

PingFederate®

EULA IdP Adapter v1.0.0

User Guide



© 2005-2018 Ping Identity ® Corporation. All rights reserved.

PingFederate EULA IdP Adapter User Guide
Version 1.0.0
April 2018

Ping Identity Corporation
1001 17th Street, Suite 100
Denver, CO 80202
USA

Phone: 877.898.2905 (+1 303.468.2882 outside North America)

Fax: 303.468.2909 E-mail: info@pingidentity.com

Web Site: <http://www.pingidentity.com>

Trademarks

Ping Identity, the Ping Identity logo, PingFederate, PingID, PingOne, PingConnect, and PingEnable are registered trademarks of Ping Identity Corporation (“Ping Identity”). All other trademarks or registered trademarks are the property of their respective owners.

Disclaimer

This document is proprietary and not for general publication. It may be provided ad hoc for informational purposes only, and the information herein is subject to change without notice. Ping Identity does not provide any warranties and specifically disclaims any liability in connection with this document.

Note that Ping Identity may not provide support for any sample configurations provided in this document. The variability inherent among security environments prevents full testing and support for all possible platform configurations. If you need special assistance or would like to inquire about implementation or support programs, please contact Ping Identity Global Client Services (<http://support.pingidentity.com>).

Table of Contents

Purpose	4
Prerequisites.....	4
Installation.....	4
Configuration	5
Adapter Configuration Details	9
LDAP Configuration	10
Testing.....	11
Test Case 1 – User Accepts EULA.....	11
Test Case 2 – User Declines EULA	12
Test Case 3 – User Accepts EULA on behalf of an organization	13
Logging.....	15

Purpose

This user guide is intended for use by PingFederate clients, who would like the ability to leverage an IdP adapter that can display an “End User License Agreement” (EULA) during the authentication flow to determine if the user has accepted the EULA, and if not, to prompt the user for acceptance.

Prerequisites

This document assumes that you already have the following installed and configured:

- A functional PingFederate environment, version 9.0+
- JDK version 8+

Installation

1. From the `/dist` folder in *pf-eula-adapter-1.0.0-distro-assembly.zip*, copy the below noted files to the following directory in your PingFederate install.

From /dist	To <YourPFInstall>/pingfederate/server/default
pf-eula-adapter-1.0.0.jar	/deploy/
/language-packs/idp-eula-adapter.properties	/conf/language-packs/
/templates/*.html	/conf/templates/
/templates/mail-notifications/*.html	/conf/templates/mail-notifications/

2. Add the following key-value pairs to the end of the text file:
<YourPFInstall>/pingfederate/server/default/conf/language-packs/pingfederate-email-messages.properties

```
message-template-email-eula.html=End User License Agreement
message-template-email-eula.greetUser=Hello ${USERNAME},
message-template-email-eula.messageHeader=Please take the time to review our End User
License Agreement.
message-template-email-eula.eulaContent=${EULACONTENT}
message-template-email-eula.messageFooter=Thank you for being a loyal customer.
message-template-email-eula.regards=Sincerely,
message-template-email-eula.sender=Acme Corporation
```

- a. Feel free to modify these values to match your business needs.
 - b. The keywords `${USERNAME}` and `${EULACONTENT}` come from PingFederate and will be filled dynamically by the server with appropriate values.
3. Repeat steps 1 and 2 on other clustered engine nodes.
 4. Start or restart PingFederate.

PingFederate supports internationalization (i18n). The files *idp-eula-adapter.properties* and *pingfederate-email-messages.properties* support locale-specific data. For more information, please refer to: <https://docs.oracle.com/javase/tutorial/i18n/resbundle/concept.html>

Configuration

Note: The EULA IdP Adapter must be used as part of an Authentication Composite Adapter or in an IdP Authentication Policy, either of which performs the authentication prior to displaying the EULA.

1. Log into the PingFederate admin console and click **Adapters** under **Identity Provider >> Application Integration**.
2. Click **Create New Instance...**
3. Enter the **Instance Name**, **Instance Id**, and select **EULA IdP Adapter 1.0.0** as the **Type**, and click **Next**.

