PingFederate®

Absorb Password Credential Validator v1.0.0

User Guide

PingFederate Absorb Password Credential Validator User Guide
Version 1.0.0
January 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

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

This user guide is intended for use by PingFederate clients, who would like the ability to leverage a password credential validator that can validate credentials via a web service call against the Absorb RESTful API.

Prerequisites

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

- A functional PingFederate environment, version 8.3+
- JDK version 8+
- At least one IdP adapter for use as the primary form of authentication (i.e., HTML Form IdP Adapter), so that it can be configured to leverage the Absorb Password Credential Validator (PCV)
- At least one SP connection that can be configured with that IdP adapter as a primary form of authentication

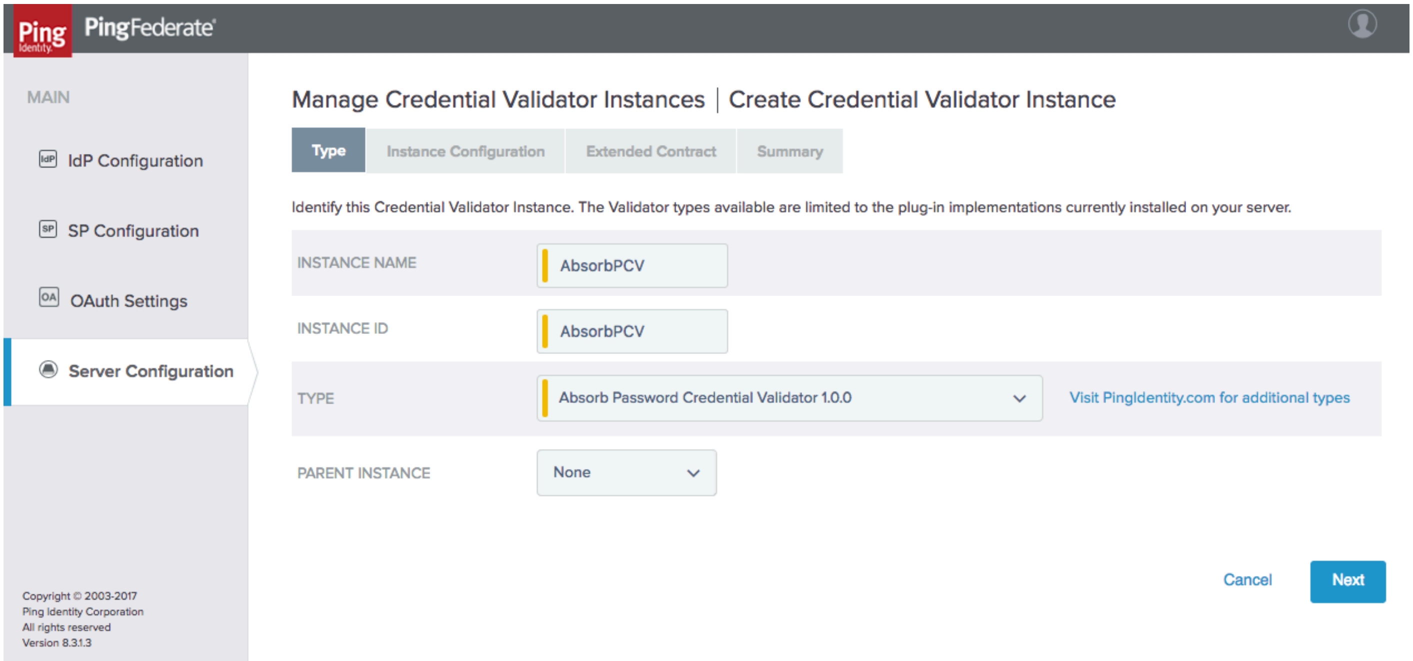
Installation

1. From the /dist folder in *pf-absorb-password-credential-validator-1.0.0.zip*, copy the noted file to the following directory in your PingFederate:
    - <PingFederateInstall>/pingfederate/server/default/deploy/
        - pf-absorb-password-credential-validator-1.0.0.jar
2. Repeat step 1 on other clustered engine nodes.
3. Start or restart PingFederate.

