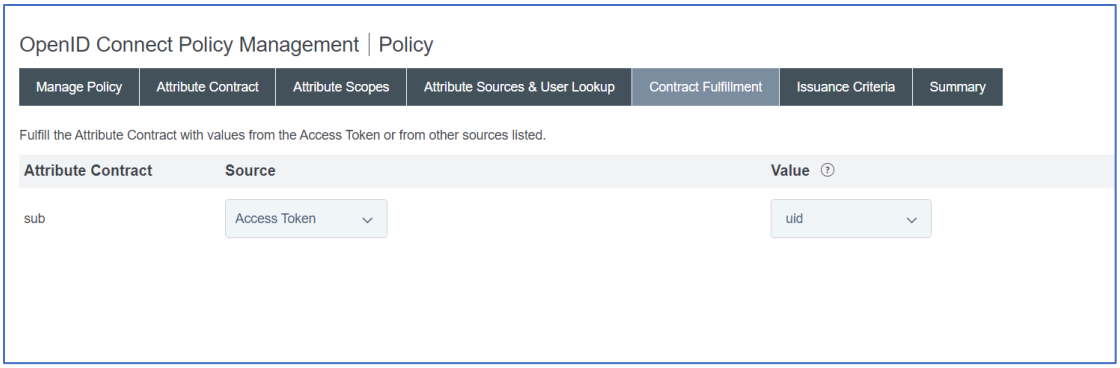




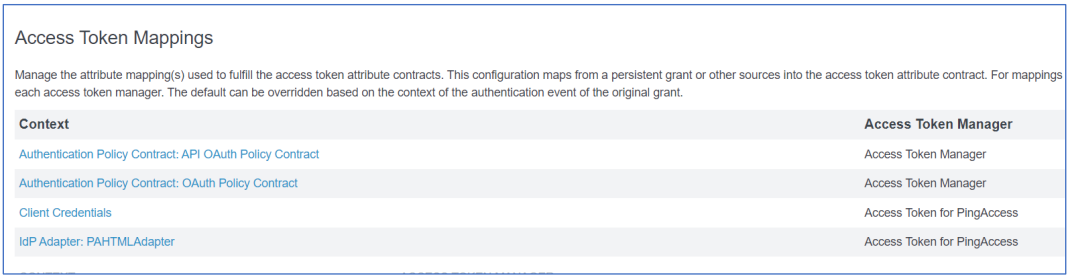
4. Create OpenID connect Policy Management Instance


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
pa_OIDC
ACCESS TOKEN MANAGER
Access Token for PingAccess
ID TOKEN LIFETIME
5
minutes
INCLUDE SESSION IDENTIFIER IN ID TOKEN
INCLUDE USER INFO IN ID TOKEN
INCLUDE STATE HASH IN ID TOKEN
INCLUDE X.509 THUMBPRINT HEADER IN ID TOKEN
ID TOKEN TYPE (TYP) HEADER VALUE
RETURN ID TOKEN ON REFRESH GRANT
REISSUE ID TOKEN IN HYBRID FLOW
Manage Access Token Managers

