Ping Identity™

# PingFederate®

## ISAM Web SP Adapter v1.1.2

## User Guide

PingFederate ISAM Web SP Adapter User Guide
Version 1.1.2
July 2017

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**


**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

The PingFederate ISAM Web SP Adapter adds a new service provider (SP) integration option to PingFederate. ISAM/TAM provides an External Authentication Interface (EAI) that enables the extension of the authentication process for WebSEAL. The integration to ISAM/TAM is based on EAI.

When using EAI, the authentication operation is performed externally to WebSEAL by PingFederate (set up as a junctioned server). The PingFederate ISAM Web SP Adapter will return identity information extracted from the inbound SAML assertion in specially named HTTP response headers.

This document is intended for system administrations with experience in the configuration and maintenance of a PingFederate server. Please consult the PingFederate documentation if encountering any difficulties in areas that are not directly associated with the PingFederate ISAM Web SP Adapter.

# Prerequisites

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

- A functional PingFederate environment, version 8.3.3.0+
- JDK version 8+
- ISAM/TAM environment using WebSEAL as a reverse proxy

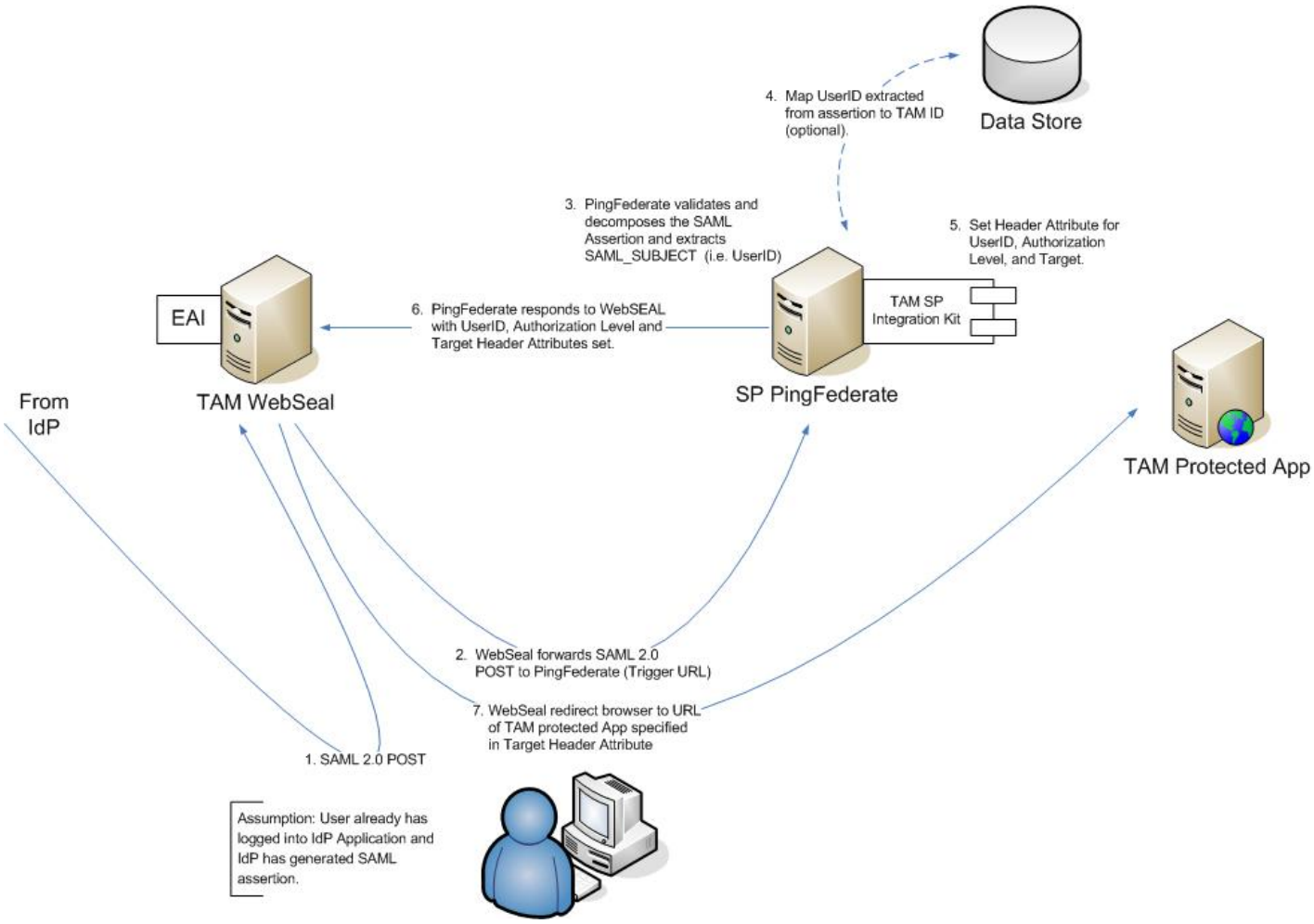
# Installation

1. From the /dist folder in *pf-isam-web-sp-adapter-1.1.2.zip*, copy the noted files to the following directory in your PingFederate:
   - <PingFederateInstall>/pingfederate/server/default/deploy/
     - pf-isam-web-sp-adapter-1.1.2.jar
     - ldap-lookup-plugin-1.0.0.jar

   Note: For upgrades, remove any older *pf-isam-web-sp-adapter* jar files.
2. Repeat step 1 on other clustered engine nodes.
3. Restart PingFederate.

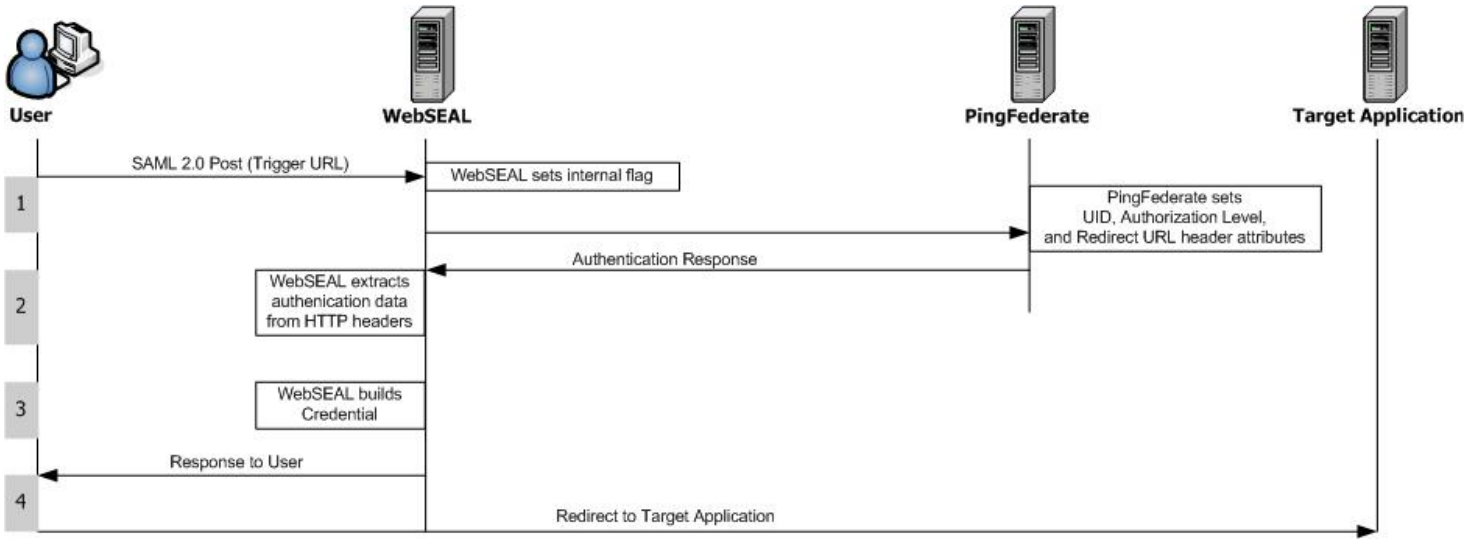
# Architecture

The following figure illustrates the architecture of ISAM/TAM solution.