Configuration

Configuring the Absorb Password Credential Validator

1. Log into the PingFederate admin console and click **Password Credential Validators** under **Server Configuration** >> **Authentication**.
2. Click **Create New Instance…**
3. Enter the **Instance Name**, **Instance Id**, choose **Absorb Password Credential Validator 1.0.0**, and click **Next**.



Manage Credential Validator Instances | Create Credential Validator Instance

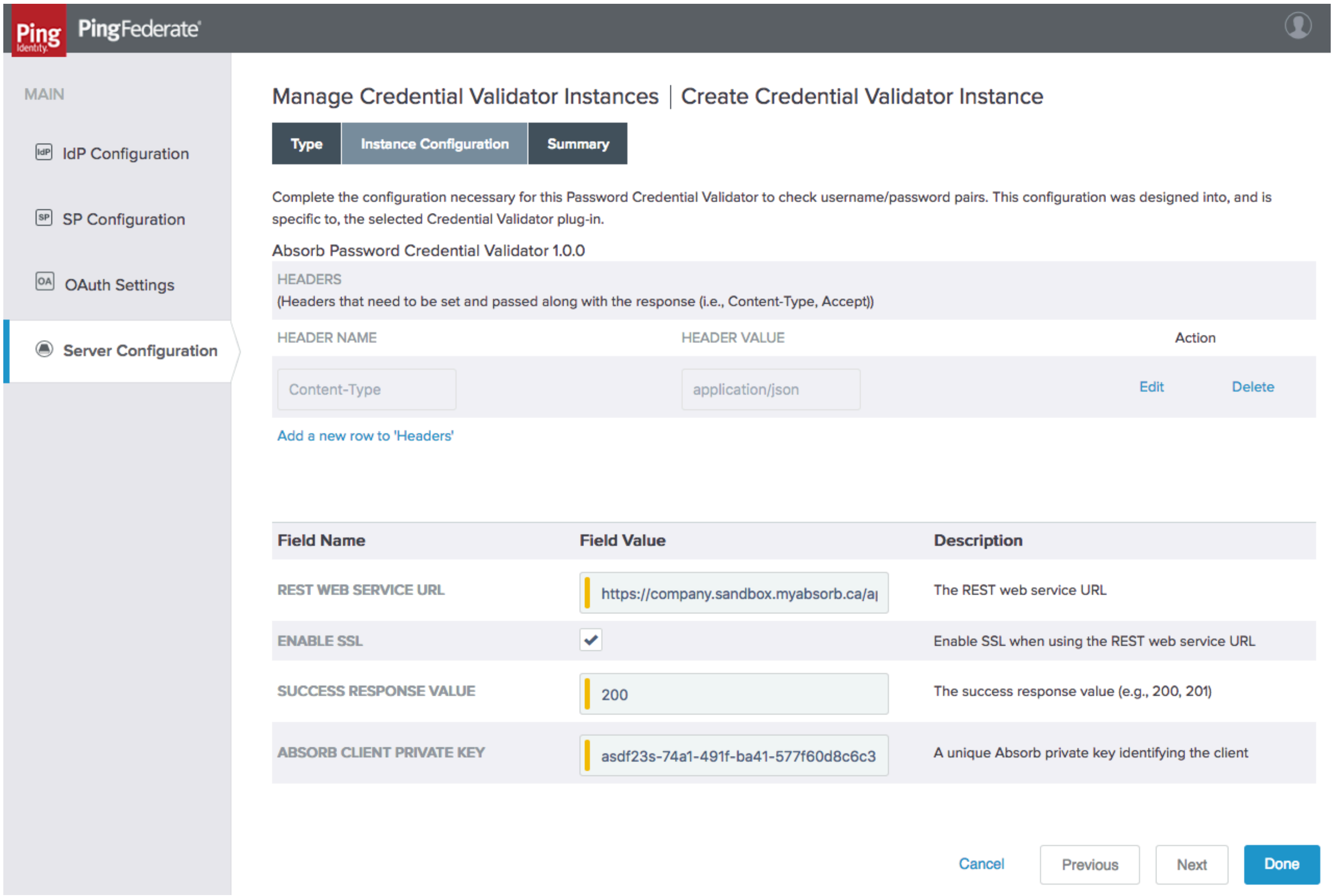
Identify this Credential Validator Instance. The Validator types available are limited to the plug-in implementations currently installed on your server.