The screenshot shows the PingFederate admin console interface. On the left is a sidebar with a 'MAIN' section containing 'Identity Provider' (selected), 'Service Provider', and 'OAuth Server', and a 'SETTINGS' section containing 'Server Configuration'. The main content area is titled 'Manage IdP Adapter Instances | Create Adapter Instance' and has a tabbed interface with 'Type' selected. Below the tabs is a text instruction: '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 'eula', 'INSTANCE ID' with the value 'eula', 'TYPE' with a dropdown menu showing 'pf-eula-adapter 1.0.0', and 'PARENT INSTANCE' with a dropdown menu showing 'None'. At the bottom right of the form are 'Cancel' and 'Next' buttons.

Type	IdP Adapter	Extended Contract	Adapter Attributes	Adapter Contract Mapping	Summary
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.					
INSTANCE NAME	<input type="text" value="eula"/>				
INSTANCE ID	<input type="text" value="eula"/>				
TYPE	<input type="text" value="pf-eula-adapter 1.0.0"/>				
PARENT INSTANCE	<input type="text" value="None"/>				

4. Fill out the configuration where needed, and click **Next**.

PingFederate

MAIN

Identity Provider

Service Provider

OAuth Server

SETTINGS

Server Configuration

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.

pf-eula-adapter 1.0.0

Field Name	Field Value	Description
LDAP DATA SOURCE	localhost:389	The LDAP Data Store that will be used for lookups.
USER BASE DN	ou=People,dc=example,dc=com	The search base for user objects (E.g. OU=Employees, DC=corp, DC=domain, DC=com).
USER FILTER	uid=\${username}	The LDAP filter for finding a user (E.g. 'uid=\${username}').
USER SEARCH SCOPE	<input checked="" type="radio"/> One Level <input type="radio"/> Subtree	
EULA ATTRIBUTE	eula	The name of the "EULA" attribute in the user's LDAP object.
REFERENCE DN ATTRIBUTE	manager	The name of the attribute in the user's LDAP object that references where the EULA attribute is maintained.
REFERENCE EULA ATTRIBUTE	eula	The name of the "EULA" attribute in the reference LDAP object.
SIGNER DN ATTRIBUTE	signerdn	The name of the "Signer's DN" attribute in the reference LDAP object.
SIGNED TIMESTAMP ATTRIBUTE	signedtimestamp	The name of the "Signed Timestamp" attribute in the reference LDAP object.
EULA CONTENT DN	cn=eula,dc=example,dc=com	The DN of the object that contains the EULA verbiage.
EULA CONTENT ATTRIBUTE	description	The name of the attribute that contains the EULA verbiage.
EULA TEMPLATE	eula.template.html	Name of the EULA template that will be displayed to the user.

Manage Data Stores
[Show Advanced Fields](#)

Cancel
Previous
Next
Done

Copyright © 2003-2018
Ping Identity Corporation
All rights reserved
Version 9.0.1.0

- If an email containing the EULA should be sent to the user, click **Show Advanced Fields** and enter appropriate values, then click **Next**. Please note that PingFederate will need to be configured with an Email Server (Server Configuration -> Server Settings -> Runtime Notifications -> Email Server Settings) for this service to work.

SEND EULA VIA EMAIL
☐

USER DISPLAY NAME ATTRIBUTE	cn	The name of the "displayName" attribute in the user's LDAP object. Default value is "cn".
USER EMAIL ATTRIBUTE	mail	The name of the "Email" attribute in the user's LDAP object. Default value is "mail".
EMAIL EULA TEMPLATE	message-template-email-eula.html	Name of the Email EULA template that will be sent to the user.

6. Choose the **Pseudonym**, and click **Next**.

Ping
Identity

PingFederate®

MAIN

IdP

Identity Provider

SP

Service Provider

AS

OAuth Server

SETTINGS

Server Configuration

Manage IdP Adapter Instances | Create Adapter Instance

Type

IdP Adapter

Extended Contract

Adapter Attributes

Adapter Contract Mapping

Summary

As an IdP, some of your SP partners may choose to receive a pseudonym to uniquely identify a user. From the attributes in this authentication adapter, please select the values that you would like to use in constructing this unique identifier. Optionally, specify here any attributes that must be masked in log files.