# Sequence Flow Diagram

The sequence flow diagram for an SP-init SSO process can be found in the figure below.




1. SAML 2.0 Post is sent from IdP to the Assertion Consumer Service (ACS) on PingFederate.

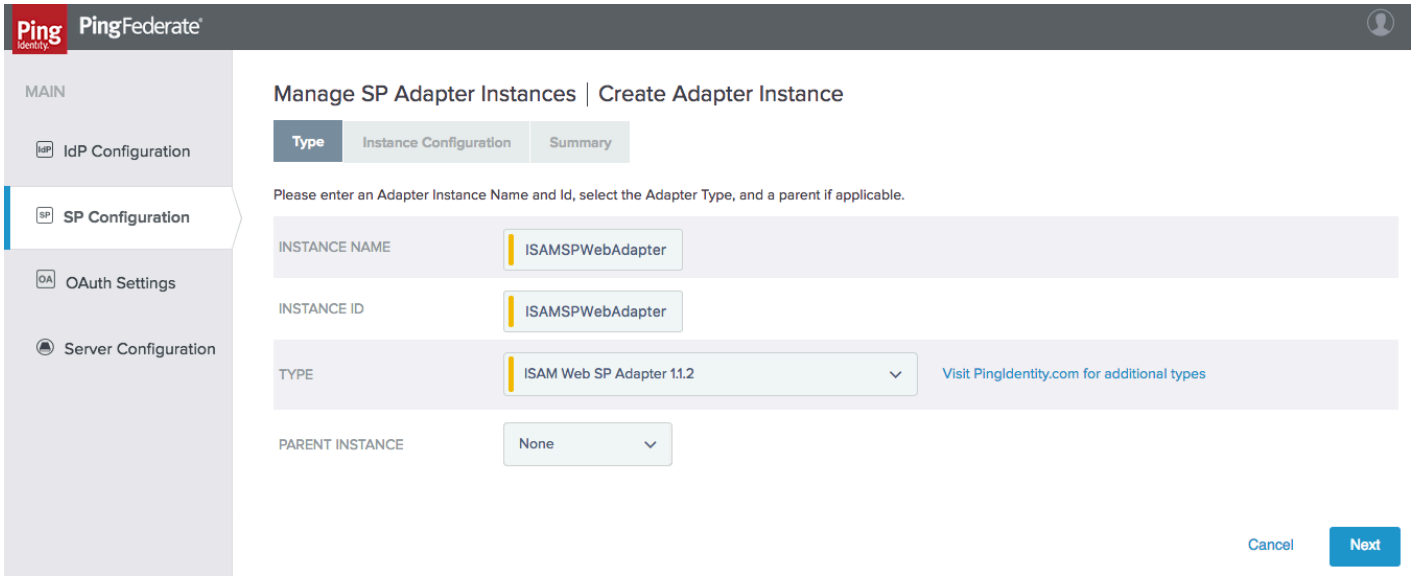
a. This ACS URL (https://[pf-server-name:port]/sp/ACS.saml2) acts as the trigger URL.
b. The recognition of the trigger URL in the request causes WebSEAL to look for authentication data in the corresponding response.
c. PingFederate will process the assertion and extract the SAML_SUBJECT (i.e. userId) and the Relay State (URL of Target Application).
d. PingFederate will then set UID, Authorization Level, and Redirect URL header attributes and respond to WebSEAL

2. WebSEAL examines the corresponding response and finds the authentication data in the HTTP headers.
3. WebSEAL uses the authentication data to build a credential for the user.
4. WebSEAL sends a response to the user and redirects the browser the location specified by that target URL specified in the header.