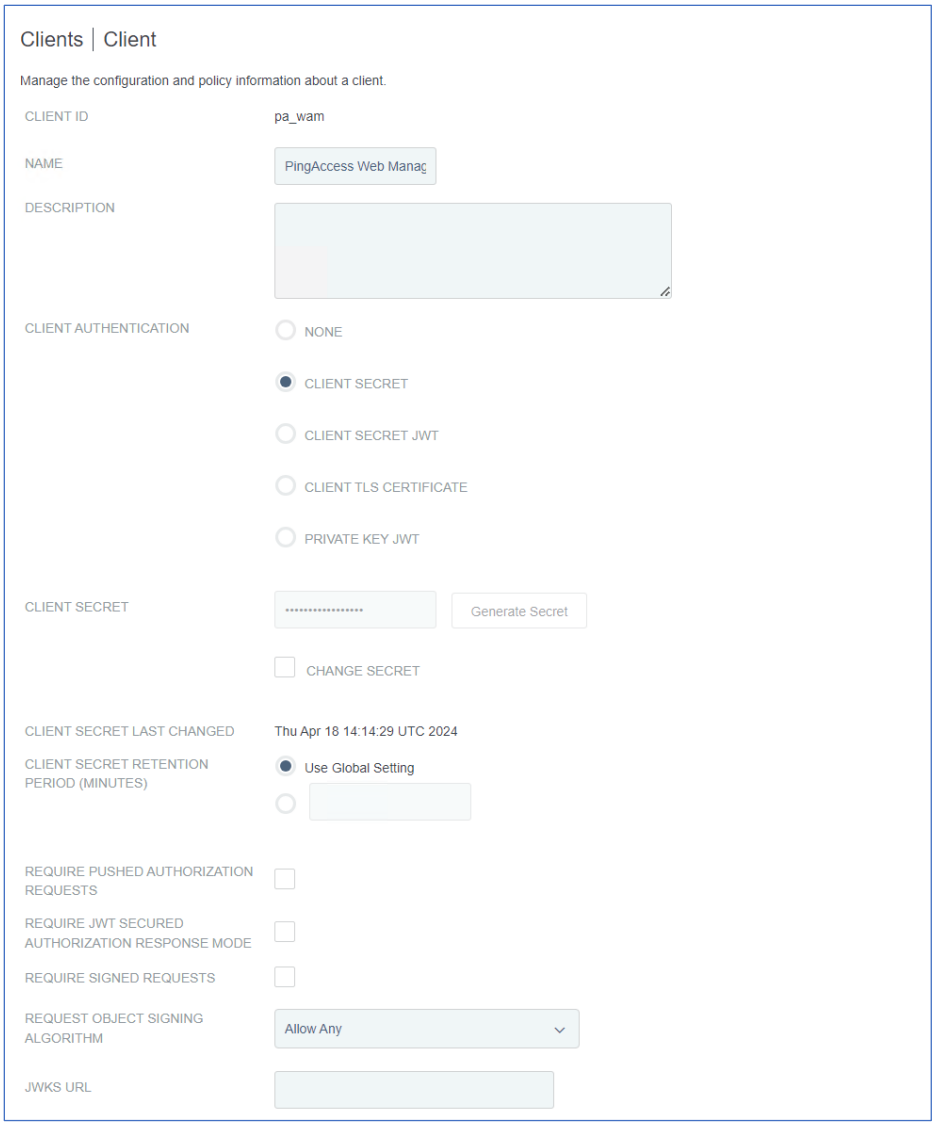

OpenID Connect Policy Management | Policy
Manage Policy
Attribute Contract
Attribute Scopes
Attribute Sources & User Lookup
Contract Fulfillment
Issuance Criteria
Summary
The required Attribute Contract consists of a user identifier (sub). You may extend the contract to include additional attributes that will be returned to OAuth clients. The preset extended-contract list contains OpenID Conne
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