INSTANCE NAME	AbsorbPCV
INSTANCE ID	AbsorbPCV
TYPE	Absorb Password Credential Validator 1.0.0
PARENT INSTANCE	None

Visit PingIdentity.com for additional types

Copyright © 2003-2017
Ping Identity Corporation
All rights reserved
Version 8.3.1.3

4. Enter the required information, and click **Next**.



Manage Credential Validator Instances | Create Credential Validator Instance

Complete the configuration necessary for this Password Credential Validator to check username/password pairs. This configuration was designed into, and is specific to, the selected Credential Validator plug-in.

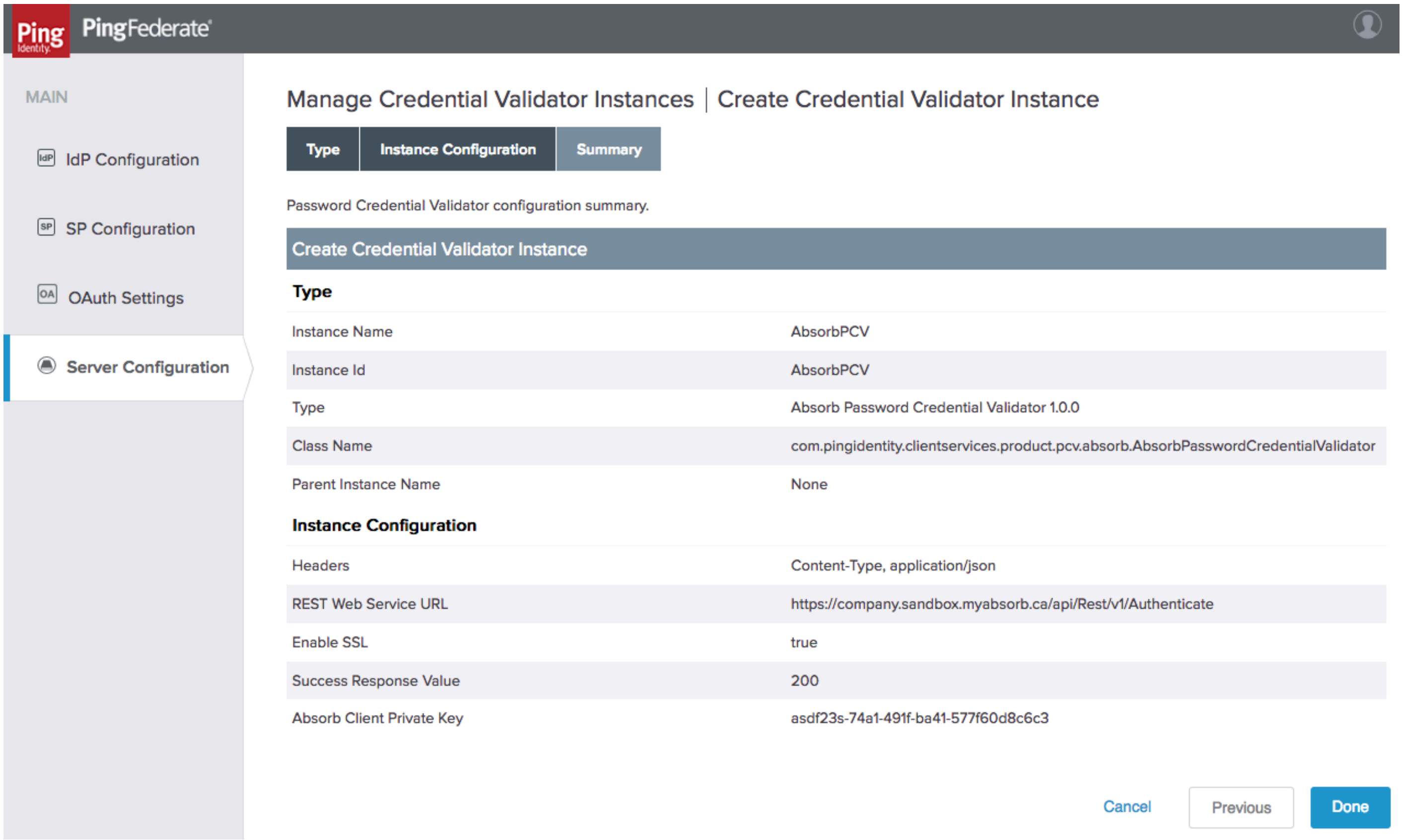
Absorb Password Credential Validator 1.0.0