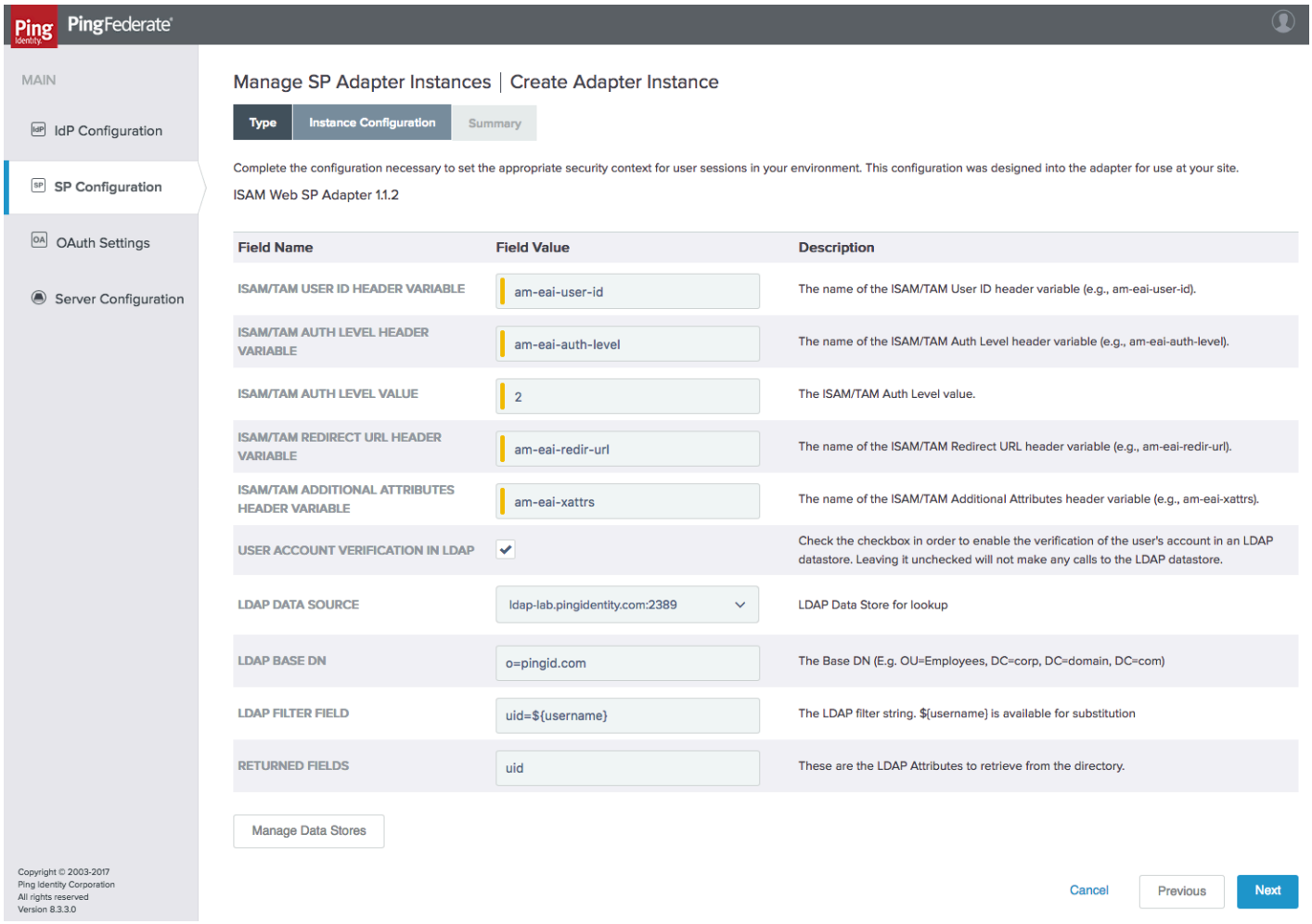
# Configuration

### *Configuring the SP Adapter*

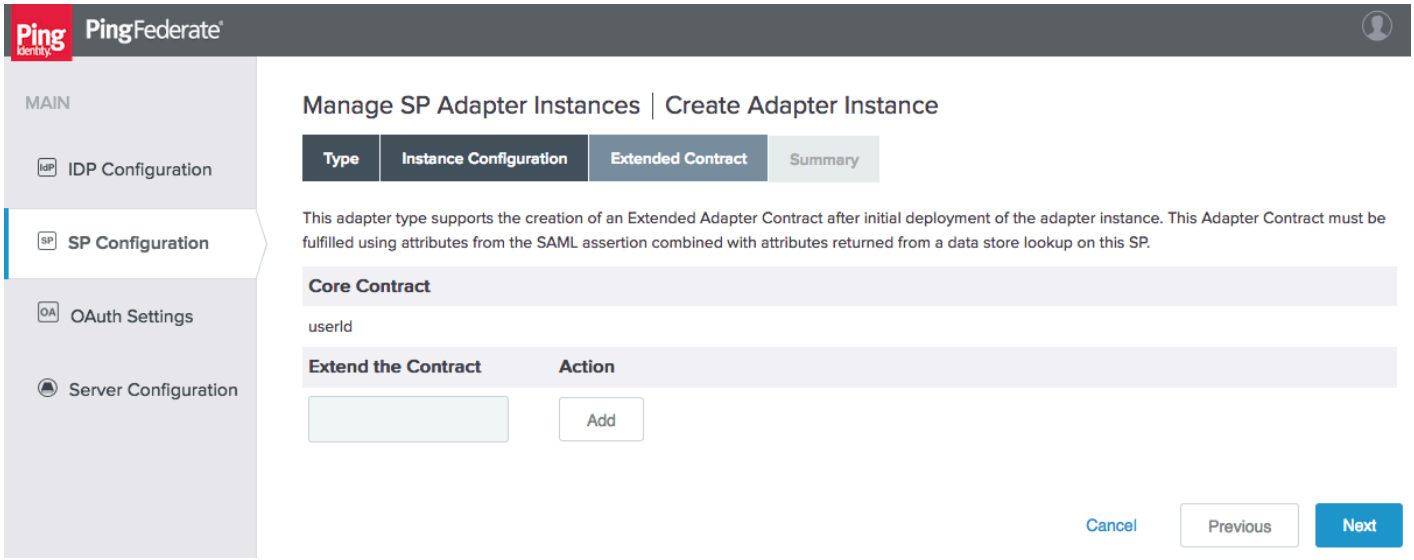
1. Log on to the PingFederate administrative console and click **Adapters** under **SP Configuration** >> **Application Integration Settings**.
2. Click **Create New Instance**...
3. Enter the **Instance Name**, **Instance Id**, and choose ISAM Web SP Adapter 1.1.2 as the **Type**. Then click **Next**.