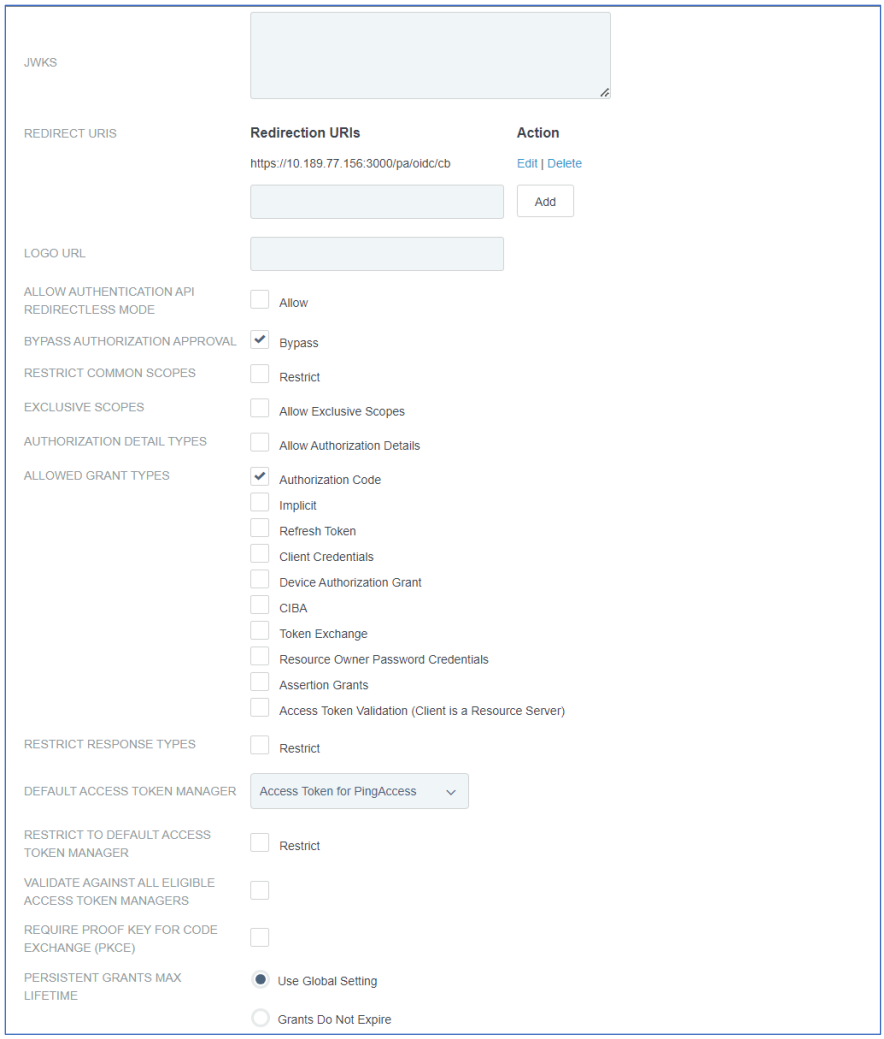


5. Create Access Token Mapping
   a. Goto Applications > Access Token Mappings
   b. Click on the dropdown list for contect and select **IdPAdapter:PAHTMLAdapter**
   c. Click on the dropdown list for Access Token Manager and select **Access Token for PingAccess**
   d. Click Add Mapping



6. Create an authorization code grant type client

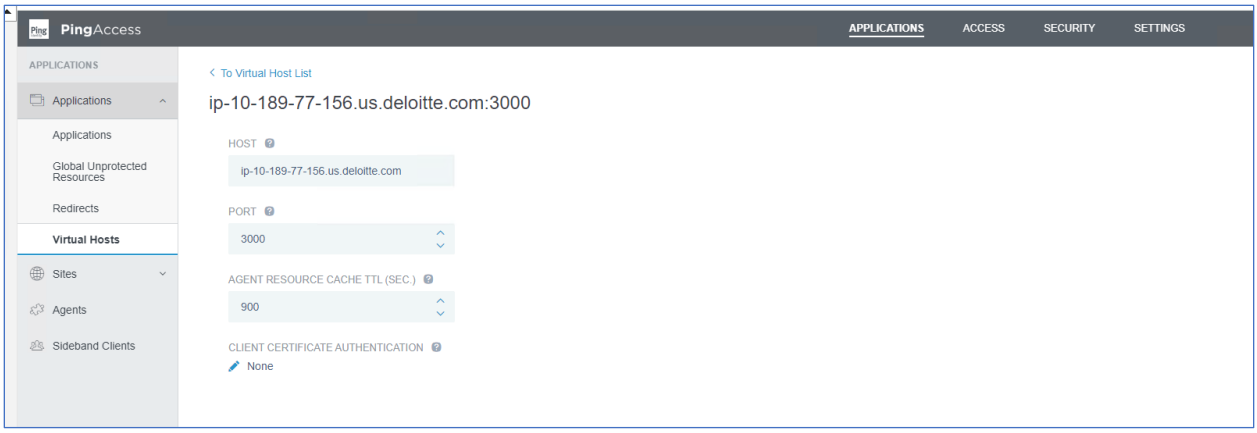

Clients | Client
Manage the configuration and policy information about a client.
CLIENT ID
pa_wam
NAME
PingAccess Web Manag
DESCRIPTION
CLIENT AUTHENTICATION
NONE
CLIENT SECRET
CLIENT SECRET JWT
CLIENT TLS CERTIFICATE
PRIVATE KEY JWT
CLIENT SECRET
Generate Secret
CHANGE SECRET
CLIENT SECRET LAST CHANGED
Thu Apr 18 14:14:29 UTC 2024
CLIENT SECRET RETENTION PERIOD (MINUTES)
Use Global Setting
REQUIRE PUSHED AUTHORIZATION REQUESTS
REQUIRE JWT SECURED AUTHORIZATION RESPONSE MODE
REQUIRE SIGNED REQUESTS
REQUEST OBJECT SIGNING ALGORITHM
Allow Any
JWKS URL