Attribute	Pseudonym	Mask Log Values
username	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MASK ALL OGNL-EXPRESSION GENERATED LOG VALUES		

Cancel

Previous

Next

7. Click **Next**.

8. Review the summary and click **Done**.

PingFederate®

MAIN

Identity Provider
Service Provider
OAuth Server

SETTINGS

Server Configuration

Manage IdP Adapter Instances | Create Adapter Instance

Type
IdP Adapter
Extended Contract
Adapter Attributes
Adapter Contract Mapping
Summary

IdP adapter instance summary information.

Create Adapter Instance

Type

Instance Nameeula
Instance IDEula
Typepf-eula-adapter 1.0.0
Class Namecom.pingidentity.ps.pf.adapter.idp.EulaAdapter
Parent Instance NameNone

IdP Adapter

LDAP Data Sourcelocalhost1389
User Base DNou=People,dc=example,dc=com
User Filteruid=\${username}
User Search ScopeOne Level
EULA Attributeeula
Reference DN Attributemanager
Reference EULA Attributeeula
Signer DN Attributesignerdn
Signed Timestamp Attributesignedtimestamp
EULA Content DNcn=eula,dc=example,dc=com
EULA Content Attributiondescription
EULA Templateeula.template.html
Send EULA via Emailtrue
User Display Name Attributecn
User Email Attributemail
Email EULA Templatemessage-template-email-eula.html

Extended Contract

Attributeusername

Adapter Attributes

Mask all OGNL expression log valuesfalse
Pseudonymusername

Adapter Contract Mapping

Attribute Sources & User Lookup

Data Sources(None)

Adapter Contract Fulfillment

usernameusername (Adapter)

Issuance Criteria

Criterion(None)

Cancel

Previous

Done

Copyright © 2003-2018
Ping Identity Corporation
All rights reserved
Version 9.01.0

9. Click **Save**.

Adapter Configuration Details

The table below describes in more detail each of the fields needed to configure the EULA IdP Adapter.

Field Name	Description	LDAP Syntax
LDAP Data Source	The LDAP data store that will be used by the adapter. The LDAP data store is configured thru <i>PingFederate Server Configuration -> Data Stores</i> .	
User Base DN	The LDAP search base DN for user lookups.	DN
User Filter	The LDAP search filter for user lookups. "username" substitution is allowed (ie., 'uid=\${username}').	LDAP Search Filter
User Search Scope	The LDAP search scope for user lookups.	LDAP Search Scope
EULA Attribute	The name of the attribute, in the user object, that holds the Boolean value of whether the user has accepted or declined the EULA.	Boolean { TRUE FALSE } A null value would be treated as FALSE.
Reference DN Attribute	<p>The name of the attribute, in the user object, that holds a reference to an LDAP object that will maintain the EULA state (at an organization level).</p> <p>Only useful when users in an organization inherit the value of a single EULA acceptance. Otherwise leave the default value of "dn" to imply that each user will accept their own EULA.</p>	DN
Reference EULA Attribute	The name of the attribute, in the reference object, that holds the Boolean value of whether an organization has accepted or declined the EULA. If each user will accept their own EULA, then this field would be the same as the EULA Attribute.	Boolean { TRUE FALSE } A null value would be treated as FALSE.
Signer DN Attribute	The name of the attribute that holds the DN of the user that accepted the EULA. This attribute must exist on the reference object (if an organization will maintain the EULA state) or the user (if each user will accept their own EULA).	DN
Signed Timestamp Attribute	The name of the attribute that holds the date and time when the EULA was accepted. This attribute must exist on the reference object (if an organization will maintain the EULA state) or the user (if each user will accept their own EULA).	Generalized Time
EULA Content DN	The DN of the object will contain the EULA content that will be displayed.	DN

EULA Content Attribute	The name of the attribute in the EULA Content object that holds the actual verbiage of the EULA.	Directory String
EULA Template	The HTML template that will be displayed to the user.	
Send EULA via Email	A checkbox to configure whether PingFederate will send an email to the user that has accepted the EULA with the content of the EULA.	
User Display Name Attribute	The name of the attribute that contains the user's display name.	Directory String
User Email Attribute	The name of the attribute that contains the user's email address.	IA5 String
Email EULA Template	The Email template that will be sent to the user.	

