



EBS Integration Kit Version 2.2.0.x

Deployment Guide – Deploying the EIK in the PingFederate Server
Doc version 1.1

Change Log

Date	Type	Description
13/04/2022	Supported PingFederate Version	EIK 2.2.0.12 now supports PingFederate 11.0.2
07/06/2022	Pre-requisites and EIK configuration parameters	Importing PingFederate's SSL cert into the Java Keystore + EBS landing page format

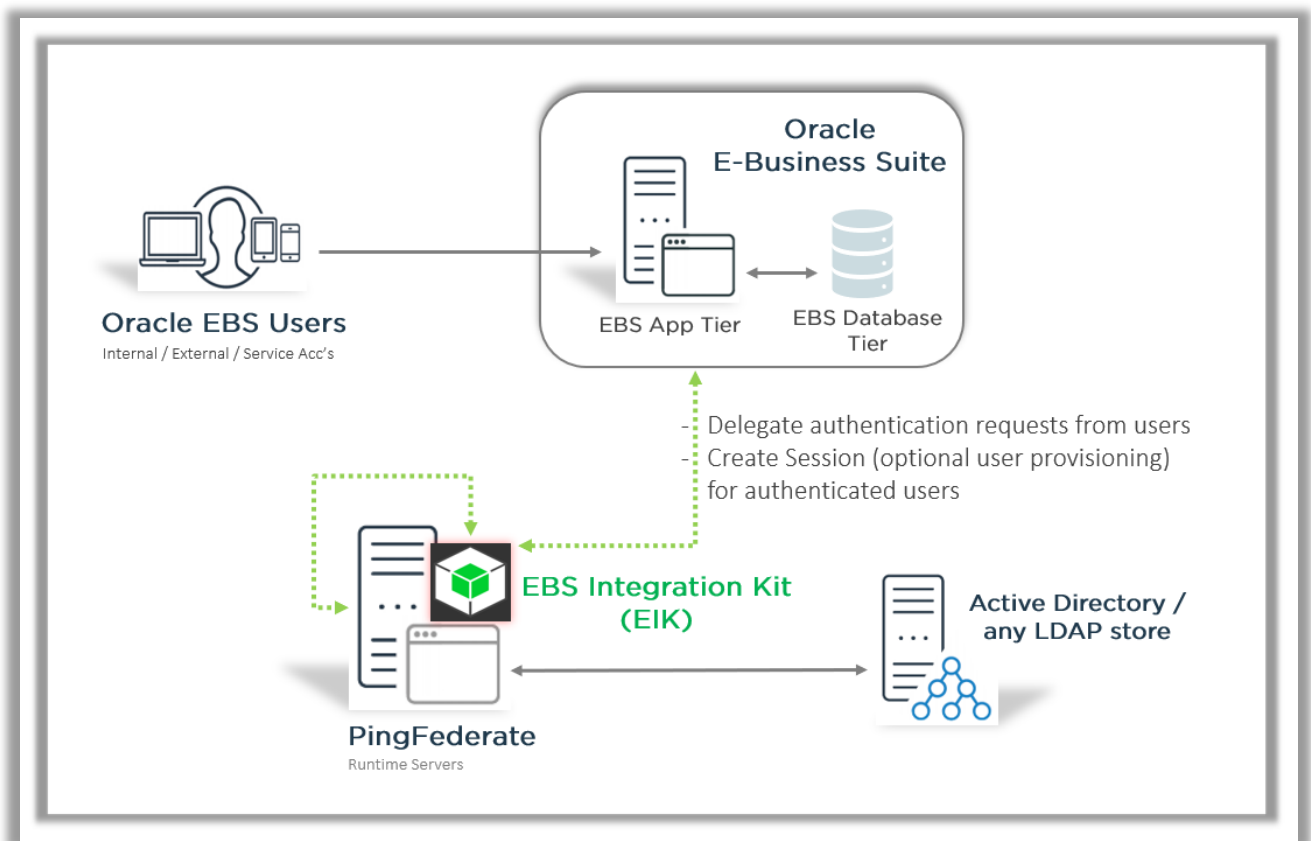
Contents

1. EBS INTEGRATION KIT DESCRIPTION	4
2. FEATURES.....	5
3. BENEFITS	5
4. SYSTEM REQUIREMENTS	5
5. OVERVIEW OF THE FLOW	6
6. DEPLOYMENT AND CONFIGURATION OF PINGFEDERATE	6
6.1 Basic Configurations in Pingfederate for EIK	6
6.1.1 Configure HTML Form Adapter	6
6.1.2 OAuth Server side Configuration.....	8
6.2 Configure SSL Server certificate.....	19
6.2.1 Importing the SSL Certificate into the Java Key Store.....	19
7. EIK Deployment in PingFederate.....	21
7.1 EIKAuth Config File Generation.....	22
7.2 EBS DataSource (DBCX) File Creation	23
7.3 Deploying the log4j2.xml File.....	25
7.4 Deploying EBSAuth.war File	25
8. System Profile Parameter changes in EBS.....	26
8.1 System Profile Changes	26
9. SSO Testing for Oracle EBS.....	27

1. EBS INTEGRATION KIT DESCRIPTION

PingFederate as an Identity Federation product includes adapters and integration kits that simplify integrations with Identity Stores as well as Applications. The Oracle EBS solution uses these capabilities to enable Single Sign-On. The EBS INTEGRATION KIT (EIK) from LikeMinds Consulting provides a simple deployment path with PingFederate to enable single sign-on (SSO) to Oracle E-Business Suite.

How does the EBS Integration Kit work?



The EBS Integration Kit is a light-weight java application which can be deployed in the PingFederate jetty-container which eliminates the need for dedicated server/hardware. The EIK is OpenID Connect Compliant as a resource server and can be configured with PingFederate to receive Authentication and Authorization tokens. The EBS Integration Kit communicates with the Oracle E-Business Suite Database for Session creation and optional user-provisioning if required.

2. FEATURES

- Works seamlessly with PingFederate
- Eliminated the need for additional Oracle components like Oracle Internet Directory or EBS AccessGate
- Provides flexibility of Deployment Methods: The EIK can be installed on the PingFederate server or any other J2EE container
- Supports Just-In-Time provisioning

3. BENEFITS

- Helps achieve painless integration of modern IAM into your existing architecture
- Enables you to modernize or migrate off legacy IAM without disrupting critical access to Oracle E-Business Suite
- Frees you from vendor lock-in with legacy IAM licensing—you will only require your EBS license
- Requires no provisioning of additional hardware components

4. SYSTEM REQUIREMENTS

- Java JDK 1.8 (Recommended Version)
- PingFederate 8 and above
- EBS IKT package with a valid license file.

EBS Integration Kit	Oracle E-Business Suite	Oracle Database	PingFederate	PingAccess (optional)
EIK 2.2.0.12	Releases with update packs 12.0.x to 12.1.x & 12.2 to 12.2.10	From 11g up to 19c release	PingFederate versions 8.x to 11.2	PingAccess versions 4.x to 7.0.x

5. OVERVIEW OF THE FLOW

1. When a user tries to login, his/her credentials are sent to Pingfederate.
2. Pingfederate validates the entered credentials against the configured Authentication Store (i.e., any LDAP directory).
3. The existence of the authenticated user will be checked against the EBS Database. If the user does exist in the EBS DB, an EBS session would be created, and the user would be allowed access to the requested page in EBS.
4. If the authenticated user does not exist in the EBS DB, the user would not be authorized to access the EBS Application.
5. If Just-In-Time Provisioning is enabled, authenticated users not present in the EBS DB would be provisioned by the EBS IKT, and EBS Sessions would then be created, thereby giving access to the EBS Application.

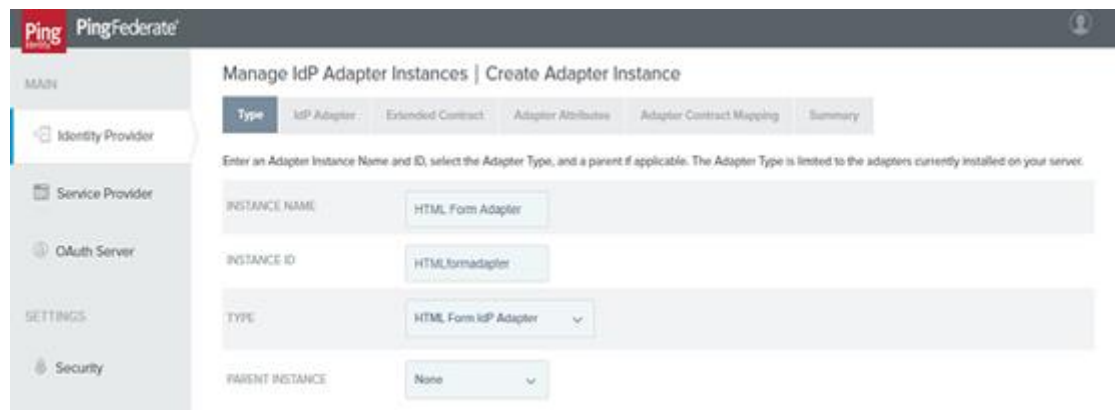
6. DEPLOYMENT AND CONFIGURATION OF PINGFEDERATE

PingFederate is a federation server that provides web single sign-on and API security for the resources in your Organization.