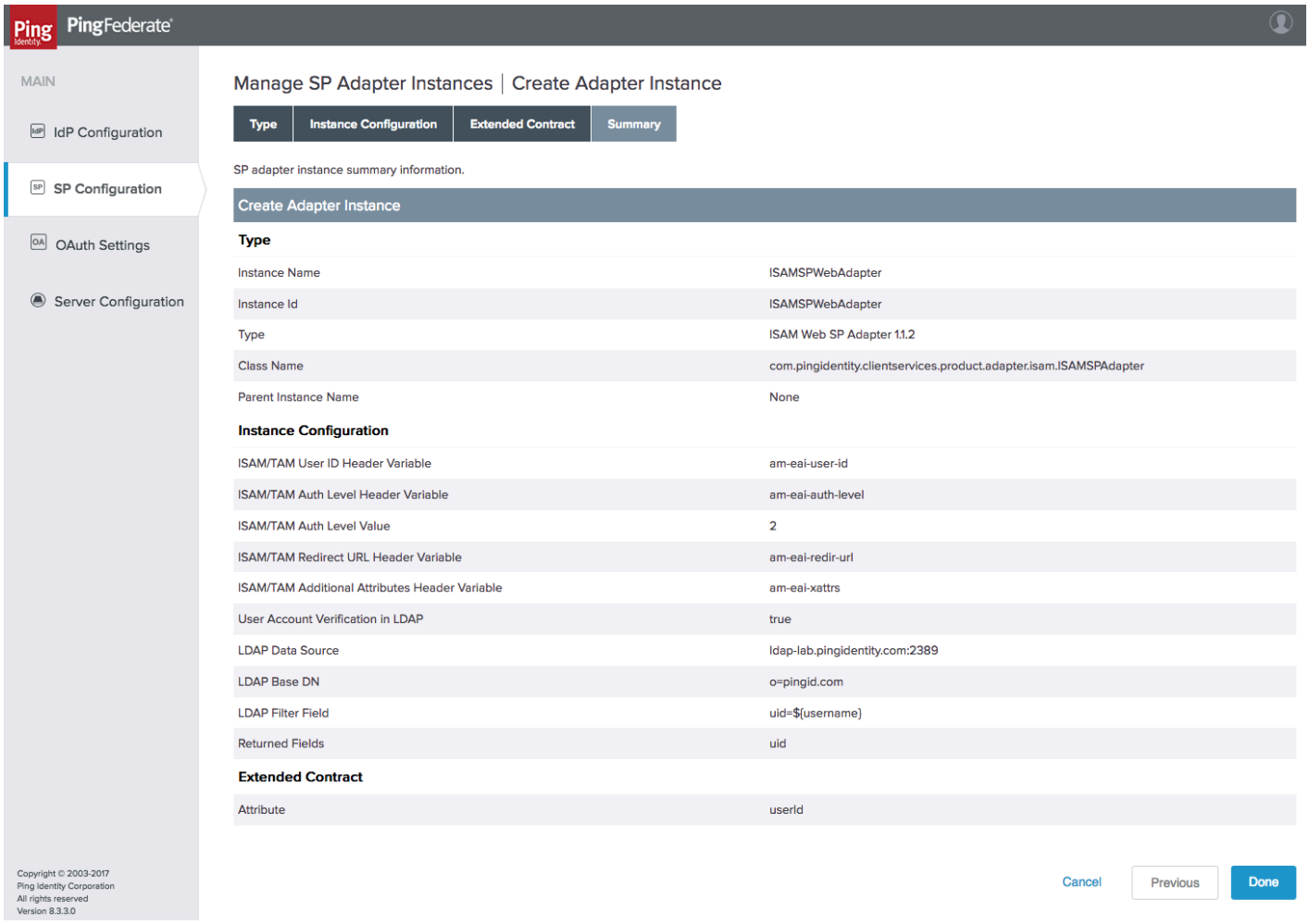

4. Enter the appropriate values for the configuration and click **Next**.




5. Add any additional attributes to the contract if needed. Otherwise, click **Next**.




6. On the summary screen, verify that the information is correct, and click **Done**.




7. Click **Save** to complete the adapter configuration.

## *Enabling the WebSEAL External Authentication Interface (EAI)*

1. Enable the WebSEAL EAI.

   The eai-auth stanza entry, located in the [eai] stanza of the WebSEAL configuration file, enables and disables the external authentication interface functionality. The external authentication interface can be implemented over HTTP, HTTPS, or both. It is highly recommended that you use HTTPS in production.