HEADERS
(Headers that need to be set and passed along with the response (i.e., Content-Type, Accept))

HEADER NAME	HEADER VALUE	Action
Content-Type	application/json	Edit Delete

Field Name	Field Value	Description
REST WEB SERVICE URL	https://company.sandbox.myabsorb.ca/a|	The REST web service URL
ENABLE SSL	✓	Enable SSL when using the REST web service URL
SUCCESS RESPONSE VALUE	200	The success response value (e.g., 200, 201)
ABSORB CLIENT PRIVATE KEY	asdf23s-74a1-491f-ba41-577f60d8c6c3	A unique Absorb private key identifying the client

5. Review the configuration on the summary page, and click **Done**.



Manage Credential Validator Instances | Create Credential Validator Instance

Password Credential Validator configuration summary.

Create Credential Validator Instance

Type

Instance Name	AbsorbPCV
Instance Id	AbsorbPCV
Type	Absorb Password Credential Validator 1.0.0
Class Name	com.pingidentity.clientservices.product.pcv.absorb.AbsorbPasswordCredentialValidator
Parent Instance Name	None

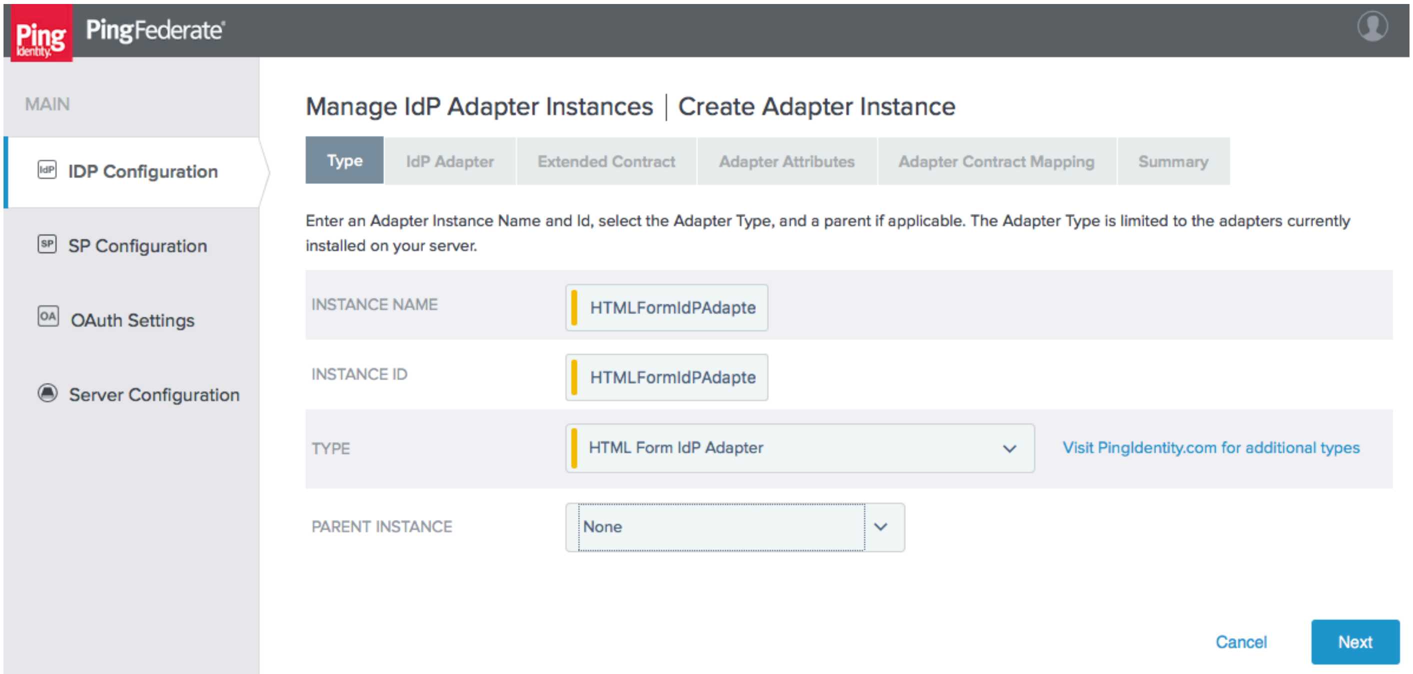
Instance Configuration

Headers	Content-Type, application/json
REST Web Service URL	https://company.sandbox.myabsorb.ca/api/Rest/v1/Authenticate
Enable SSL	true
Success Response Value	200
Absorb Client Private Key	asdf23s-74a1-491f-ba41-577f60d8c6c3

6. Click **Save**.

Configuring an IdP Adapter to Leverage the Absorb Password Credential Validator

1. Click **Adapters** under **IdP Configuration >> Application Integration Settings**.
2. Click **Create New Instance…**
3. Enter the **Instance Name** and **Instance Id**, choose the adapter type (e.g., HTML Form IdP Adapter), and click **Next**.



Manage IdP Adapter Instances | Create Adapter Instance

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.