6.1 Basic Configurations in Pingfederate for EIK

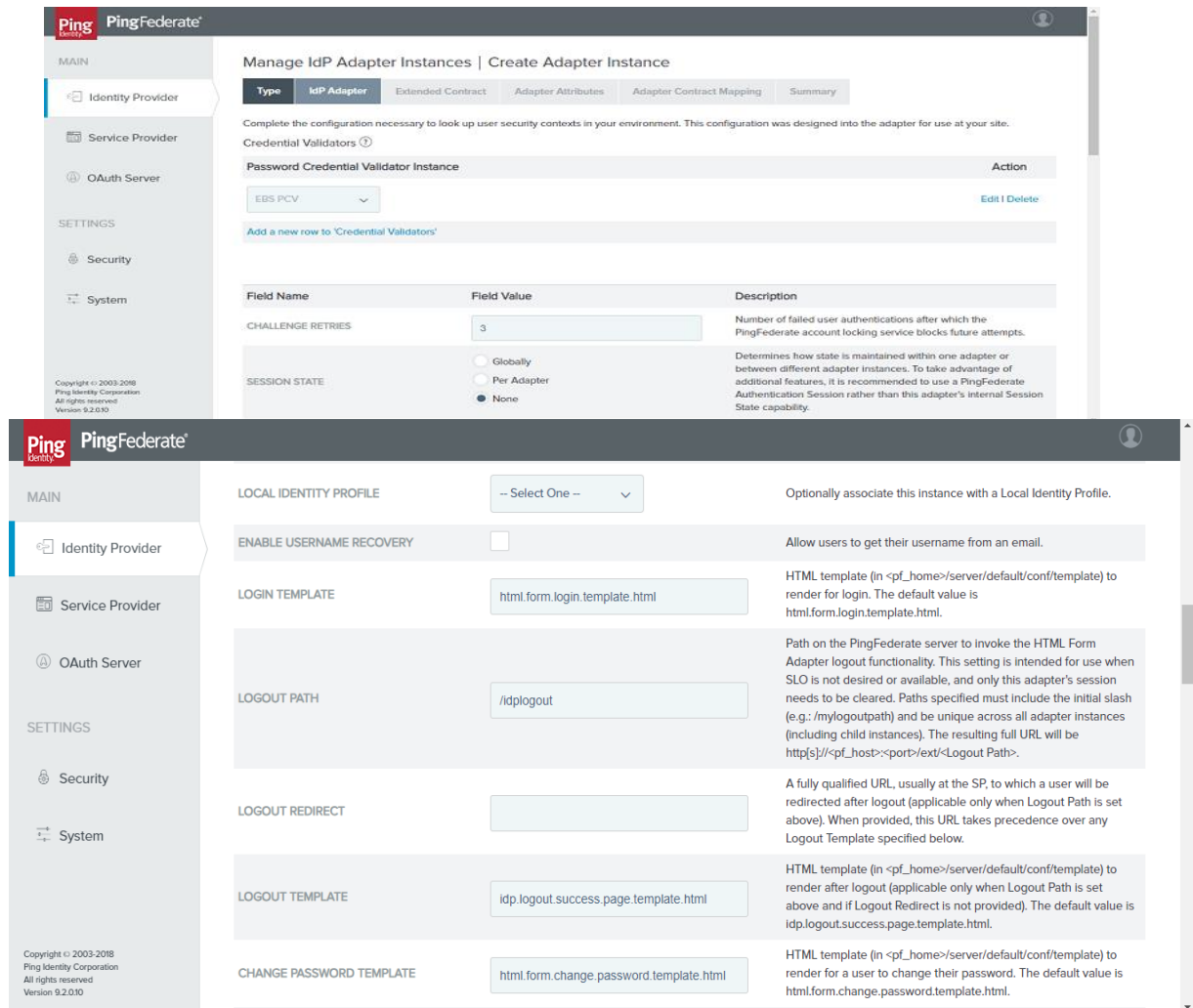
6.1.1 Configure HTML Form Adapter

1. In PingFederate console go to Identity Provider >> Adapters>>Click New Adapter
2. Provide the Instance Name & ID then Select “Type” as “HTML Form IdP Adapter” and click Next.



The screenshot shows the PingFederate console interface. On the left is a navigation menu with options: MAIN, Identity Provider, Service Provider, OAuth Server, SETTINGS, and Security. The main content area is titled 'Manage IdP Adapter Instances | Create Adapter Instance'. It features a tabbed interface with 'Type' selected. Below the tabs, there is a text prompt: 'Enter an Adapter Instance Name and ID, select the Adapter Type, and a parent if applicable. The Adapter Type is limited to the adapters currently installed on your server.' The form contains four fields: 'INSTANCE NAME' with the value 'HTML Form Adapter', 'INSTANCE ID' with the value 'HTMLformadapter', 'TYPE' with a dropdown menu showing 'HTML Form IdP Adapter', and 'PARENT INSTANCE' with a dropdown menu showing 'None'.

3. In the Next page, Add the “Password Credentials Validator” and click “Show advanced field” to add “/idplogout” in Logout Path Text Field. Then Click Next.



PingFederate

Manage IdP Adapter Instances | Create Adapter Instance

Type: **IdP Adapter** | Extended Contract | Adapter Attributes | Adapter Contract Mapping | Summary

Complete the configuration necessary to look up user security contexts in your environment. This configuration was designed into the adapter for use at your site.

Credential Validators ⓘ

Password Credential Validator instance Action

EBS PCV Edit | Delete

Add a new row to 'Credential Validators'

Field Name	Field Value	Description
CHALLENGE RETRIES	3	Number of failed user authentications after which the PingFederate account locking service blocks future attempts.
SESSION STATE	<input type="radio"/> Globally <input type="radio"/> Per Adapter <input checked="" type="radio"/> None	Determines how state is maintained within one adapter or between different adapter instances. To take advantage of additional features, it is recommended to use a PingFederate Authentication Session rather than this adapter's internal Session State capability.

LOCAL IDENTITY PROFILE: -- Select One -- Optionally associate this instance with a Local Identity Profile.

ENABLE USERNAME RECOVERY: ☐ Allow users to get their username from an email.

LOGIN TEMPLATE: HTML template (in <pf_home>/server/default/conf/template) to render for login. The default value is html.form.login.template.html.

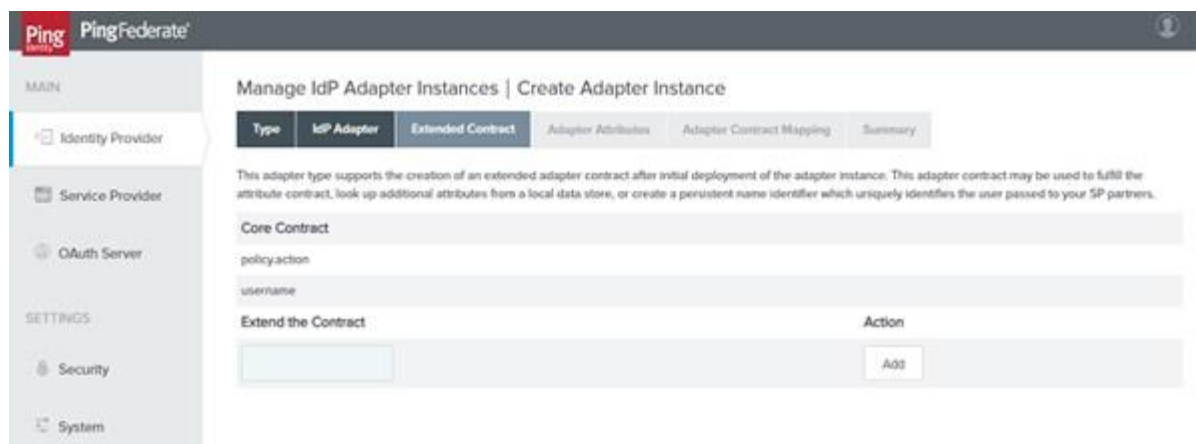
LOGOUT PATH: Path on the PingFederate server to invoke the HTML Form Adapter logout functionality. This setting is intended for use when SLO is not desired or available, and only this adapter's session needs to be cleared. Paths specified must include the initial slash (e.g.: /mylogoutpath) and be unique across all adapter instances (including child instances). The resulting full URL will be http[s]://<pf_host>:<port>/ext/<Logout Path>.

LOGOUT REDIRECT: A fully qualified URL, usually at the SP, to which a user will be redirected after logout (applicable only when Logout Path is set above). When provided, this URL takes precedence over any Logout Template specified below.

LOGOUT TEMPLATE: HTML template (in <pf_home>/server/default/conf/template) to render after logout (applicable only when Logout Path is set above and if Logout Redirect is not provided). The default value is idp.logout.success.page.template.html.

CHANGE PASSWORD TEMPLATE: HTML template (in <pf_home>/server/default/conf/template) to render for a user to change their password. The default value is html.form.change.password.template.html.

4. Add any additional attribute in Extended Contracts if required or leave the default values as such.



PingFederate

Manage IdP Adapter Instances | Create Adapter Instance

Type: **IdP Adapter** | **Extended Contract** | Adapter Attributes | Adapter Contract Mapping | Summary

This adapter type supports the creation of an extended adapter contract after initial deployment of the adapter instance. This adapter contract may be used to fulfill the attribute contract, look up additional attributes from a local data store, or create a persistent name identifier which uniquely identifies the user passed to your SP partners.

Core Contract

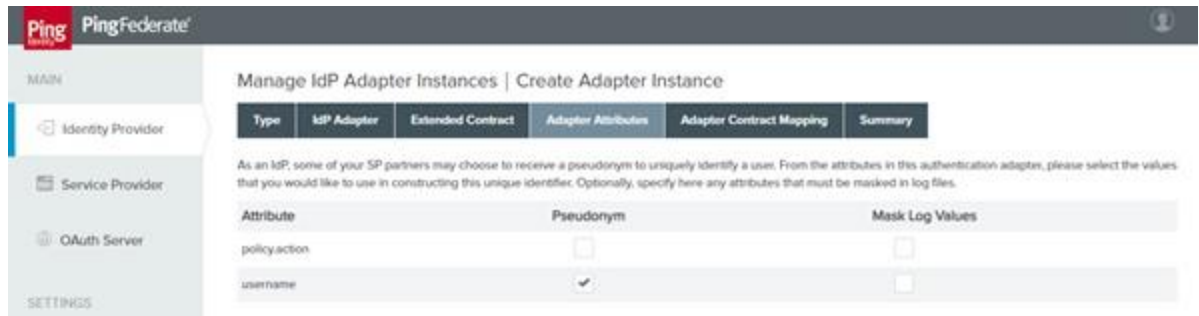
policy:action

username

Extend the Contract Action

Add

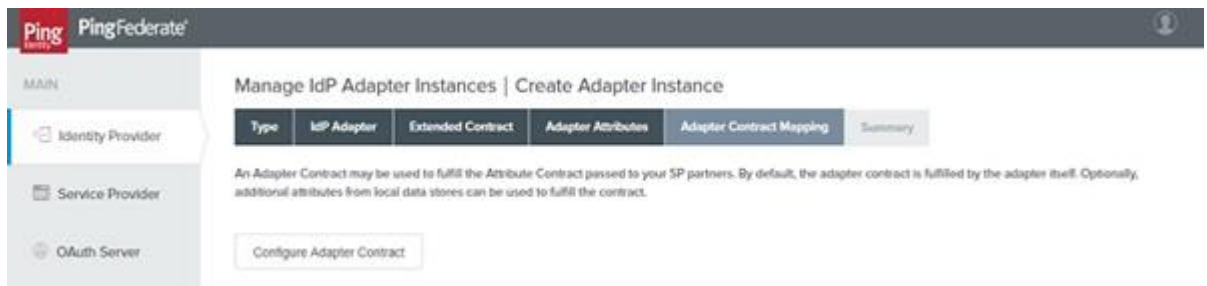
5. Enable “Pseudonym” for username (SP Partners may choose to receive so that they can uniquely identify a user) and click Next.



The screenshot shows the 'Adapter Attributes' tab in the PingFederate console. It displays a table with columns for 'Attribute', 'Pseudonym', and 'Mask Log Values'. The 'username' attribute has the 'Pseudonym' checkbox checked.

Attribute	Pseudonym	Mask Log Values
policyaction	<input type="checkbox"/>	<input type="checkbox"/>
username	<input checked="" type="checkbox"/>	<input type="checkbox"/>

6. Configure the Adapter Contract Mapping or leave it as default and click Next.



The screenshot shows the 'Adapter Contract Mapping' tab in the PingFederate console. It displays a button labeled 'Configure Adapter Contract'.

7. Review the Summary and Click Done and proceed to Save the adapter.

6.1.2 OAuth Server side Configuration

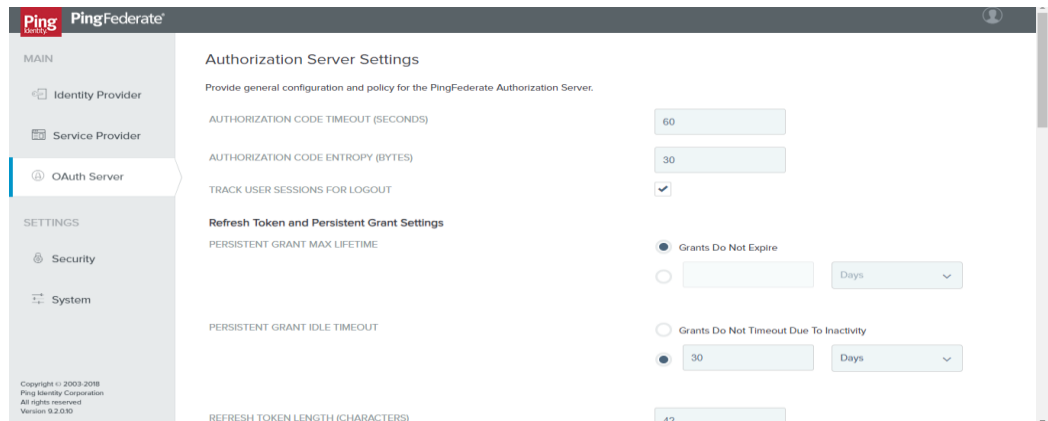
Configuring OAuth/OIDC flow PingFederate & EBS Integration Kit requires the following sections to be configured.