LDAP Configuration

The EULA IdP Adapter supports two use cases:

1. Each user accepts the EULA

The user's EULA attribute is an LDAP Boolean attribute that is defined as an optional and single-value attribute of the user object LDAP schema. The default value is FALSE which means the user has either not accepted the EULA yet or the user declined the EULA. A null value would be treated as FALSE.

2. A user accepts the EULA on behalf of an organization

The user's EULA attribute is an LDAP Boolean attribute that is a virtual attribute generated dynamically by the LDAP directory server. The value of the virtual attribute is generated by a lookup that is performed by the LDAP directory server. In this use case, the LDAP directory server must support virtual attributes.

For PingDirectory 6.x, a virtual attribute can be created as follows:

```
dsconfig create-virtual-attribute \
  --name EulaVirtualAttrib \
  --type mirror \
  --set attribute-type:eula \
  --set enabled:true \
  --set source-attribute:eula \
  --set source-entry-dn-attribute:manager
```

In this example, a virtual attribute (called "eula") is generated by mirroring the value of an attribute of another object in the directory. In this specific case, the directory server looks up the "eula" attribute of the object that is defined in the "manager" attribute, which is a DN to another user object.

Example:

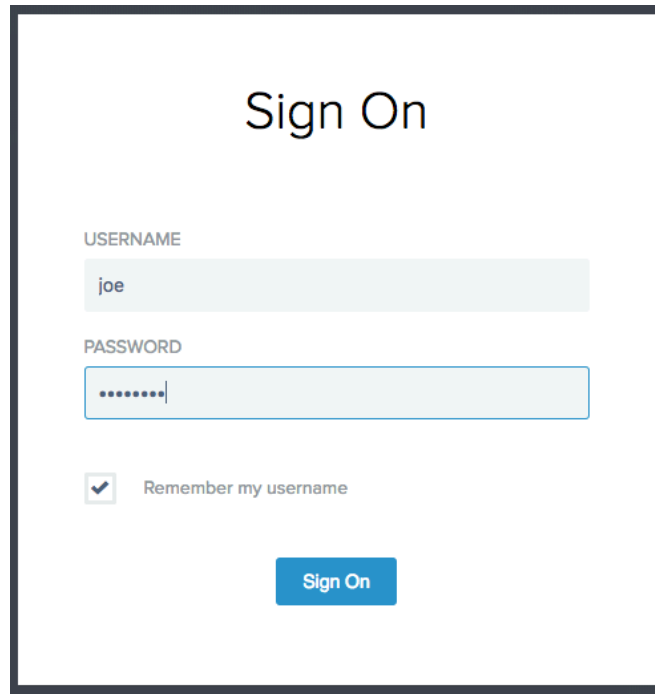
objectClass	inetOrgPerson (structural)
objectClass	organizationalPerson (structural)
objectClass	person (structural)
objectClass	posixPerson (structural)
objectClass	top (abstract)
cn	Joe Tester
sn	Tester
eula	true
manager	uid=admin,dc=example,dc=com
uid	joe
userPassword	SSHA-256 hashed password
createTimestamp	Mar 26. 2018 11:45:45 AM EDT (20180326154545.219Z)
creatorsName	cn=Directory Manager,cn=Root DNs,cn=config
ds-entr-Checksum	6168591165
entrUUID	a541faaf-56c4-4a04-9611-11cde8f94ca6
modifiersName	cn=Directory Manager,cn=Root DNs,cn=config
modifyTimestamp	Apr 10. 2018 7:58:01 AM EDT (20180410115801.866Z)
nsUniqueId	62c593db-afdc-4679-a919-d2d0d9c8615e
pwdChangedTime	Mar 27. 2018 3:31:30 PM EDT (20180327193130.330Z)
subschemaSubentry	cn=schema

Testing

Please note: For all test cases below, please make sure to log out, clear browser data, close and re-open the browser.