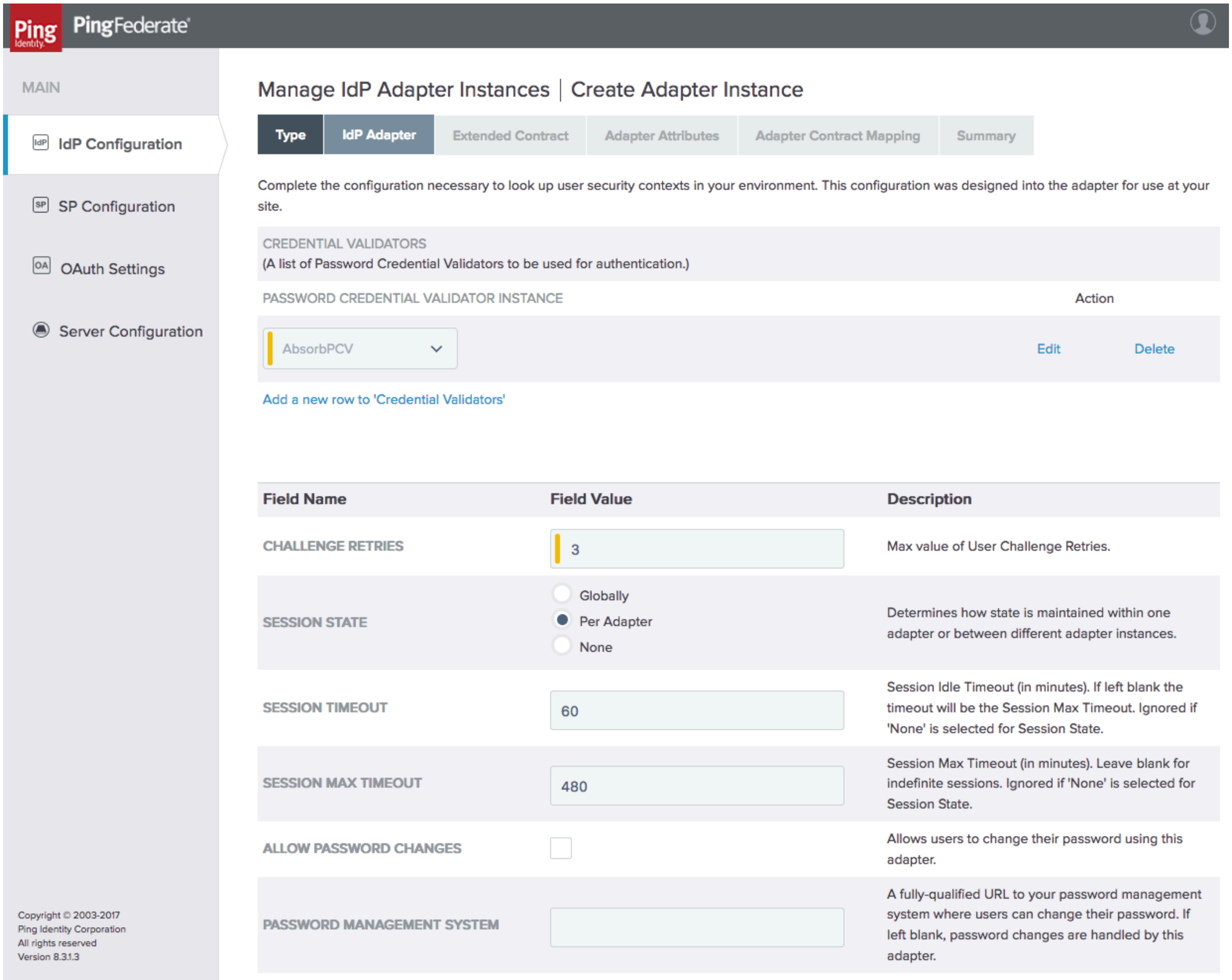
INSTANCE NAME: HTMLFormIdPAdapte

INSTANCE ID: HTMLFormIdPAdapte

TYPE: HTML Form IdP Adapter

PARENT INSTANCE: None

4. Click **Add a new row to ‘Credential Validators.’**
5. Select the Absorb Password Credential Validator created, and click **Update** (should