- Authorization server settings
- Scope Management
- IDP Adapter Mapping
- Access Token Management
- Access Token Mapping
- OpenID Connect Policy Management.
- Client Creation

6.1.2.1 Authorization Server Settings

Authorization Server Settings provide general configuration and policy for the PingFederate Authorization Server.

1. Go to OAuth Server >> Under Authorization Server >> Authorization Server Settings.
2. Enable the Track Users session for Log out checkbox and leave the remaining as default and click Save.



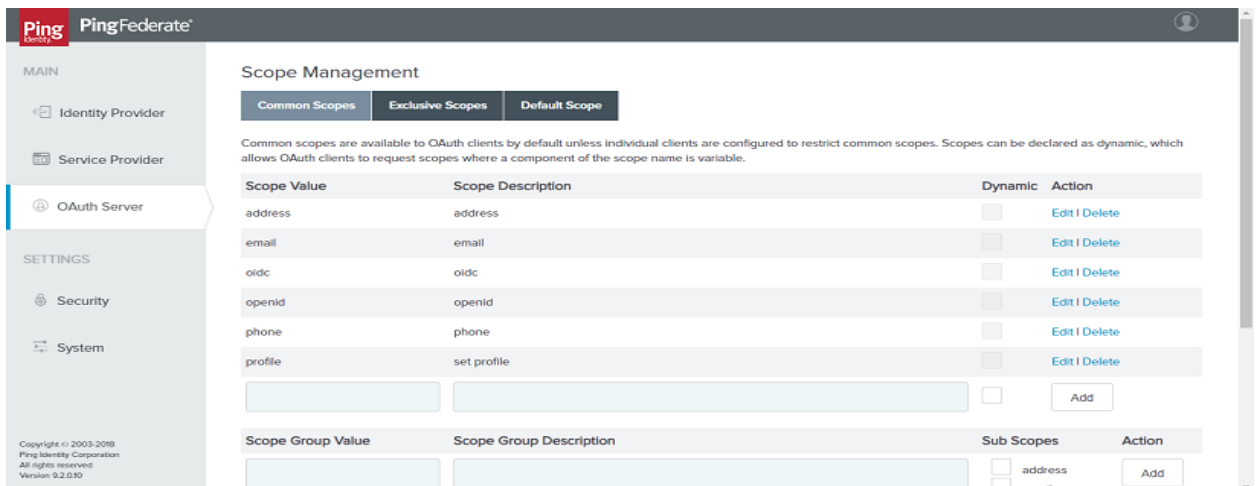
The screenshot shows the 'Authorization Server Settings' page in the PingFederate interface. The left sidebar has a 'MAIN' section with 'Identity Provider', 'Service Provider', and 'OAuth Server' (selected), and a 'SETTINGS' section with 'Security' and 'System'. The main content area is titled 'Authorization Server Settings' and includes a description: 'Provide general configuration and policy for the PingFederate Authorization Server.' The settings include:

- AUTHORIZATION CODE TIMEOUT (SECONDS): 60
- AUTHORIZATION CODE ENTROPY (BYTES): 30
- TRACK USER SESSIONS FOR LOGOUT: ☒
- Refresh Token and Persistent Grant Settings:
 - PERSISTENT GRANT MAX LIFETIME: ☒ Grants Do Not Expire
 - PERSISTENT GRANT IDLE TIMEOUT: ☐ Grants Do Not Timeout Due To Inactivity
- REFRESH TOKEN LENGTH (CHARACTERS): 42

6.1.2.2 Scope Management

Scopes can be declared as dynamic, which allows OAuth clients to request scopes where a component of the scope name is variable. Common scopes are available to OAuth clients by default unless individual clients are configured to restrict common scopes.

1. Go to OAuth Server >> Under Authorization Server >> Scope Management
2. These are the Default scopes for PingFederate
 - a) Email
 - b) Profile
 - c) Openid
 - d) Address
 - e) Phone



The screenshot shows the 'Scope Management' page in the PingFederate interface. The left sidebar is the same as the previous screenshot. The main content area is titled 'Scope Management' and has three tabs: 'Common Scopes', 'Exclusive Scopes', and 'Default Scope' (selected). Below the tabs is a description: 'Common scopes are available to OAuth clients by default unless individual clients are configured to restrict common scopes. Scopes can be declared as dynamic, which allows OAuth clients to request scopes where a component of the scope name is variable.' The table below lists the default scopes:

Scope Value	Scope Description	Dynamic	Action
address	address	<input type="checkbox"/>	Edit Delete
email	email	<input type="checkbox"/>	Edit Delete
oidc	oidc	<input type="checkbox"/>	Edit Delete
openid	openid	<input type="checkbox"/>	Edit Delete
phone	phone	<input type="checkbox"/>	Edit Delete
profile	set profile	<input type="checkbox"/>	Edit Delete

Below the table is a form to add a new scope:

Scope Value: Scope Description: Dynamic: ☐ Add:

Below that is a form to add a new scope group:

Scope Group Value: Scope Group Description: Sub Scopes: ☐ address ☐ email Add

6.1.2.3 IdP Adapter Mapping

This configuration allows you to map attributes based on an IdP adapter configuration into the USER_KEY and USER_NAME attributes (presented to the user for authorization permission) for a persistent grant, as well as the extended attributes.

1. Go to OAuth Server >> Authorization Server >> IdP Adapter Mapping and select HTML Form Adapter and click Add Mapping.
2. Add any Data Store details if values are pulled from a Data Store. If not, click Next.
3. In Contract Fulfillment, Map the USER_NAME & USER_KEY value from either the Adapter or Data Store.



PingFederate

IdP Adapter Mappings | IdP Adapter Mapping

Attribute Sources & User Lookup | **Contract Fulfillment** | Issuance Criteria | Summary

Select a Source and Value to map into each item in the Contract list.

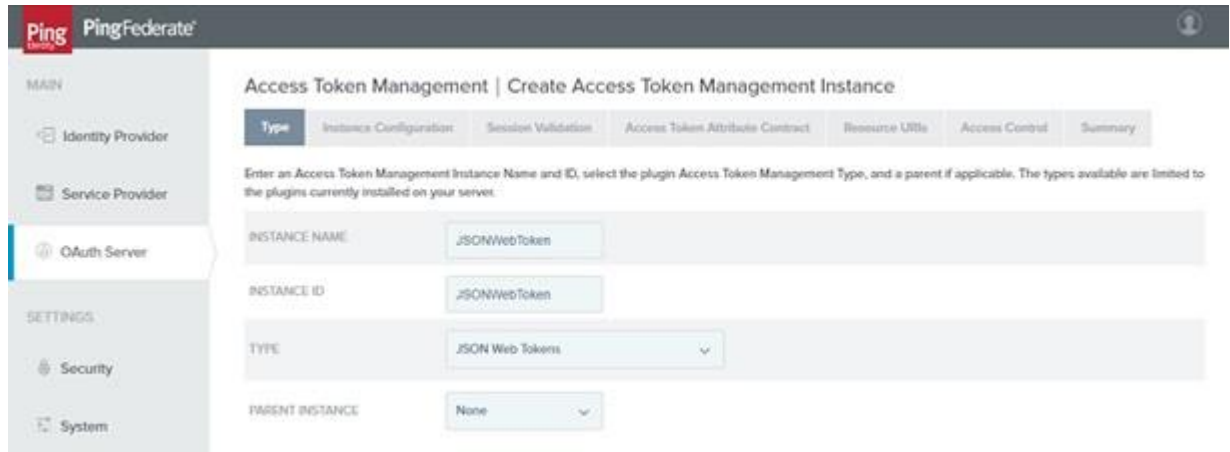
Contract	Source	Value	Actions
USER_KEY	Adapter	username	None available
USER_NAME	Adapter	username	None available

4. In the next page, provide any access restriction criteria details if the restriction of user access is required or click Next.
5. Review the Summary and then click Done and Save.

6.1.2.4 Access Token Management

PingFederate uses Access Token Management plugins to issue and validate OAuth access tokens. Each plugin instance can have its own token type, configuration settings, and attribute contract.

1. Go to OAuth Server >> Under Token Mapping >> Access Token Management >> Create New Instance by providing the Instance Name & ID, Type as “JSON Web Token” Click Next.



PingFederate

Access Token Management | Create Access Token Management Instance

Type Instance Configuration Session Validation Access Token Attribute Contract Resource URIs Access Control Summary

Enter an Access Token Management Instance Name and ID, select the plugin Access Token Management Type, and a parent if applicable. The types available are limited to the plugins currently installed on your server.

INSTANCE NAME: JSONWebToken

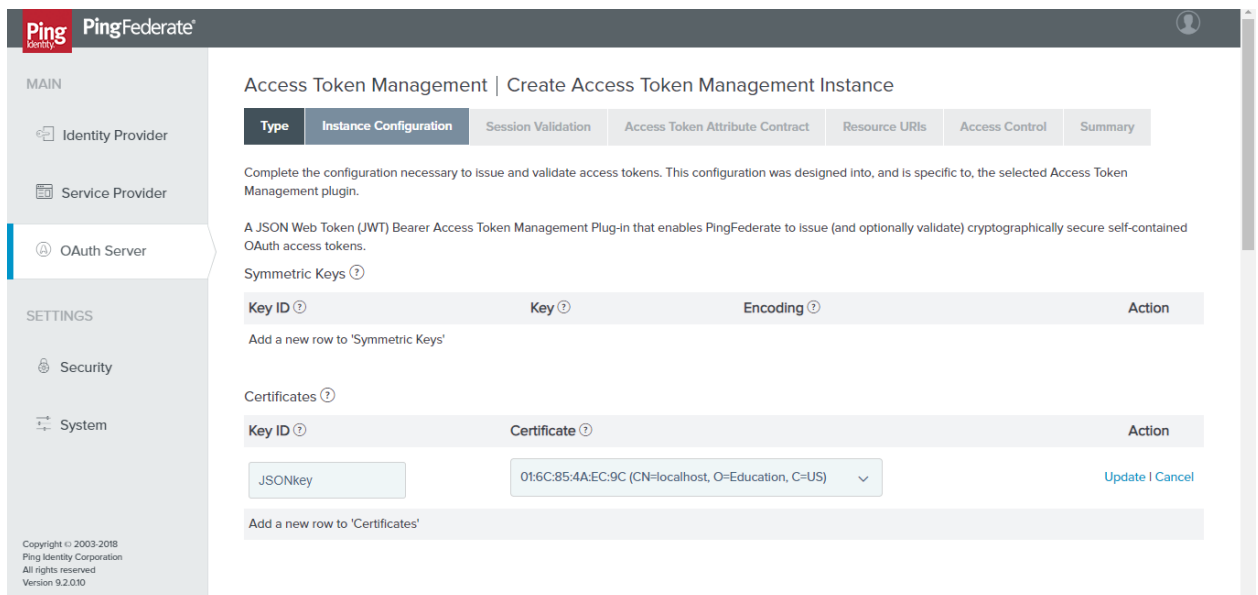
INSTANCE ID: JSONWebToken

TYPE: JSON Web Tokens

PARENT INSTANCE: None

2. In Instance Configuration Section, under Certificates, Add the Signing & Decryption certificate.

Note: When defining an access token management instance, you can customize various settings, including the token format, lifetime, and attribute contract for this instance.



