

# **PingFederate®**

## **IdP Discovery Authentication Selector v1.3.0**

### **User Guide**



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

PingFederate IdP Discovery Authentication Selector User Guide  
Version 1.3.0  
February 2018

Ping Identity Corporation  
1001 17<sup>th</sup> 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](mailto: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>).

# Contents

*Purpose* .....4

*Prerequisites*.....4

*Installation*.....4

*Configuration*.....4

*Logging* .....7

# Purpose

This user guide is intended for use by PingFederate clients, with the need to provide a dynamic option to redirect users to the correct service provider for authentication based on the user's email or domain.

## Prerequisites

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

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

## Installation

1. From the `/dist` folder in *pf-idp-discovery-authentication-selector-1.3.0.zip*, copy the below noted files to the following directory in your PingFederate install.

From /dist	To <YourPFInstall>/pingfederate/server/default
pf-idp-discovery-authentication-selector-1.3.0.jar	/deploy/
/language-packs/idp-discovery-authn-selector.properties	/conf/language-packs/
/templates/idp.discovery.authn.selector.template.html	/conf/templates/

2. Repeat step 1 on all clustered engine nodes.
3. Start or restart PingFederate.

## Configuration

### *Configuring the IdP Discovery Authentication Selector*

1. Log into the PingFederate Administrator web console.
2. Go to either **SP Configuration** or **IdP Configuration** >> **Authentication Policies** >> **Selectors**.
3. Click the **Create New Instance** button.
4. Enter the **Instance Name**, **Instance ID**, and select the **IdP Discovery Authentication Selector 1.3.0** as the **Type**.

**Ping** Identity **PingFederate**

MAIN

IdP Identity Provider

SP Service Provider

OA OAuth Server

SETTINGS

Server Configuration

### Manage Authentication Selector Instances | Create Authentication Selector Instance

Type Authentication Selector Selector Result Values Summary

These values identify the Authentication Selector Instance.

INSTANCE NAME IdPDiscoveryAuthnSele

INSTANCE ID IdPDiscoveryAuthnSele

TYPE IdP Discovery Authentication Selector 1.3.0

Cancel Next

5. Click **Next**.

6. Enter the **Cookie Name** and adjust field values if necessary, and click **Next**.

**Ping** Identity **PingFederate**

MAIN

IdP IdP Configuration

SP SP Configuration

OA OAuth Settings

Server Configuration

### Manage Authentication Selector Instances | Create Authentication Selector Instance

Type Authentication Selector Selector Result Values Summary

Complete the configuration needed for this Selector Instance.

IdP Discovery Authentication Selector

Field Name	Field Value	Description
EMAIL ADDRESS OR DOMAIN NAME TEMPLATE	idp.discovery.authn.selector.template.htn	HTML template (i.e., idp.discovery.authn.selector.template.html) to render when a user is expected to provide an email address or a domain name. If the a email address is provided, a domain will be extracted from the input email address. An attempt will be made to match the extracted domain with a Selector Result Value hence resulting in the mapped authentication source.
COOKIE NAME	IdPDiscoveryDomain	Name of the cookie which saves the domain name. Once the email address or domain name is provided, upon successful authentication (or login), a cookie will be saved with this name.
COOKIE AGE	30	Number of days that the domain name is stored as a cookie in the browser. The cookie age is reset upon each successful login.

Cancel Previous Next Done

7. Add the domains in **lowercase** as the **Result Values**, and click **Next**.

PingFederate®

MAIN

IdP Identity Provider

SP Service Provider

AS OAuth Server

SETTINGS

Server Configuration

Manage Authentication Selector Instances | Create Authentication Selector Instance

Type Authentication Selector Selector Result Values Summary

Specify expected result values. Each result value will be mapped to an appropriate Authentication Source.

Core Contract

Default

Result Values	Action
acme.com	<a href="#">Edit</a>   <a href="#">Delete</a>
pingidentity.com	<a href="#">Edit</a>   <a href="#">Delete</a>

Cancel

Previous

Next

8. Review the configuration, and click **Done**.

PingFederate®

MAIN

IdP Identity Provider

SP Service Provider

AS OAuth Server

SETTINGS

Server Configuration

Manage Authentication Selector Instances | Create Authentication Selector Instance

Type Authentication Selector Selector Result Values Summary

Summary information.

Create Authentication Selector Instance

Type

Instance Name	IdPDiscoveryAuthnSelector
Instance ID	IdPDiscoveryAuthnSelector
Type	IdP Discovery Authentication Selector 1.3.0
Class Name	com.pingidentity.clientservices.product.idpdiscovery.IdPDiscoveryAuthenticationSelector

Authentication Selector

Email Address or Domain Name Template	idp.discovery.authn.selector.template.html
Cookie Name	IdPDiscoveryDomain
Cookie Age	30

Selector Result Values

Attribute	Default
Attribute	acme.com
Attribute	pingidentity.com

Cancel

Previous

Done

9. Click **Save**.

10. Go to either **SP Configuration** or **IdP Configuration >> Authentication Policies >> Policies**.
11. Configure the IdP Discovery Authentication Selector according to the desired flow.
12. Enable both or either the SP or IdP Authentication Policies according to the desired flow.  
Please note that error handling for invalid domains is configurable by configuring an Action for the "Default" result.

## Manage Authentication Policies

Authentication policies define how PingFederate authenticates users. Selectors and authentication sources can be conditionally chained together in paths to form policies. Ensure that successful paths end with authentication policy contracts to reuse mapping configuration across protocols and applications.

☒ ENABLE IDP AUTHENTICATION POLICIES

☐ ENABLE SP AUTHENTICATION POLICIES

☐ FAIL IF POLICY ENGINE FINDS NO AUTHENTICATION SOURCE

Action	Result	Action
<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">IdPDiscoveryAuthnSelector - (Select</div> <span style="margin: 0 5px;">×</span>	acme.com	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Select</div> <div style="text-align: right;">▼</div> <div style="color: #007bff; font-size: small;">Continue</div>
	Default	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Select</div> <div style="text-align: right;">▼</div> <div style="color: #007bff; font-size: small;">Continue</div>
	pingidentity.com	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Select</div> <div style="text-align: right;">▼</div> <div style="color: #007bff; font-size: small;">Continue</div>

## Logging

To enable various logging modes for the IdP Discovery Authentication Selector, 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.clientservices.product.idpdiscovery" level="[ DEBUG |
INFO | WARN | ERROR ]" />
```

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

```
<RollingFile name="IdPDiscoveryAuthnSelector"
fileName="${sys:pf.log.dir}/idpdiscoveryauthnselector.log"
filePattern="${sys:pf.log.dir}/idpdiscoveryauthnselector.%d{yyyy-MM-dd}.log"
ignoreExceptions="false">
  <PatternLayout>
    <!-- Uncomment this if you want to use UTF-8 encoding instead of system's
    default encoding.
```

```
        <charset>UTF-8</charset> -->
        <pattern>%d %m%n</pattern>
    </PatternLayout>
    <Policies>
        <TimeBasedTriggeringPolicy />
    </Policies>
</RollingFile>

<Logger name="com.pingidentity.clientservices.product.idpdiscovery"
level="[ DEBUG | INFO | WARN | ERROR ]" additivity="false" includeLocation="true">
    <appender-ref ref="IdPDiscoveryAuthnSelector" />
</Logger>
```

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

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