change to **Edit** after updated).



Manage IdP Adapter Instances | Create Adapter Instance

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.

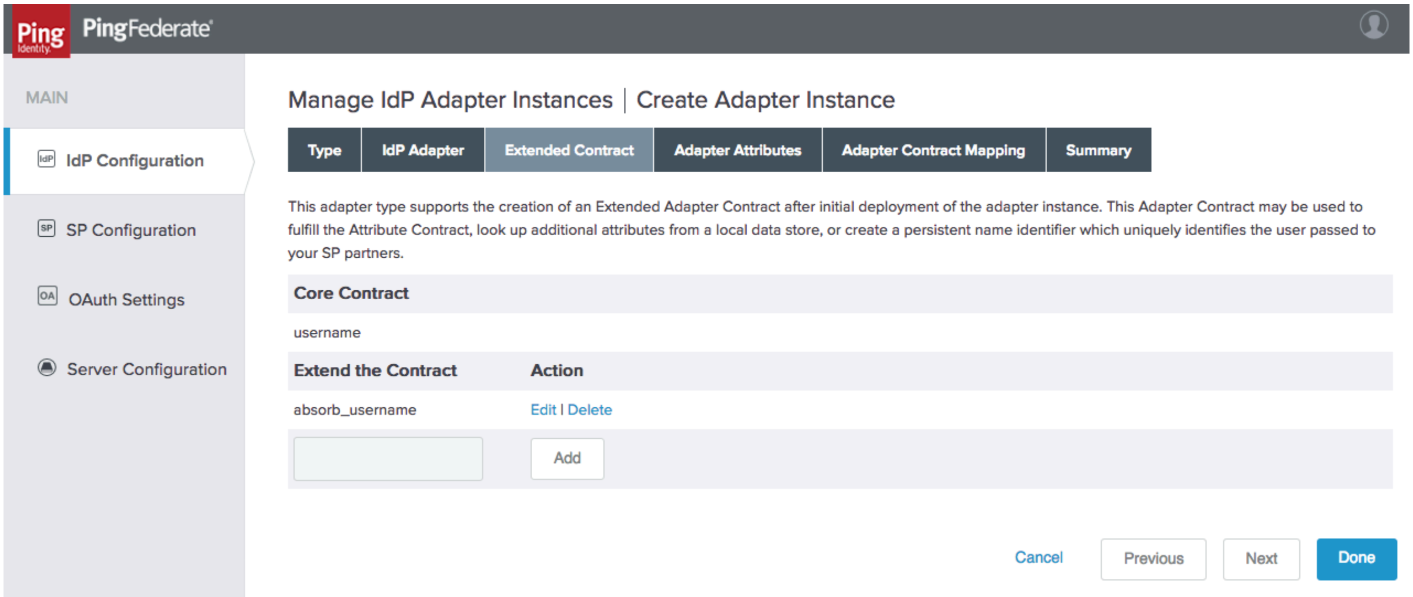
CREDENTIAL VALIDATORS
(A list of Password Credential Validators to be used for authentication.)