PingFederate

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

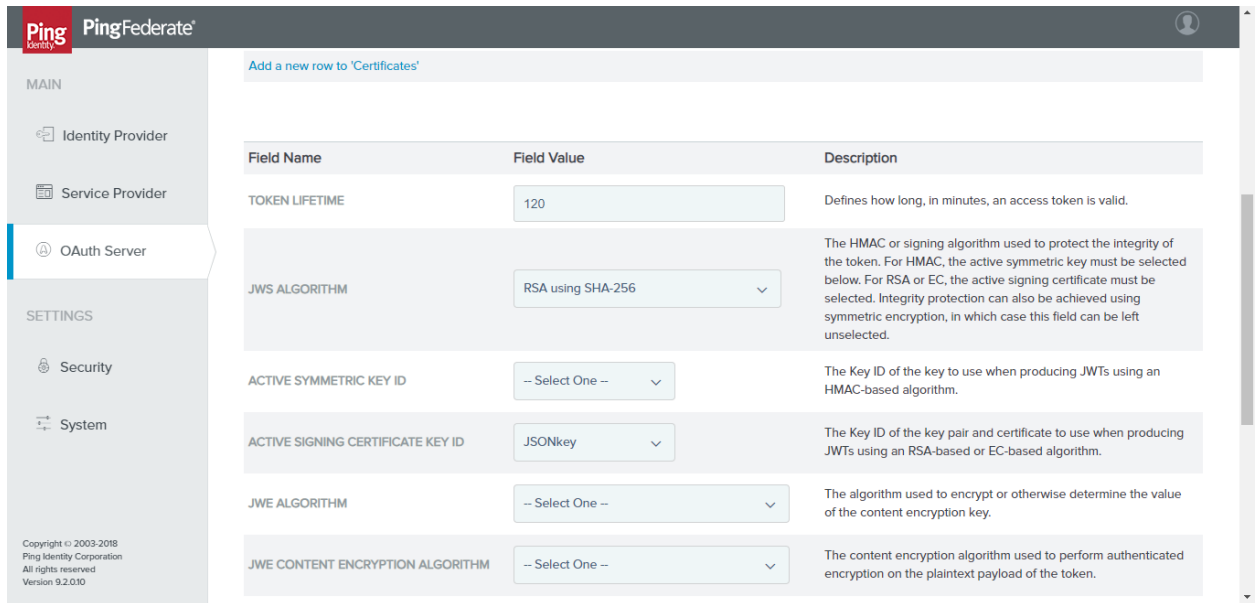
Key ID	Key	Encoding	Action
Add a new row to 'Symmetric Keys'			

Certificates

Key ID	Certificate	Action
JSONkey	01:6C:85:4A:EC:9C (CN=localhost, O=Education, C=US)	Update Cancel
Add a new row to 'Certificates'		

Copyright © 2003-2018 Ping Identity Corporation All rights reserved Version 9.2.0.0

3. Under JWS Algorithm Dropdown, choose RSA using SHA-256.
4. Under Active Signing Certificate Key ID Dropdown, select the key ID which is added above.



PingFederate

MAIN

- Identity Provider
- Service Provider
- OAuth Server**

SETTINGS

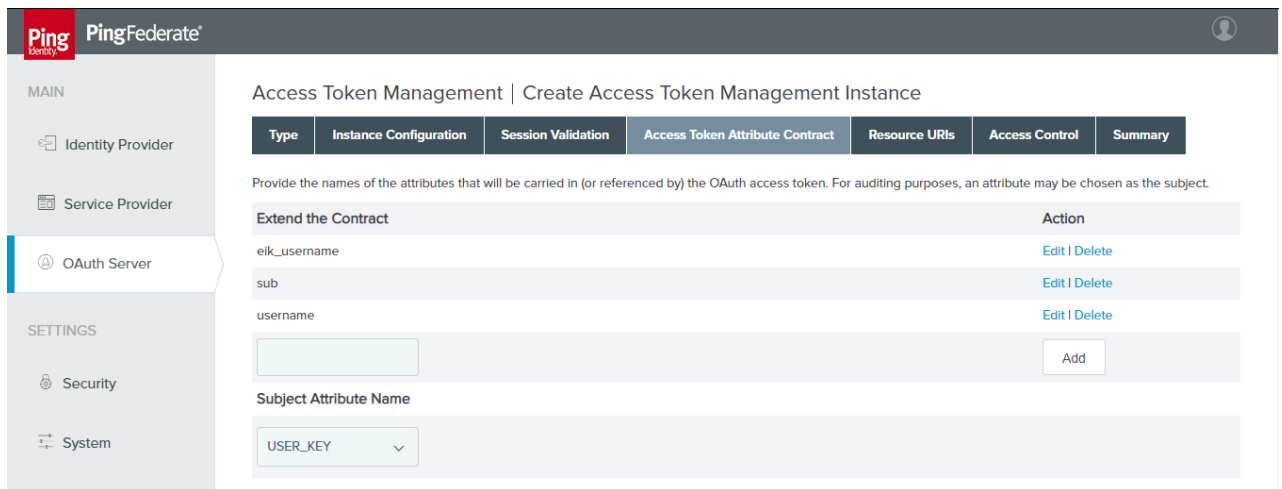
- Security
- System

Copyright © 2003-2018 Ping Identity Corporation All rights reserved Version 9.2.0.10

Add a new row to 'Certificates'

Field Name	Field Value	Description
TOKEN LIFETIME	120	Defines how long, in minutes, an access token is valid.
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	JSONkey	The Key ID of the key pair and certificate to use when producing JWTs using an RSA-based or EC-based algorithm.
JWE ALGORITHM	-- Select One --	The algorithm used to encrypt or otherwise determine the value of the content encryption key.
JWE CONTENT ENCRYPTION ALGORITHM	-- Select One --	The content encryption algorithm used to perform authenticated encryption on the plaintext payload of the token.

5. In the next page, there will be no changes to the Session Validation Settings here. So, leave it defaults.
6. In the below screenshot, In Access Token Attribute Contract, we define the attribute contract for the access tokens issued by this access token management instance. Extend the contract with the 'eik_username' & 'username' attributes.



PingFederate

MAIN

- Identity Provider
- Service Provider
- OAuth Server**

SETTINGS

- Security
- System

Access Token Management | Create Access Token Management Instance

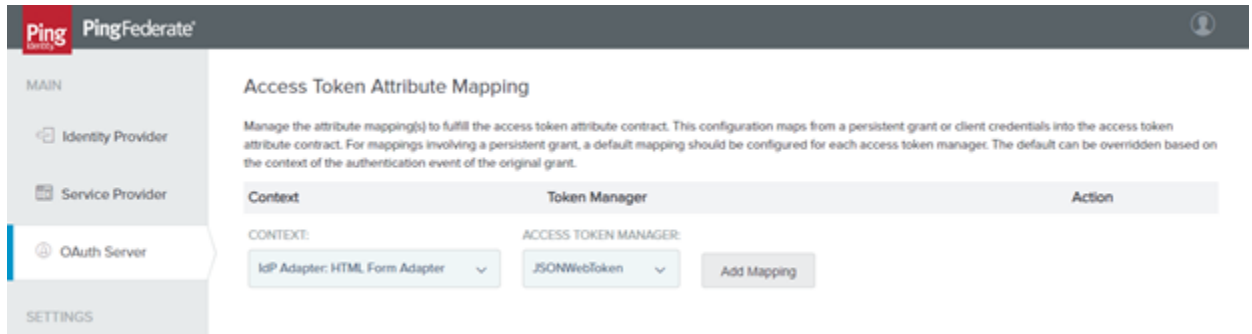
Type	Instance Configuration	Session Validation	Access Token Attribute Contract	Resource URIs	Access Control	Summary
Provide the names of the attributes that will be carried in (or referenced by) the OAuth access token. For auditing purposes, an attribute may be chosen as the subject.						
Extend the Contract						Action
eik_username						Edit Delete
sub						Edit Delete
username						Edit Delete
<input type="text"/>						Add
Subject Attribute Name						
USER_KEY						

7. Click Next.
8. Under Access Control, we can restrict the clients who can use this Access Token Management Instance, which we do not use here. So, click Next.
9. Review the Summary and Click Save.

6.1.2.5 Access Token Mapping

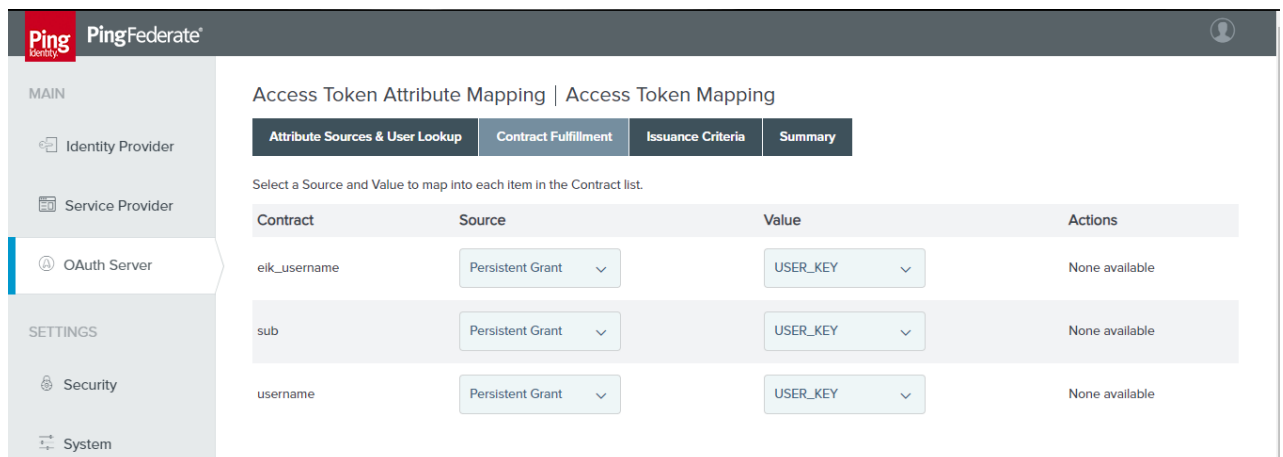
Access Token Mapping is used to map the attributes to fulfill the access token attribute contract. This configuration maps from a persistent grant into the access token attribute contract and there should be a default mapping configured for each access token manager.

1. Go to OAuth Server >> Token Mapping >> Access Token Mapping.
2. Map the “Context” (IDP Adapter: HTMLFormAdapter) to “Access Token Manager” (JSONWebToken) and then click “Add Mapping”.



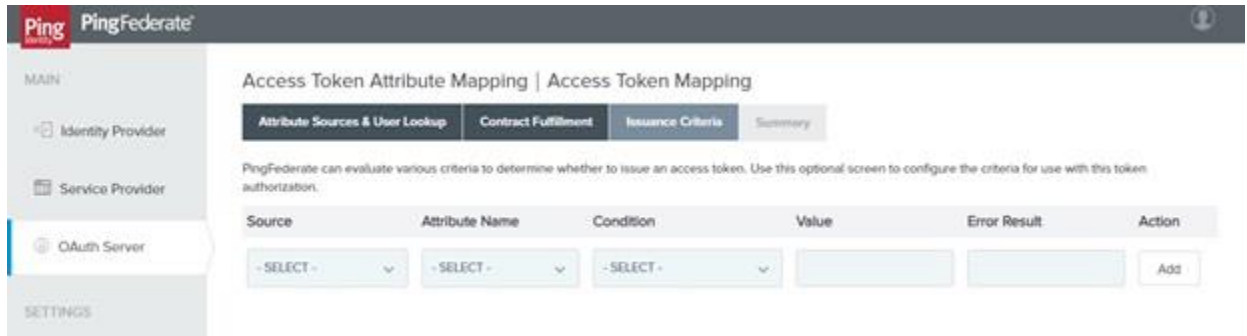
3. In “Attribute Source Lookup” Tab (optional), we can add any Attribute Source to fetch the attribute values from any of your desired datastore and on completion click Next.
4. In “Contract Fulfillment” tab, map the Source as Persistent Grant and its value as “USER_KEY” for all contracts as shown in the below screenshot.