2. PingAcces configuration for protected web app

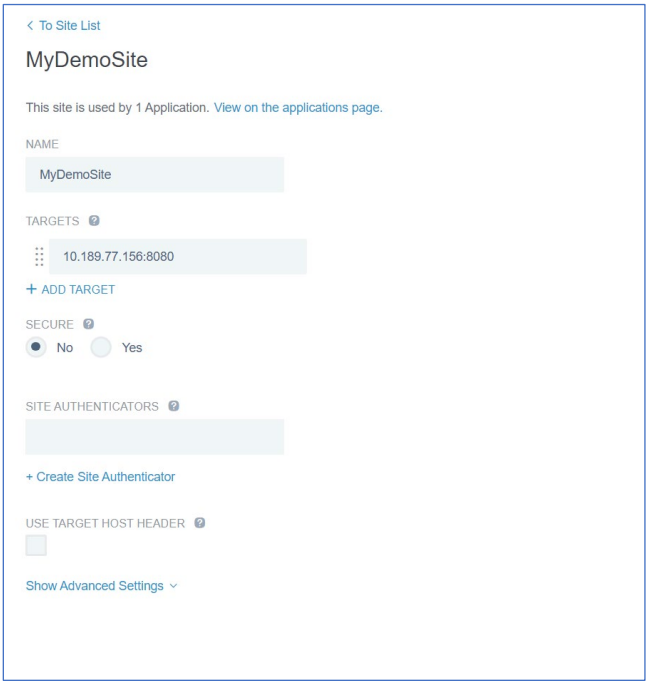
1. Virtual Host

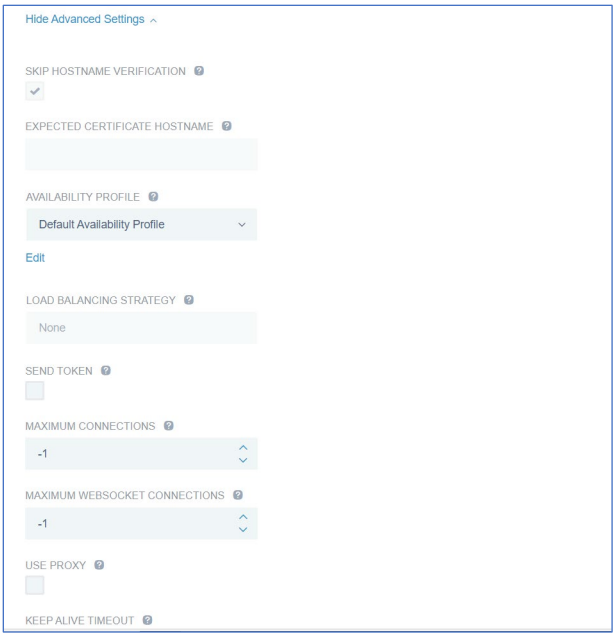
a. Goto Applications > Virtual Hosts
b. In the host field, enter the public facing domain name of the web application, in this case it is PingAccess Hostname
c. In the port field, enter the port number of the public facing domain name, , in this case it is PingAccess runtime port



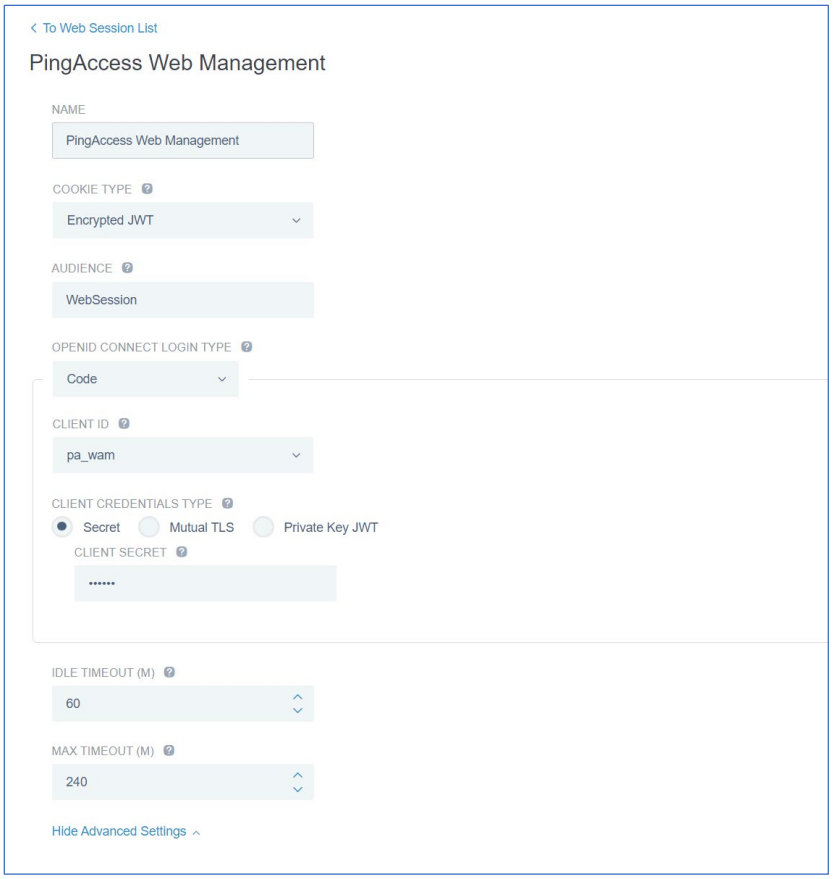
2. Site

a. Goto Applications > Sites
b. In the name field enter the domain name
c. In the target field, enter the target server webserver
d. Select a Trusted Certificate Group





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**



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