PASSWORD CREDENTIAL VALIDATOR INSTANCE	Action	
AbsorbPCV	Edit	Delete

Add a new row to 'Credential Validators'

Field Name	Field Value	Description
CHALLENGE RETRIES	3	Max value of User Challenge Retries.
SESSION STATE	○ Globally ● Per Adapter ○ None	Determines how state is maintained within one adapter or between different adapter instances.
SESSION TIMEOUT	60	Session Idle Timeout (in minutes). If left blank the timeout will be the Session Max Timeout. Ignored if 'None' is selected for Session State.
SESSION MAX TIMEOUT	480	Session Max Timeout (in minutes). Leave blank for indefinite sessions. Ignored if 'None' is selected for Session State.
ALLOW PASSWORD CHANGES	□	Allows users to change their password using this adapter.
PASSWORD MANAGEMENT SYSTEM		A fully-qualified URL to your password management system where users can change their password. If left blank, password changes are handled by this adapter.

6. Modify the other configuration parameters on that page if needed, and click **Next**.
7. Extend the contract by adding **absorb_username,** and click **Next**.



Manage IdP Adapter Instances | Create Adapter Instance

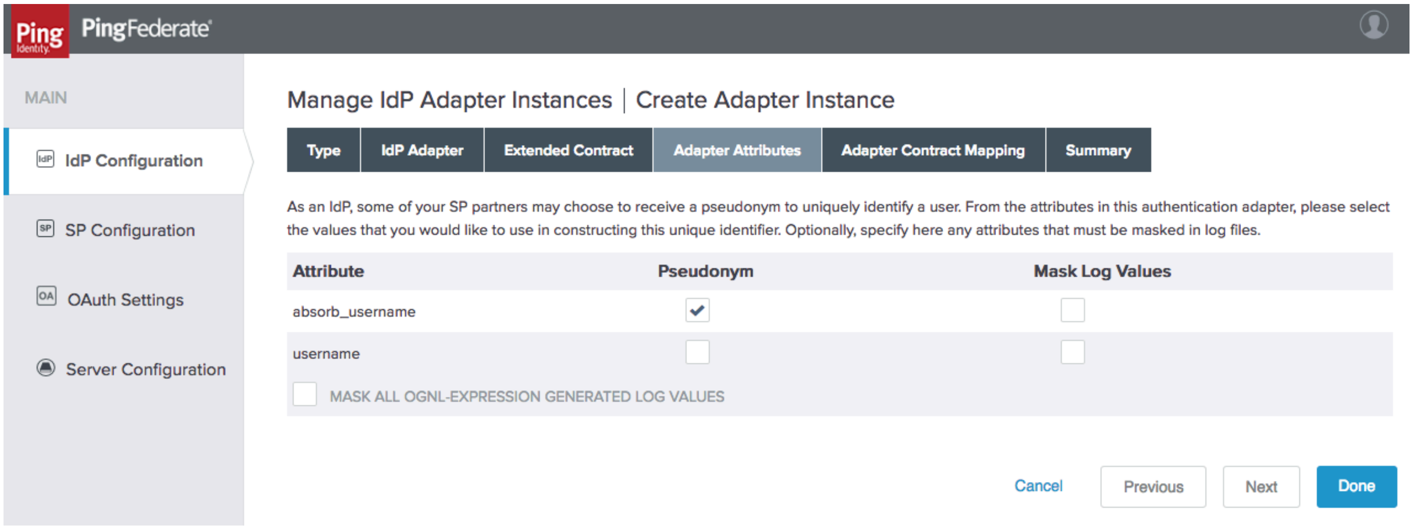
This adapter type supports the creation of an Extended Adapter Contract after initial deployment of the adapter instance. This Adapter Contract may be used to fulfill the Attribute Contract, look up additional attributes from a local data store, or create a persistent name identifier which uniquely identifies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