Note: Usually in the Contract Fulfillment screen, we map values into the token attribute contract. These are the attributes that will be included or referenced in the access token. When we select Persistent Grant, the associated Value list is populated by the USER_KEY and extended attributes from the persistent access-token grant.



Contract	Source	Value	Actions
eik_username	Persistent Grant	USER_KEY	None available
sub	Persistent Grant	USER_KEY	None available
username	Persistent Grant	USER_KEY	None available

Note: In this screen, we define the criteria that must be satisfied so that PingFederate processes the request further. In essence, this *token authorization* feature provides the capability to conditionally approve or reject requests based on individual attributes.



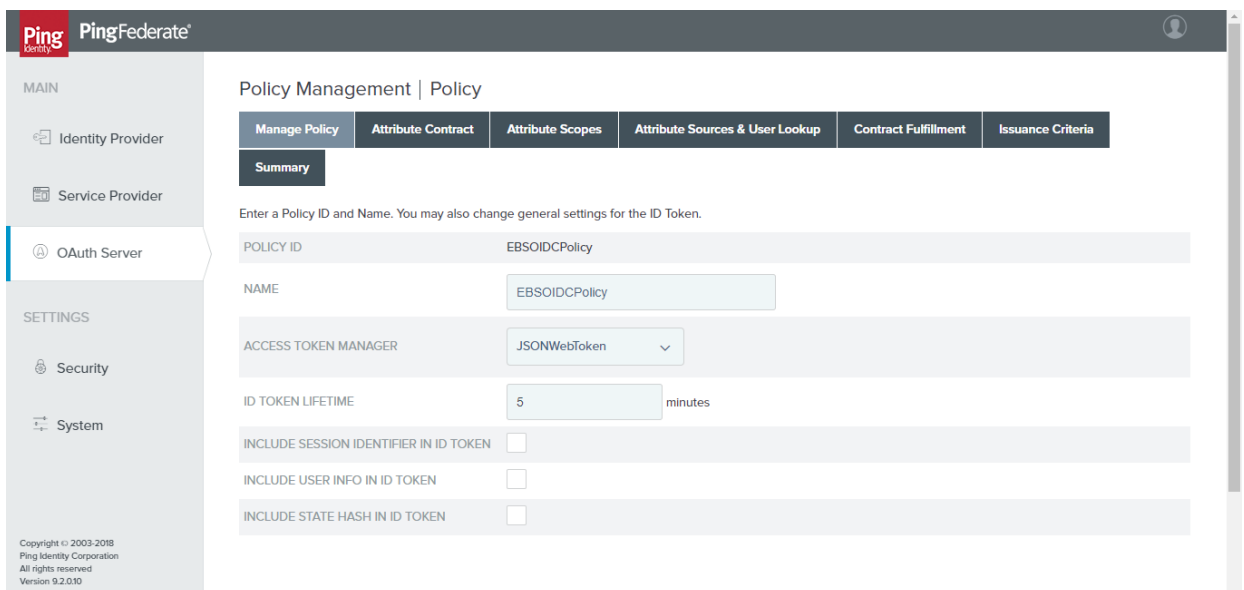
The screenshot shows the 'Access Token Attribute Mapping' screen in PingFederate. The left sidebar has 'OAuth Server' selected under the 'MAIN' section. The main content area has tabs for 'Attribute Sources & User Lookup', 'Contract Fulfillment', 'Issuance Criteria', and 'Summary'. The 'Issuance Criteria' tab is active. Below the tabs, there is a table with columns: Source, Attribute Name, Condition, Value, Error Result, and Action. Each of the first three columns has a '- SELECT -' dropdown menu. There is an 'Add' button at the end of the table. A note above the table states: 'PingFederate can evaluate various criteria to determine whether to issue an access token. Use this optional screen to configure the criteria for use with this token authorization.'

6. Review the Summary and tap Save.

6.1.2.6 OpenID Connect Policy Management

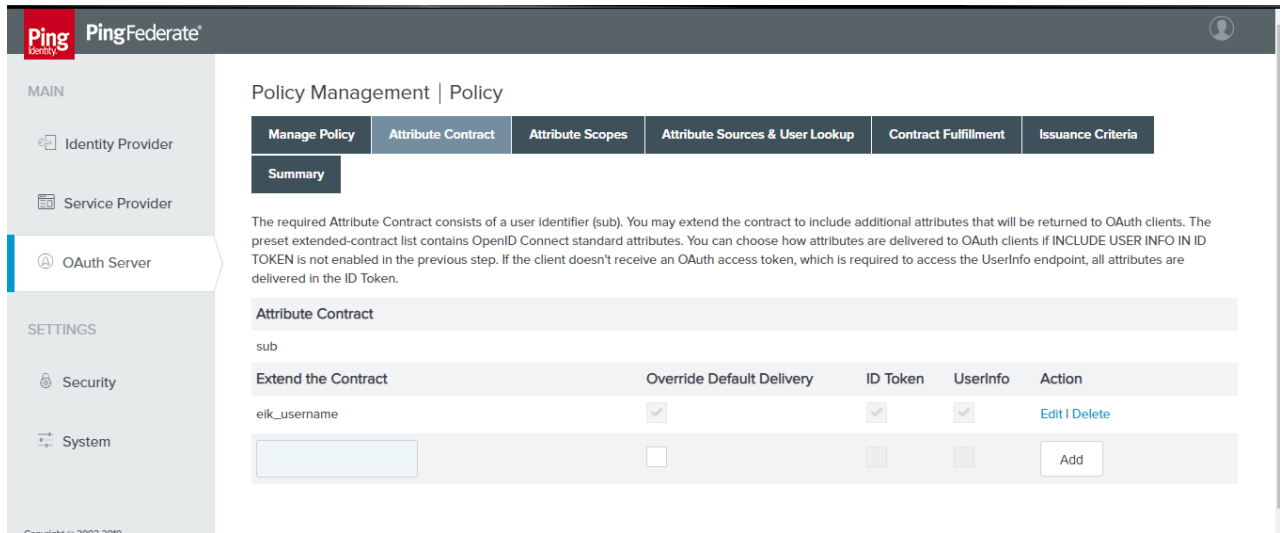
Here we define OpenID Connect policies and manage them for obtaining user attributes which act as the claims to be sent in an ID Token and, also in response to requests received at the PingFederate User Info endpoint. Policies that are defined here can be mapped to specific OAuth clients.

1. Go to OAuth Server >> Token Mapping >> OpenID Connect Policy Management >> Add Policy.
2. Provide a Policy Name & Select the Access Token Manager and leave the remaining as default. Click Next.



The screenshot shows the 'Policy Management' screen in PingFederate. The left sidebar has 'OAuth Server' selected under the 'MAIN' section. The main content area has tabs for 'Manage Policy', 'Attribute Contract', 'Attribute Scopes', 'Attribute Sources & User Lookup', 'Contract Fulfillment', and 'Issuance Criteria'. The 'Manage Policy' tab is active. Below the tabs, there is a 'Summary' section. It contains the following fields: 'POLICY ID' (EBSOIDCPolicy), 'NAME' (EBSOIDCPolicy), 'ACCESS TOKEN MANAGER' (JSONWebToken), 'ID TOKEN LIFETIME' (5 minutes), and three checkboxes: 'INCLUDE SESSION IDENTIFIER IN ID TOKEN', 'INCLUDE USER INFO IN ID TOKEN', and 'INCLUDE STATE HASH IN ID TOKEN'. A note above the fields states: 'Enter a Policy ID and Name. You may also change general settings for the ID Token.'

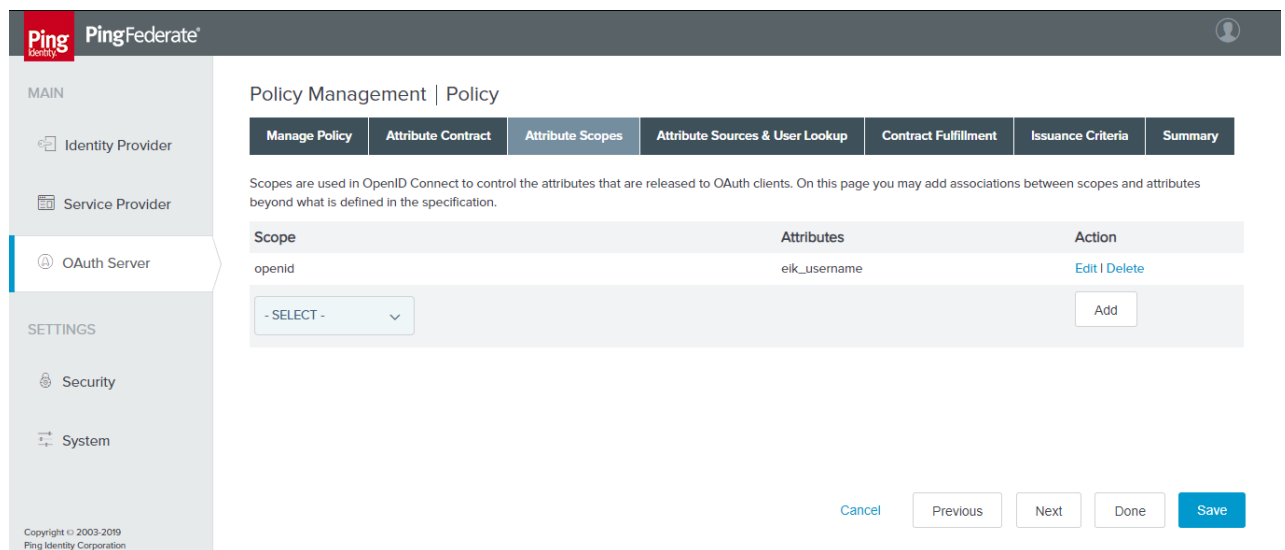
- Under Attribute Contract, Extend the Contract by manually adding 'eik_username' and delete the other attributes present. Enable checkboxes for 'Override Default Delivery',



The screenshot shows the PingFederate Policy Management interface. The left sidebar has 'MAIN' (Identity Provider, Service Provider, OAuth Server) and 'SETTINGS' (Security, System). The 'OAuth Server' is selected. The main area is 'Policy Management | Policy' with tabs: Manage Policy, Attribute Contract (selected), Attribute Scopes, Attribute Sources & User Lookup, Contract Fulfillment, Issuance Criteria, and Summary. Below the tabs is a 'Summary' section with a text block explaining the required Attribute Contract. Below that is the 'Attribute Contract' section with a table:

Extend the Contract	Override Default Delivery	ID Token	Userinfo	Action
eik_username	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit Delete
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Add"/>

- Click Next.
- Under Attribute Scopes Section, select openid from the Scope dropdown and in Attributes tick the 'eik_username' checkbox.