Test Case 1 – User Accepts EULA

1. Optional: Modify the LDAP schema by adding a Boolean attribute that will be used to hold the EULA value and add the attribute to the user object.
2. Open a browser and go to the SP connection that leverages the EULA IdP adapter.
3. Log in.

A screenshot of a 'Sign On' form. At the top, the title 'Sign On' is centered. Below it, there are two input fields: 'USERNAME' with the value 'joe' and 'PASSWORD' with masked characters '.....'. A checkbox labeled 'Remember my username' is checked. At the bottom, there is a blue 'Sign On' button.

Sign On

USERNAME

joe

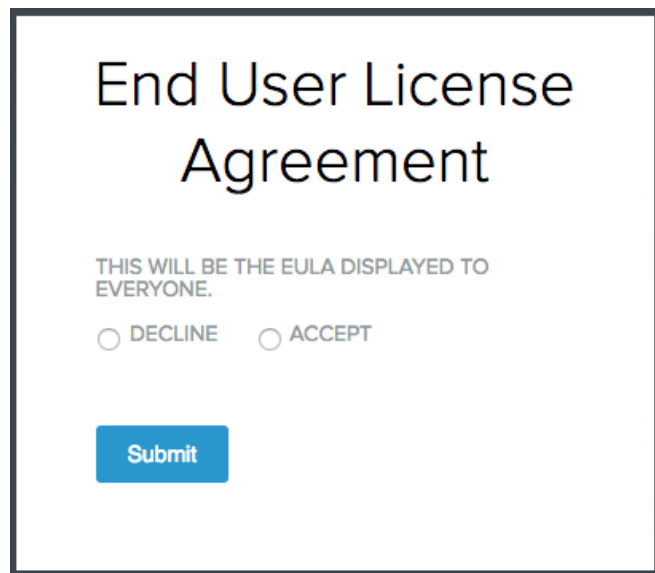
PASSWORD

.....

☒ Remember my username

Sign On

4. Accept the EULA.

A screenshot of an 'End User License Agreement' form. The title 'End User License Agreement' is centered at the top. Below it, the text 'THIS WILL BE THE EULA DISPLAYED TO EVERYONE.' is shown. There are two radio buttons: 'DECLINE' and 'ACCEPT', with 'ACCEPT' being the selected option. At the bottom, there is a blue 'Submit' button.

End User License Agreement

THIS WILL BE THE EULA DISPLAYED TO EVERYONE.

