Ping Identity™

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 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 Iogo, 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	
Installation	
Configuration	4
Logging	

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.

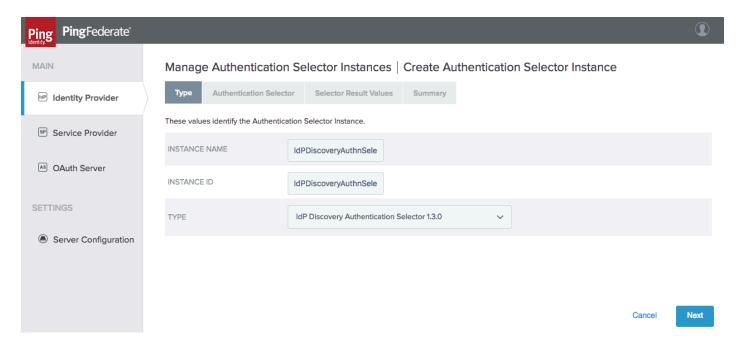
From /dist	To <yourpfinstall>/pingfederate/server/default</yourpfinstall>
pf-idp-discovery-authentication-selector-1.3.0.jar	/deploy/
/language-packs/idp-discovery-authn-selector.properties	/conf/language-packs/
/templates/idp.discovery.authn.selector.template.html	/conf/templates/

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

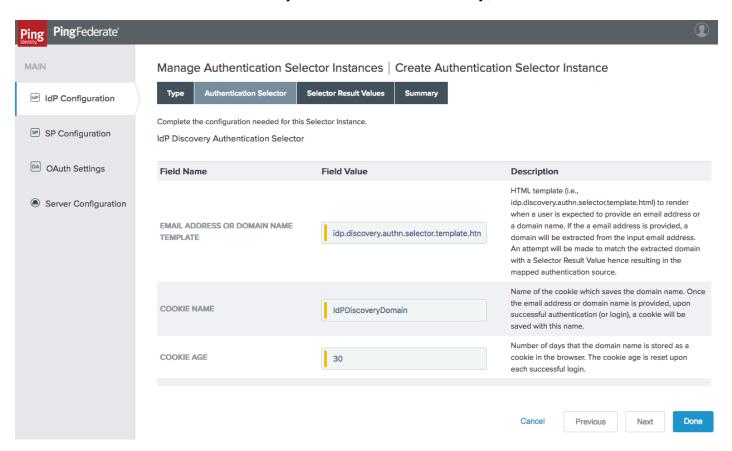
Configuration

Configuring the IdP Discovery Authentication Selector

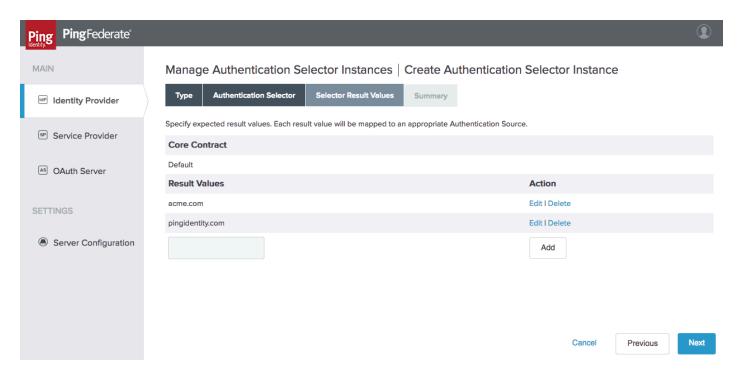
- 1. Log into the PingFederate Administrator web console.
- 2. Go to either SP Configuration or IdP Configuration >> Authentication Policies >> Selectors.
- 3. Click the Create New Instance button.
- 4. Enter the Instance Name, Instance ID, and select the IdP Discovery Authentication Selector 1.3.0 as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



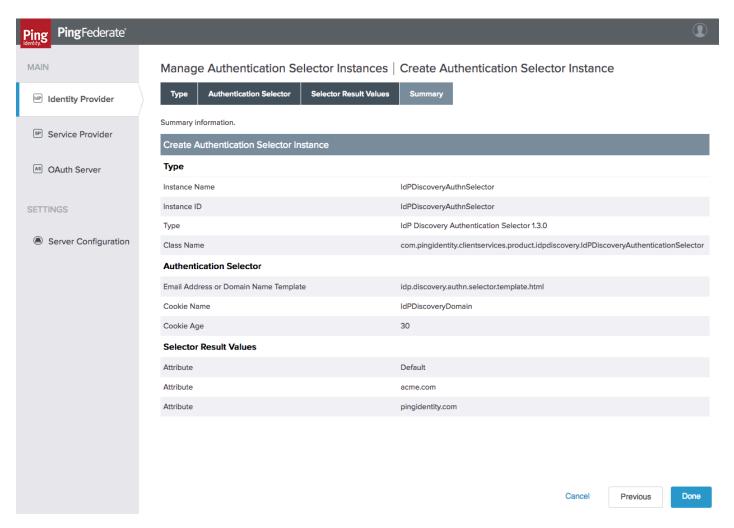
- 5. Click Next.
- 6. Enter the Cookie Name and adjust field values if necessary, and click Next.



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



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

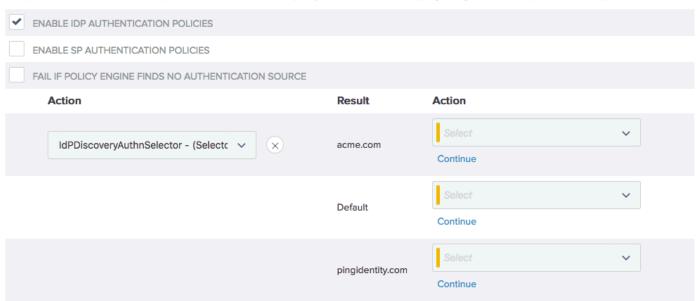


9. Click Save.

- 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.



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.

<u>Please note</u>: the double quotes may need to be re-typed if copying and pasting the below. The log42j.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.</pre>
```

Detailed training on using Log4j in PingFederate can be found at: https://ping.force.com/Support/PingIdentityKnbSearchHome?searchText=log4j