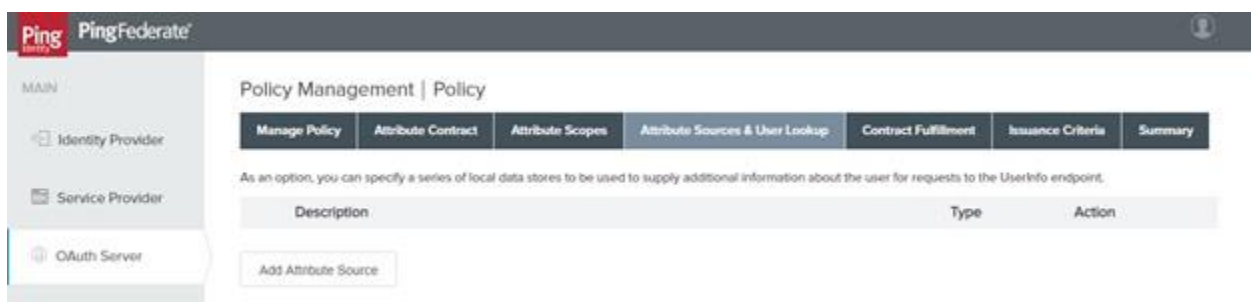


The screenshot shows the PingFederate Policy Management interface. The left sidebar is the same. The main area is 'Policy Management | Policy' with tabs: Manage Policy, Attribute Contract, Attribute Scopes (selected), Attribute Sources & User Lookup, Contract Fulfillment, Issuance Criteria, and Summary. Below the tabs is a text block explaining Scopes. Below that is the 'Attribute Scopes' section with a table:

Scope	Attributes	Action
openid	eik_username	Edit Delete
-SELECT-		<input type="button" value="Add"/>

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

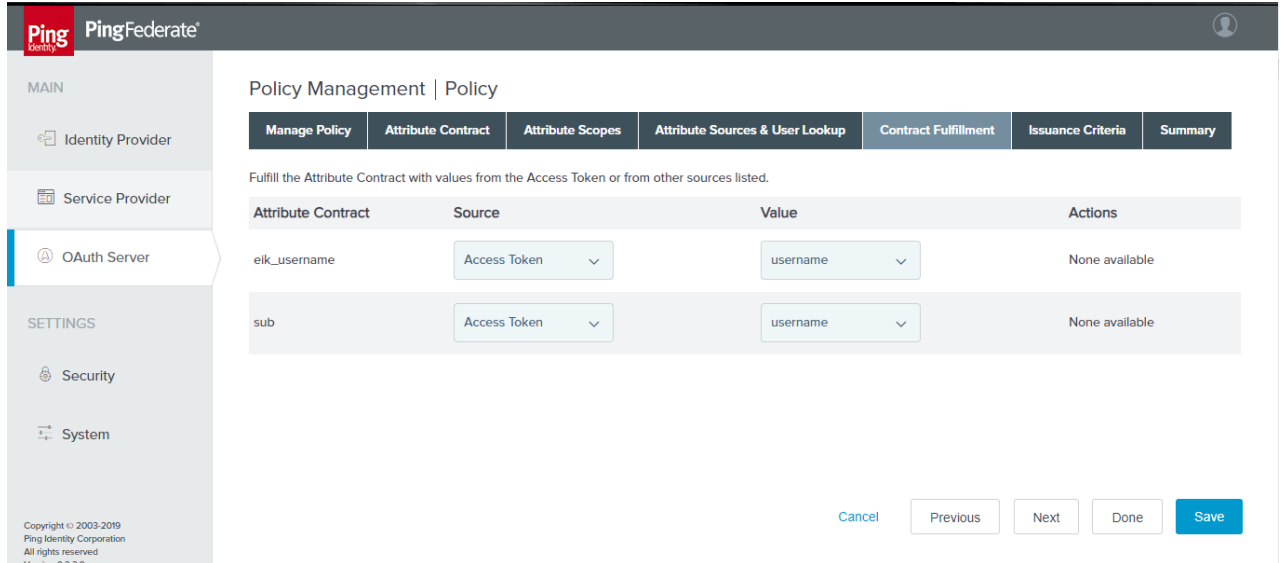
- Attributes can be fetched from any of the datastore at the runtime or leave it as to use the values presented in the Token.



The screenshot shows the PingFederate Policy Management interface. The left sidebar is the same. The main area is 'Policy Management | Policy' with tabs: Manage Policy, Attribute Contract, Attribute Scopes, Attribute Sources & User Lookup (selected), Contract Fulfillment, Issuance Criteria, and Summary. Below the tabs is a text block explaining the option to specify local data stores. Below that is a table with columns: Description, Type, and Action. There is an 'Add Attribute Source' button below the table.

- Under Contract Fulfillment Section, Map the Sub & eik_username attribute from the source - Access Token and value – username.

Note: In the Contract Fulfillment screen, we map attributes from the access token or other sources to fulfill the attribute contract. Here, the value is provided from the access token.

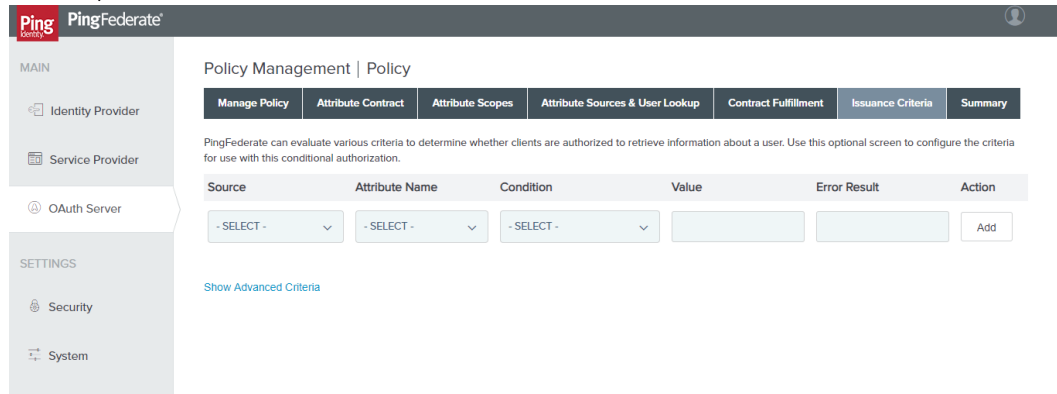


The screenshot shows the PingFederate Policy Management interface. The left sidebar has a 'MAIN' section with 'Identity Provider', 'Service Provider', and 'OAuth Server' (selected), and a 'SETTINGS' section with 'Security' and 'System'. The main content area is titled 'Policy Management | Policy' and has tabs for 'Manage Policy', 'Attribute Contract', 'Attribute Scopes', 'Attribute Sources & User Lookup', 'Contract Fulfillment' (active), 'Issuance Criteria', and 'Summary'. Below the tabs, a message states: 'Fulfill the Attribute Contract with values from the Access Token or from other sources listed.' A table follows with columns: 'Attribute Contract', 'Source', 'Value', and 'Actions'. It contains two rows: one for 'eik_username' and one for 'sub', both mapped to 'Access Token' with a value of 'username'. At the bottom right are buttons for 'Cancel', 'Previous', 'Next', 'Done', and 'Save'.

Attribute Contract	Source	Value	Actions
eik_username	Access Token	username	None available
sub	Access Token	username	None available

- In the next page, provide any restriction rules in case of restricting any unauthorized access.

Note: In this screen, we define the criteria that must be satisfied so that PingFederate processes the request further. In essence, this *token authorization* feature provides the capability to conditionally approve or reject requests based on individual attributes. We can define multiple criteria, so that in this case, *ALL* the criteria must be satisfied in order for PingFederate to move a request to the next phase.



The screenshot shows the PingFederate Policy Management interface, specifically the 'Issuance Criteria' tab. The left sidebar is the same as the previous screenshot. The main content area is titled 'Policy Management | Policy' and has tabs for 'Manage Policy', 'Attribute Contract', 'Attribute Scopes', 'Attribute Sources & User Lookup', 'Contract Fulfillment', 'Issuance Criteria' (active), and 'Summary'. Below the tabs, a message states: 'PingFederate can evaluate various criteria to determine whether clients are authorized to retrieve information about a user. Use this optional screen to configure the criteria for use with this conditional authorization.' A table follows with columns: 'Source', 'Attribute Name', 'Condition', 'Value', 'Error Result', and 'Action'. The first row shows dropdown menus for 'Source', 'Attribute Name', and 'Condition', followed by input fields for 'Value' and 'Error Result', and an 'Add' button. Below the table is a link 'Show Advanced Criteria'.

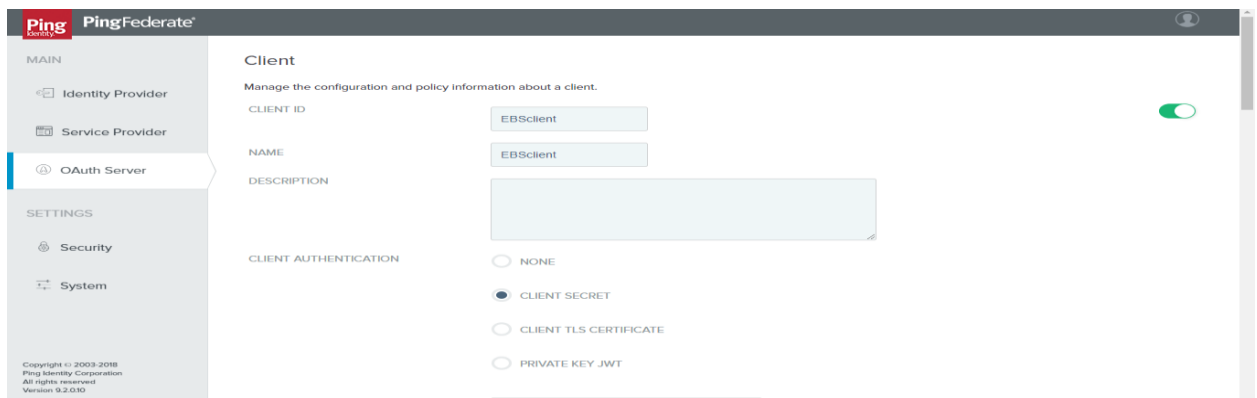
Source	Attribute Name	Condition	Value	Error Result	Action
- SELECT -	- SELECT -	- SELECT -			Add

- Review Summary and Click Save.

6.1.2.7 Client Configuration for OAuth Server

Here we can manage the configurations and policy information related to a client.

1. In the PingFederate Admin Console, go to OAuth Server >> Clients >> Create New
2. Create a new client with the following details
 - Client Name : "<Specify any Client Name for EIK>"
 - Client ID : "<Specify any Client ID for EIK>"
 - Client Secret : "<(Create secret using Generate Secret option)>"
3. Type the Redirection URL in the format:
`https://<pf-hostname>:<pf-runtime-port>/<context>/handler`
4. Tick the checkbox for Bypass Authorization Approval.
5. For Allowed Grant Types, select Authorization Code and Refresh Token.
6. For Default Access Token Manager choose JSONWebToken.
7. Under OpenID Connect section, choose the Policy you configured just before.
8. Leave the remaining as default and click Save.



PingFederate

MAIN

- Identity Provider
- Service Provider
- OAuth Server**

SETTINGS

- Security
- System

Copyright © 2003-2018 Ping Identity Corporation. All rights reserved. Version 9.2.0.30

Client

Manage the configuration and policy information about a client.