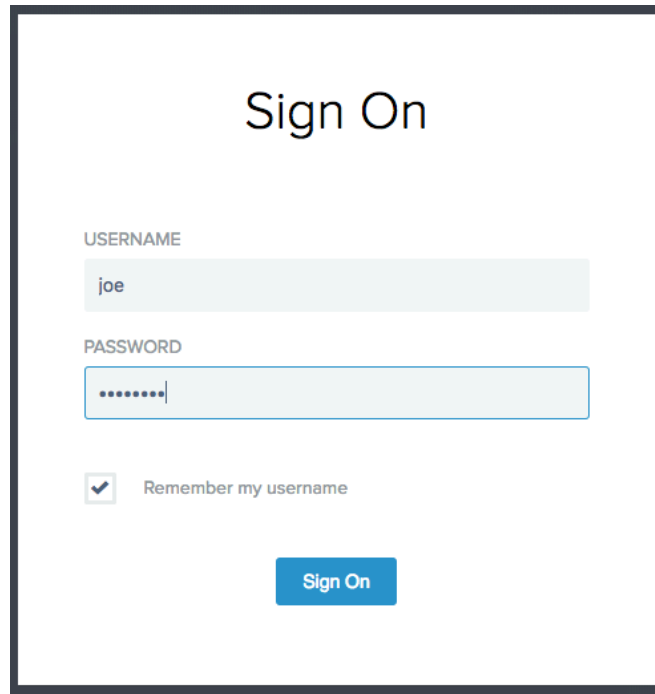
☐ DECLINE ☒ ACCEPT

Submit

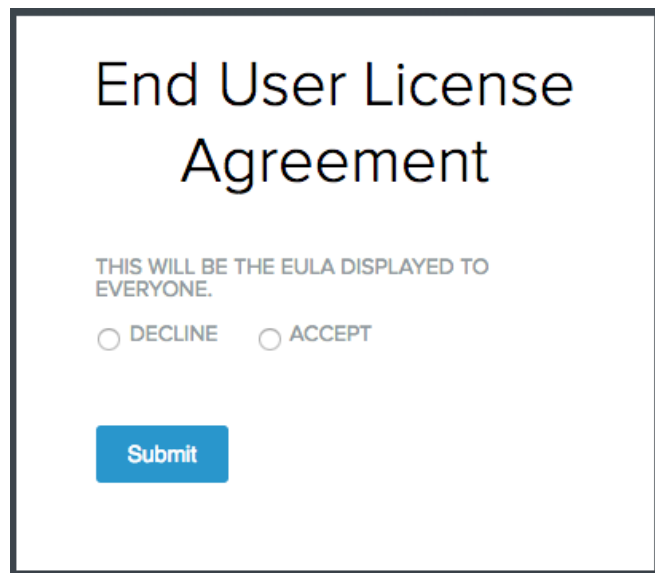
Results: User should be logged in. Perform an LDAP search query to confirm the user's EULA attribute is set to "TRUE". Repeat the steps to confirm that the EULA is not displayed again.

Test Case 2 – User Declines EULA

1. Optional: Modify the LDAP schema by adding a Boolean attribute that will be used to hold the EULA value and add the attribute to the user object.
2. Open a browser and go to the SP connection that leverages the EULA IdP adapter.
3. Log in.

A screenshot of a 'Sign On' form. At the top, the text 'Sign On' is centered. Below it, there are two input fields. The first is labeled 'USERNAME' and contains the text 'joe'. The second is labeled 'PASSWORD' and contains a series of dots. Below the password field, there is a checkbox that is checked, followed by the text 'Remember my username'. At the bottom, there is a blue button labeled 'Sign On'.

4. Decline the EULA.

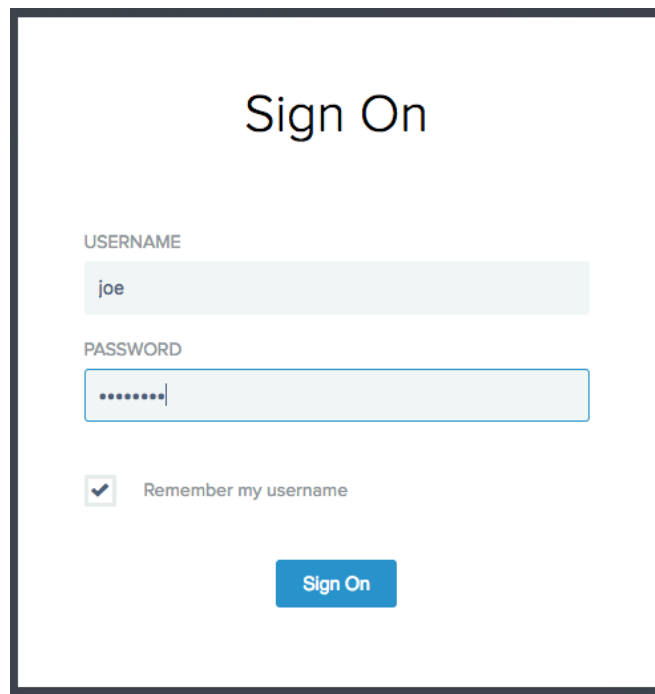
A screenshot of an 'End User License Agreement' form. The title 'End User License Agreement' is centered at the top. Below it, the text 'THIS WILL BE THE EULA DISPLAYED TO EVERYONE.' is centered. Underneath, there are two radio buttons. The first is labeled 'DECLINE' and is selected. The second is labeled 'ACCEPT'. At the bottom, there is a blue button labeled 'Submit'.

Results: User should not be logged in. Perform an LDAP search query to confirm the user's EULA attribute is set to "FALSE". Repeat the steps to confirm that the EULA is displayed again.