   To configure the external authentication interface:
   1. Stop the WebSEAL server.
   2. Edit the WebSEAL configuration file. In the [eai] stanza, specify the protocols to support in your network environment.
      The protocols are as follows:

| Protocol to Support | Configuration File Entry |
|---|---|
| HTTP | eai-auth = http |

| | |
|---|---|
| HTTPS (recommended) | eai-auth = https |
| Both HTTP and HTTPS | eai-auth = both |
| Disable external authentication interface | eai-auth = none |

3. Restart the WebSEAL server.

2. Configure the external authentication interface trigger URL .

   The external authentication interface authentication process allows for multiple request-response exchanges. For efficiency and the security of the WebSEAL server, these exchanges are normally streamed through WebSEAL. WebSEAL intercepts this exchange only when there is an occurrence of a special "trigger URL" in a request.

   A trigger URL is a server-relative or absolute URL string configured in the WebSEAL configuration file. The trigger URL usually requests authentication from the external authentication application. For example, the trigger URL could be the URL to the external authentication application located in a special link on a customized login page.

   When WebSEAL detects the trigger URL in a request, WebSEAL intercepts the corresponding response and examines it for authentication data located in special HTTP headers.

   Use the trigger stanza entry, **located in the [eai-trigger-urls] stanza of the WebSEAL configuration file** to specify one or more trigger URL strings.

   The trigger URL should be configured as follows:

   ***[eai-trigger-urls]***

   ***trigger = http://[pf-server-name:port]/sp/ACS.saml2***

3. Specify HTTP header names for authentication data.

   You must specify the names of the HTTP headers that contain the authentication data returned from the external authentication application. Please confirm that the headers are configured as follows in the WebSEAL configuration file:

   ***[eai]***
   ***eai-user-id-header = am-eai-user-id***
   ***eai-auth-level-header = am-eai-auth-level***
   ***eai-redir-url-header = am-eai-redir-url***

4. Configure the external authentication interface mechanism

   The built-in eaiauthn module is used to process the authentication data found in the special HTTP headers. After WebSEAL extracts the authentication data from the headers in the response, the data is passed to the eaiauthn module.

| Operation System | Module |
|---|---|
| Solaris | libeaiauthn.so |
| AIX | libeaiauthn.a |
| HPUX | libeaiauthn.sl |
| Linux | libeaiauthn.so |
| Windows | libeaiauthn.dll |

You can configure the external authentication interface authentication mechanism by entering the ext-auth-interface stanza entry with the platform-specific name of the shared library file in the [authentication-mechanism] stanza of the WebSEAL configuration file. For example, on Windows it would be configured as follows:

***[authentication-mechanisms] ext-auth-interface = eaiauthn.dll***

# Testing

1. Open a browser and go to the ISAM/TAM application and login with valid credentials.
   Results: The user should be able to login successfully.

2. Repeat the primary test case as defined above in a new browser session, but with invalid credentials.
   Results: The user should not be able to login successfully.

3. Repeat the primary test case as defined above, but in the same browser session.
   Results: The user should login successfully and seamlessly (will not need to re-enter valid credentials).

# Logging

To enable logging in a separate log file (isamwebspadapter.log) for the ISAM Web SP Adapter, add the following to <PingFederateInstall>/pingfederate/server/default/conf/log4j2.xml (make sure a backup is made of this file prior to editing):

```
<!-- ISAM Web SP Adapter log : A time/date based rolling appender -->
<RollingFile name="ISAMWebSPAdapter" fileName="${sys:pf.log.dir}/isamwebspadapter.log"
   filePattern="${sys:pf.log.dir}/isamwebspadapter.%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.adapter.isam" level="DEBUG"
additivity="false" includeLocation="false">
        <appender-ref ref="ISAMWebSPAdapter" />
    </Logger>
```

The ‘isamwebspadapter.log’ will be created in <PingFederateInstall>/pingfederate/log upon usage.

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