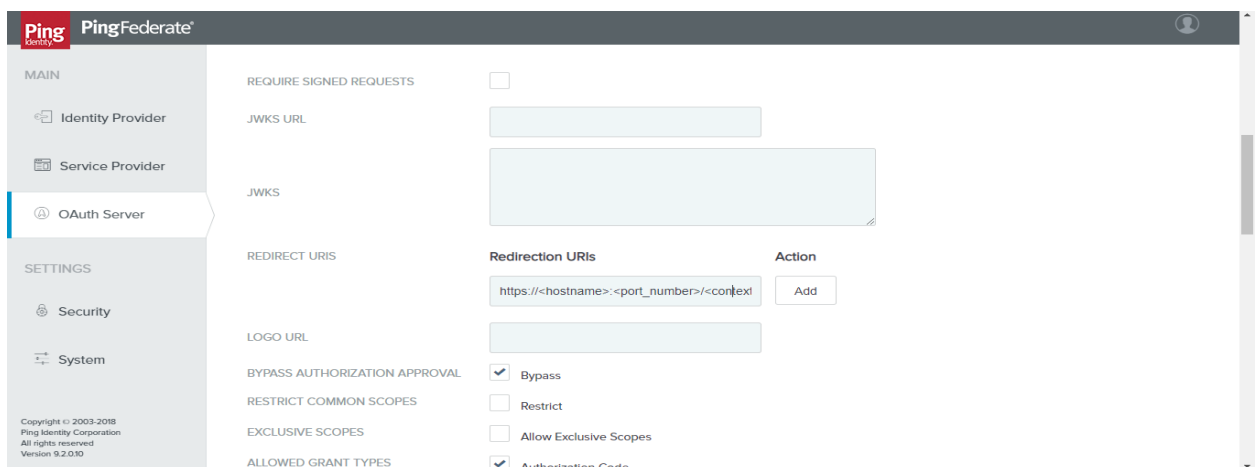
CLIENT ID:

NAME:

DESCRIPTION:

CLIENT AUTHENTICATION

- ☐ NONE
- ☒ CLIENT SECRET
- ☐ CLIENT TLS CERTIFICATE
- ☐ PRIVATE KEY JWT



PingFederate

MAIN

- Identity Provider
- Service Provider
- OAuth Server**

SETTINGS

- Security
- System

Copyright © 2003-2018 Ping Identity Corporation. All rights reserved. Version 9.2.0.30

REQUIRE SIGNED REQUESTS: ☐

JWKS URL:

JWKS:

REDIRECT URIS

Redirection URIs	Action
<input type="text" value="https://<hostname>:<port_number>/<context>"/>	<input type="button" value="Add"/>

LOGO URL:

BYPASS AUTHORIZATION APPROVAL: ☒ Bypass

RESTRICT COMMON SCOPES: ☐ Restrict

EXCLUSIVE SCOPES: ☐ Allow Exclusive Scopes

ALLOWED GRANT TYPES: ☒ Authorization Code

Ping Federate

MAIN

- Identity Provider
- Service Provider
- OAuth Server**

SETTINGS

- Security
- System

Copyright © 2003-2018
Ping Identity Corporation
All rights reserved
Version 9.2.0.10

BYPASS AUTHORIZATION APPROVAL ☒ Bypass

RESTRICT COMMON SCOPES ☐ Restrict

EXCLUSIVE SCOPES ☐ Allow Exclusive Scopes

ALLOWED GRANT TYPES

- ☒ Authorization Code
- ☐ Implicit
- ☐ Refresh Tokens
- ☐ Client Credentials
- ☐ Device Flow
- ☐ Resource Owner Password Credentials
- ☐ Extension Grants
- ☐ Access Token Validation (Client is a Resource Server)

RESTRICT RESPONSE TYPES ☐ Restrict

DEFAULT ACCESS TOKEN MANAGER **JSONWebToken**

VALIDATE AGAINST ALL ELIGIBLE ACCESS TOKEN MANAGERS ☐

PERSISTENT GRANTS MAX LIFETIME ☒ Use Global Setting

Activate Windows
Go to PC settings to activate Windows.

Ping Federate

MAIN

- Identity Provider
- Service Provider
- OAuth Server**

SETTINGS

- Security
- System

Copyright © 2003-2018
Ping Identity Corporation
All rights reserved
Version 9.2.0.10

PERSISTENT GRANTS IDLE TIMEOUT ☒ Use Global Setting

☐ Grants Do Not Timeout Due To Inactivity

☐ Days

REFRESH TOKEN ROLLING POLICY ☒ Use Global Setting ☐ Don't Roll ☐ Roll

OPENID CONNECT

ID Token Signing Algorithm **Default**

ID Token Key Management Encryption Algorithm **No Encryption**

Policy **EBSOIDCPOLICY**

☐ Grant Access to Session Revocation API

6.2 Configure SSL Server certificate

SSL certificates are created as they need to be presented for getting access to the PingFederate administrative console and for all the incoming HTTPS connections at the runtime engine nodes.

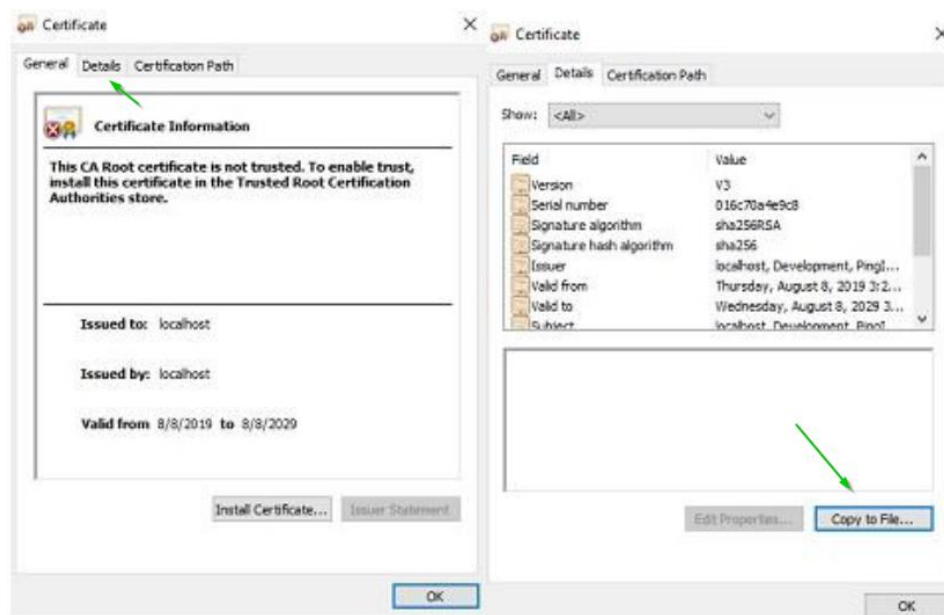
If you already own an SSL certificate for pingfederate we can skip to the Key Generation part, else we need to proceed with the following steps to configure a self-signed certificate;

1. In PingFederate Click Security >> Security and Certificate Key Management >> SSL Server Certificate >> Create New
2. Enter the details and create a certificate.
3. Export this certificate now with the option of exporting “Certificate Only” and not with the private key.

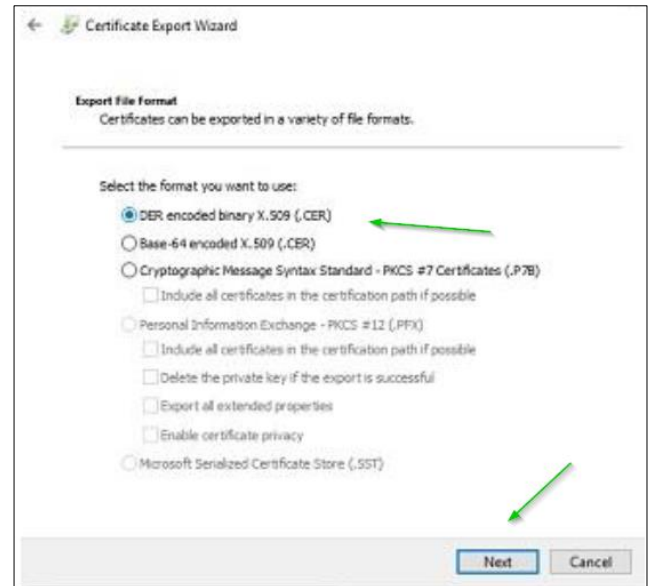
Note: As part of the Key Generation process, add the exported certificate to Trusted CAs in PingFederate Admin console.

6.2.1 Importing the SSL Certificate into the Java Key Store

1. The EIK requires the SSL certificates used by the PingFederate Runtime engines to be imported into the trusted java keystore of the node it is deployed in. This step should be replicated on all PingFederate-EIK nodes if a clustered setup is implemented.
2. Open the .crt file that was generated in step 6.2. Select the “Details” tab and select the “Copy to File” button:



3. In the Certificate Export Wizard click “Next” and select the format as “DER encoded binary X.509(.CER)” and click “Next”:



4. Choose any folder where you’d like to export this file and click “Next” and proceed to “Finish”. Copy the generated .cer file to the PingFederate-EIK node.
5. Now run the below command on the PingFederate-EIK node:

Keytool -keystore “<path of JAVA_HOME folder>\jre\lib\security\cacerts” -importcert -alias <anyname> -file <path of the .cer file that was generated>

```
C:\Program Files\Java\jdk1.8.0_161\jre>keytool -keystore "C:\Program Files\Java\jdk1.8.0_161\jre\lib\security\cacerts" -importcert -alias
Enter keystore password:
Owner: CN=localhost, OU=Development, O=PingIdentity, L=Denver, ST=CO, C=US
Issuer: CN=localhost, OU=Development, O=PingIdentity, L=Denver, ST=CO, C=US
Serial number: 16c70a4e9c8
Valid from: Thu Aug 08 15:22:31 IST 2019 until: Wed Aug 08 15:22:31 IST 2029
Certificate fingerprints:
    MD5: 19:82:FE:C0:C6:61:AF:51:F1:7D:00:89:DD:FE:4D:D6
    SHA1: 2A:F7:7C:01:BF:C7:S9:B2:A9:3B:DA:AF:48:8C:B5:95:2C:EB:88:47
    SHA256: F8:F5:39:2C:8A:FD:FC:AC:D8:9F:B6:DC:C4:70:86:F8:D8:B1:B0:84:82:F9:87:F5:0F:CE:5B:A5:35:A9:80:ED
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3
Trust this certificate? [no]: yes
Certificate was added to keystore
C:\Program Files\Java\jdk1.8.0_161\jre>
```

6. Enter the keystore password as “changeit” (default password)
7. Enter “yes” to the “Trust this certificate?” prompt.

Note: The process of importing the .cer file into the java keystore should be replicated on all PingFederate-EIK nodes.

7. EIK Deployment in PingFederate

The following steps should be followed for the deployment of EBS Integration Kit in PingFederate server. As a pre-requisite, the EIKAuth.config configuration file & EIK.dbcx EBS DataSource (DBCX) file should be generated before deploying the EIK war package.

Pre-Requisite: An environment variable 'EIK_HOME' should be set in the PingFederate server before deploying the EBS Integration Kit.

1. Navigate to <pf_install>/pingfederate directory
2. Create a new directory named "EBSAuth". After creation, the directory structure will look like the following:
 <pf_install>/pingfederate/EBSAuth
3. Now, Place the EBS IKT license file "ebsauth.lic" in <pf_install>/pingfederate /EBSAuth directory.
4. Now navigate to user's base path using `cd ~` and set the environmental variable for EIK_HOME in .bash profile : `vi .bash_profile`
5. Set EIK_HOME using this command: `export EIK_HOME = <pf_install>/pingfederate`
6. Save and close the file.
7. Enter the following command to source the bash file: `./bash_profile`
8. Verify the new settings using the following commands, `echo $EIK_HOME`

Note: If PingFederate is configured in Cluster, repeat steps 1 to 8 in all the runtime servers.