Test Case 3 – User Accepts EULA on behalf of an organization

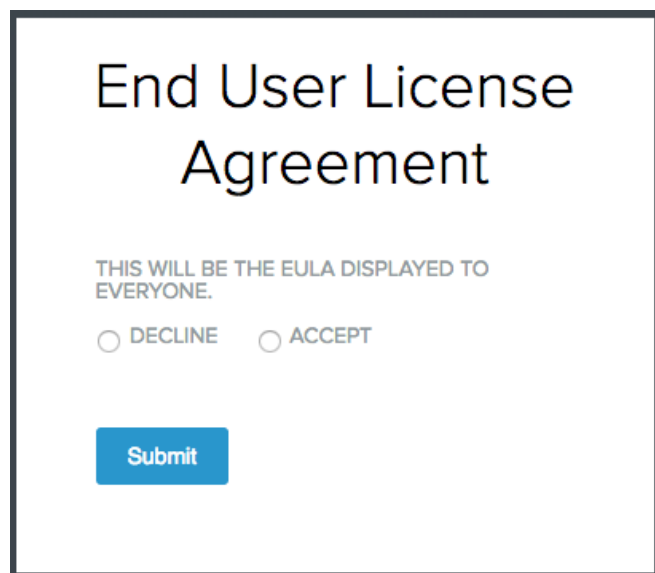
1. Optional: Modify the LDAP schema by adding a Boolean attribute that will be used to hold the EULA value and add the attribute to the LDAP object that represent the administrator.
2. Add a virtual attribute to user objects that mirrors the value of the EULA attribute in the administrator object.

3. Open a browser and go to the SP connection that leverages the EULA IdP adapter.
4. Log in.



A screenshot of a 'Sign On' web form. The title 'Sign On' is centered at the top. Below it, there are two input fields: 'USERNAME' with the text 'joe' and 'PASSWORD' with masked characters '.....'. A checkbox labeled 'Remember my username' is checked. At the bottom is a blue 'Sign On' button.

5. Accept the EULA.



A screenshot of an 'End User License Agreement' web form. The title 'End User License Agreement' is centered at the top. Below it, the text 'THIS WILL BE THE EULA DISPLAYED TO EVERYONE.' is shown. There are two radio buttons: 'DECLINE' (selected) and 'ACCEPT'. At the bottom is a blue 'Submit' button.

Results: User should be logged in. Perform an LDAP search query to confirm the administrator's EULA attribute is set to "TRUE". Any user object that is configured with the virtual attribute would show the same value. Repeat the steps to confirm that the EULA is not displayed again.

Logging

To enable various logging modes for the EULA IdP Adapter, add the following in the relevant sections in <PingFederateInstall>/pingfederate/server/default/conf/log4j2.xml.

Please note: the double quotes may need to be re-typed if copying and pasting the below. The log4j2.xml file may process the copied double quotes as foreign objects, thus creating errors upon PingFederate startup.

```
<Logger name="com.pingidentity.ps.pf.adapter.idp" level="[ DEBUG | INFO | WARN | ERROR ]" />
```

To enable logging for the EULA IdP Adapter in a separate file, add the following in the relevant sections in <PingFederateInstall>/pingfederate/server/default/conf/log4j2.xml.

```
<RollingFile name="EulaldPAdapter" fileName="${sys:pf.log.dir}/EulaldPAdapter.log"
filePattern="${sys:pf.log.dir}/EulaldPAdapter.%d{yyyy-MM-dd}.log" ignoreExceptions="false">
  <PatternLayout>
    <pattern>%d %-5p [%c{1}] %m%n</pattern>
  </PatternLayout>
  <Policies>
    <TimeBasedTriggeringPolicy />
  </Policies>
</RollingFile>

<Logger name="com.pingidentity.ps.pf.adapter.idp"
level="[ DEBUG | INFO | WARN | ERROR ]" additivity="false" includeLocation="true"/>
  <appender-ref ref="EulaldPAdapter" />
</Logger>
```

Detailed training on using Log4j in PingFederate can be found at:

<https://ping.force.com/Support/PingIdentityKnSearchHome?searchText=log4j>