7.1 EIKAuth Config File Generation

1. The JAR file EIKutility.jar needs to be placed in the \$EIK_HOME directory created in the previous section.
2. Open terminal/command prompt (as Administrator) and navigate to EIK_HOME directory and execute the following command

```
java -cp EIKutility.jar com.likeminds.EBSAuth.EIKAdminUtility
```

3. On running the command, we get a dialog box as follows, Enter all values as per the configuration for all the fields using the template given below

Please enter the following:

ICX Cookie Domain :

ICX Cookie Path :

EBS Landing page :

EBS Logout page :

Authentication Server URL :

Token Endpoint URL :

Introspect URL :

Redirect URI :

JWKS Validation URL :

Grant Type :
authorization_code

Auth type :
OIDC

JIT :
false

Scope :

Authentication Attribute :
eik_username

Client ID :

Client Secret :

Enter the Context path of WAR :

Enter the issuer :

OK Cancel

```
#----- Configuration Panel-----#
icx_cookie_domain = <domain name> (the "." period should precede the root domain
name)
icx_cookie_path = /
ebs_landing_page = <EBS Home Page URL> e.g.:
http://ebs.examplecompany.com:8000/OA_HTML/OA.jsp?OAFunc=OAHOMEPAGE
ebs_logout_page = https://<pf or pa domain name>:<port>/idp/startSLO.ping
#OIDC Configuration parameters
authentication_server_url = https://<pf/pa hostname>:<port>/as/authorization.oauth2
token_endpoint_url = https:// <pf/pa hostname>:<port>/as/token.oauth2
introspect_url = https:// <pf/pa hostname>:<port>/as/introspect.oauth2
redirect_uri = https:// <pf/pa hostname>:<port>/EBSAuth/handler
jwks_validation_url = https:// <pf/pa hostname>:<port>/pf/JWKS
grant_type = authorization_code
auth_type = OIDC
JIT = false
Scope = openid (necessary scope to return EBS username from PingFederate/LDAP store)
Authentication Attribute = eik_username (non-editable)
client_id = ***** # CLIENT_ID created on the PF console
client_secret = ***** # CLIENT_SECRET created on the PF console
Enter the context path of WAR = <Context of the war>
(i.e., For EBSAuth.war, context is /EBSAuth)
(Optional - For EBSAuthInst2.war, context is /EBSAuthInst2)
Enter the issuer = <PingFederate OAuth/OIDC issuer>
#-----END-----#
```

4. After entering these values in the dialog box, a file named `EIKAuth.config` gets generated at the `EIK_HOME` directory.
5. Now, move the `EIKAuth.config` file to the following location:

```
<pf_install>/pingfederate/EBSAuth
```

Note: If PingFederate is configured in Cluster, copy the EIKAuth.config file to all the runtime servers in the same directory location.

7.2 EBS DataSource (DBCX) File Creation

1. Before proceeding with the DBCX file generation, a custom user should be created in the EBS Application FND_USER table (Username – EIKUSER) with the UMX|APPS_SCHEMA_CONNECT role enabled.
2. Place the JAR file EBSdatasource.jar in the \$EIK_HOME directory & open the terminal/command prompt and navigate to EIK_HOME directory to execute and generate the EBS Datasource file

```
java -cp EBSdatasource.jar com.likeminds.ebsauth.v1.EIKDatasource Y
```

Note: The jar file can also be placed & executed in any server outside of PingFederate, provided, there should be a connectivity to the EBS Database from the execution source.

3. In the next step, provide the configuration details of your environment as mentioned in the screenshot:

```
C:\Users\LIKEMINDS-17\Desktop\Utilities\Utilities_with_Guide>java -cp ebsdatasource-jar-with-dependencies.jar;c:\Users\LIKEMINDS-17\Desktop\Utilities\Utilities_with_Guide\ojdbc8.jar;c:\Users\LIKEMINDS-17\Desktop\Utilities\Utilities_with_Guide\ons.jar;c:\Users\LIKEMINDS-17\Desktop\Utilities\Utilities_with_Guide\ucp.jar com.likeminds.eb
sauth.v1.EIKDataSource Y
22:06:56.445 [main] TNFO com.likeminds.ebsauth.v1.EIKDataSource - Name of the DBCX file with path where database configuration will be saved C:\Users\LIKEMINDS-17\Desktop\Utilities\Utilities_with_Guide\eik.dbcx
Enter the connection factory class (oracle.jdbc.pool.OracleDataSource)->oracle.jdbc.pool.OracleDataSource
User entered following value ->oracle.jdbc.pool.OracleDataSource
Enter the JDBC URL(For eg) jdbc:oracle:thin:@EBS DB domain name:<EBS DB Port>:<SID>->jdbc:oracle:thin:@<Your EBS DB domain name>:<Your EBS DB Port>:<Your SID>
User entered following value ->jdbc:oracle:thin:@<Your EBS DB domain name>:<Your EBS DB Port>:<Your SID>
Enter the apps username->apps
User entered following value ->apps
Enter the apps password->
Enter connection pool name->EBSAuth
User entered following value ->EBSAuth
Enter initial connection pool size->30
User entered following value ->30
Enter min. connection pool size->30
User entered following value ->30
Enter max. initial pool size->50
User entered following value ->50
Enter timeout check interval (Default is 30 secs)->30
User entered following value ->30
Enter inactive connection timeout (Default is 0 secs)->0
User entered following value ->0
Enter validate connection on borrow (true/false)->true
User entered following value ->true
Enter the EIK user username->Enter your EIKUSER name>
User entered following value -><Enter your EIKUSER name>
Enter the EIK user password->
Enter the context path->/EBSAuth
User entered following value ->/EBSAuth
```

Enter the connection factory class: oracle.jdbc.pool.OracleDataSource
Enter the JDBC URL: jdbc:oracle:thin:@<EBS DB domain name>:<EBS DB Port>:<SID>
(Use Scan hostnames in case of RAC database)

Enter APPS username:
Enter APPS password:
Enter Connection pool name: EBSAuth
Enter initial connection pool size: 10
Enter min. connection pool size: 10
Enter max. initial pool size: 50
Enter timeout check interval(Default is 30 secs): 30
Enter inactive connection timeout (Default is 0 secs): 30
Enter validate connection on borrow (true/false): true
Enter the EIK username: EIKUSER
Enter the EIK user password:
Enter the Context Path: </Context of the war file>

4. After entering all the above-mentioned values, the EIKUSER will get registered with the following message.

```
connection established
Registering User
User has been registered successfully
```

5. As part of the successful execution, a new file EIK.dbcx will be generated in the EIK_HOME directory.
6. Now move the EIK.dbcx file to the following location:

<pf_install>/pingfederate/EBSAuth

Note: If PingFederate is configured in Cluster, copy the EIK.DBCX file to all the runtime servers in the same directory location.

7.3 Deploying the log4j2.xml File

Move the provided log4j2.xml file to the following location:

`<pf_install>/pingfederate/EBSAuth`

Note: If PingFederate is configured in Cluster, copy the log4j2.xml file to all the runtime servers in the same directory location.

7.4 Deploying EBSAuth.war File

1. To deploy the EBSAuth.war file in the PingFederate server, navigate to the “deploy” directory in the PingFederate installation directory.

```
cd /<pf_install>/pingfederate/server/default/deploy
```

2. Now copy and place the EBSAuth.war file in the above deploy directory.

Note: If PingFederate is configured in Cluster, copy the EBSAuth.war file to all the runtime servers.

3. Restart the PingFederate runtime servers (on All runtime engine nodes if it is a clustered deployment)

8 System Profile Parameter changes in EBS

The following Oracle EBS System Profile changes will enable SSO by delegating the authentication to PingFederate via EIK.

8.1 System Profile Changes

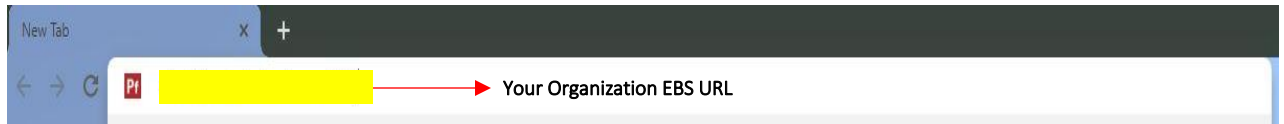
1. Login into the EBS Application using the System Admin credentials.
2. Locate and change the following EBS system profiles at Site Level for enabling SSO.

i) Application SSO Type	SSWA w/SSO
ii) Application Authenticate Agent For Example Application server (PingFederate) PingFederate Runtime port context (case-sensitive)	<a href="https://<pf-server_name>:<pf-port>/EBSAuth">https://<pf-server_name>:<pf-port>/EBSAuth https://pf-server.net:9031/EBSAuth https://pf-server.net 9031 EBSAuth
iii) Application SSO Login Types	Both
iv) Application SSO Auto Link User	Enabled
v) Application SSO LDAP Synchronization	Disabled

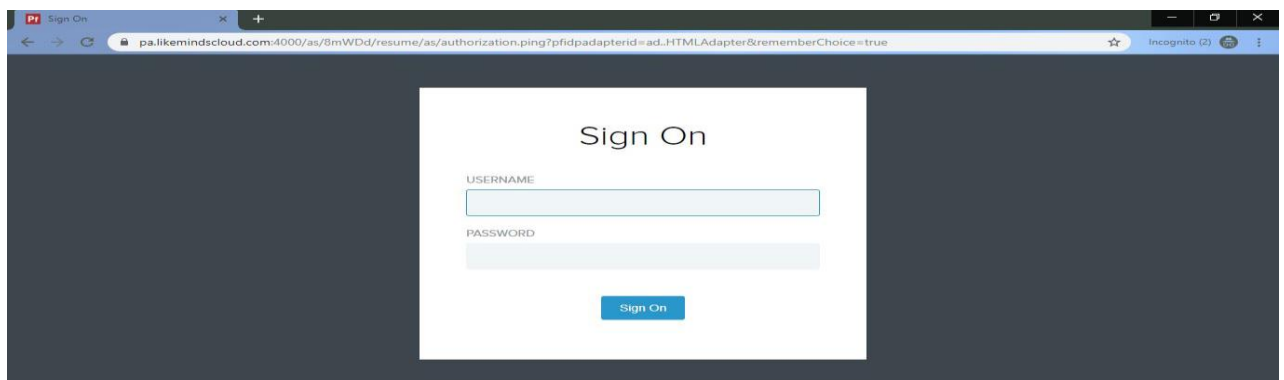
3. Restart the EBS Application Server once the changes had been made and this completes the SSO profile parameter changes in Oracle EBS.

9 SSO Testing for Oracle EBS

1. Enter the URL for SSO of EBS (For Example: <ebs-hostname>:<port>)



2. This URL redirects the user to Pingfederate which throws up an authentication prompt for entering the user credentials.



3. On successful validation of the user credentials, the user will get access to the EBS Homepage.



Thank you!



About LikeMinds Consulting Inc

LikeMinds consulting is a leading provider of consulting, systems integration and managed services and focuses on Identity Management, Application Security, Governance, Risk and Compliance solutions. We have focused on providing our customers with a full range of services which span through our core beliefs of Advising, Integrating, Maintaining and Accelerating the Complete Identity and Security Solution.

For more information, contact us toll-free 1-888-562-3528, email info@likemindsconsulting.com or visit likemindsconsulting.com

© 2020 Like Minds Consulting. All rights reserved