Core Contract

username

Extend the Contract	Action
absorb_username	Edit | Delete

8. Unselect the **username Pseudonym**, select the **absorb_username Pseudonym**, and click **Next**.



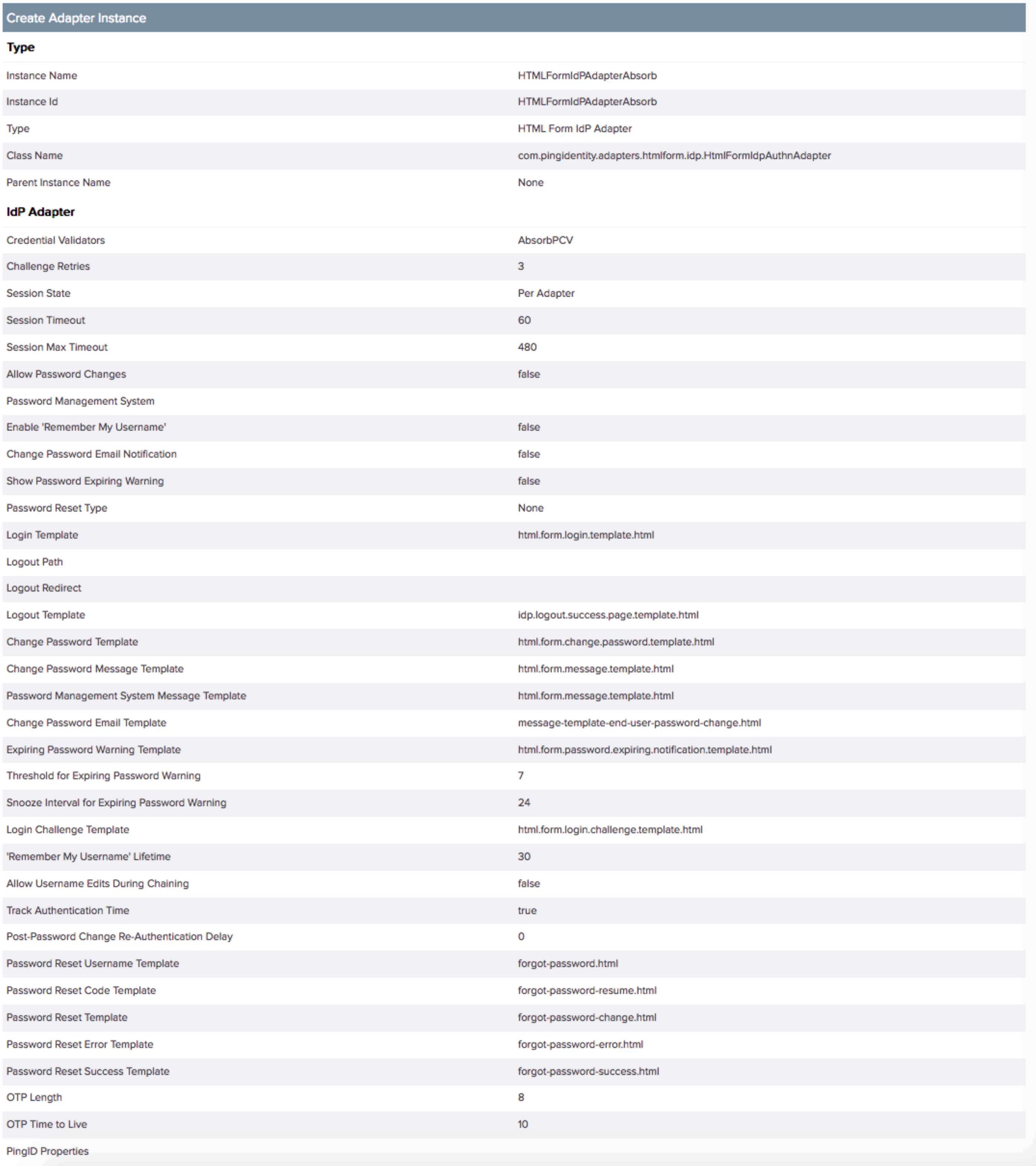
Manage IdP Adapter Instances | Create Adapter Instance

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
absorb_username	☑	□
username	□	□

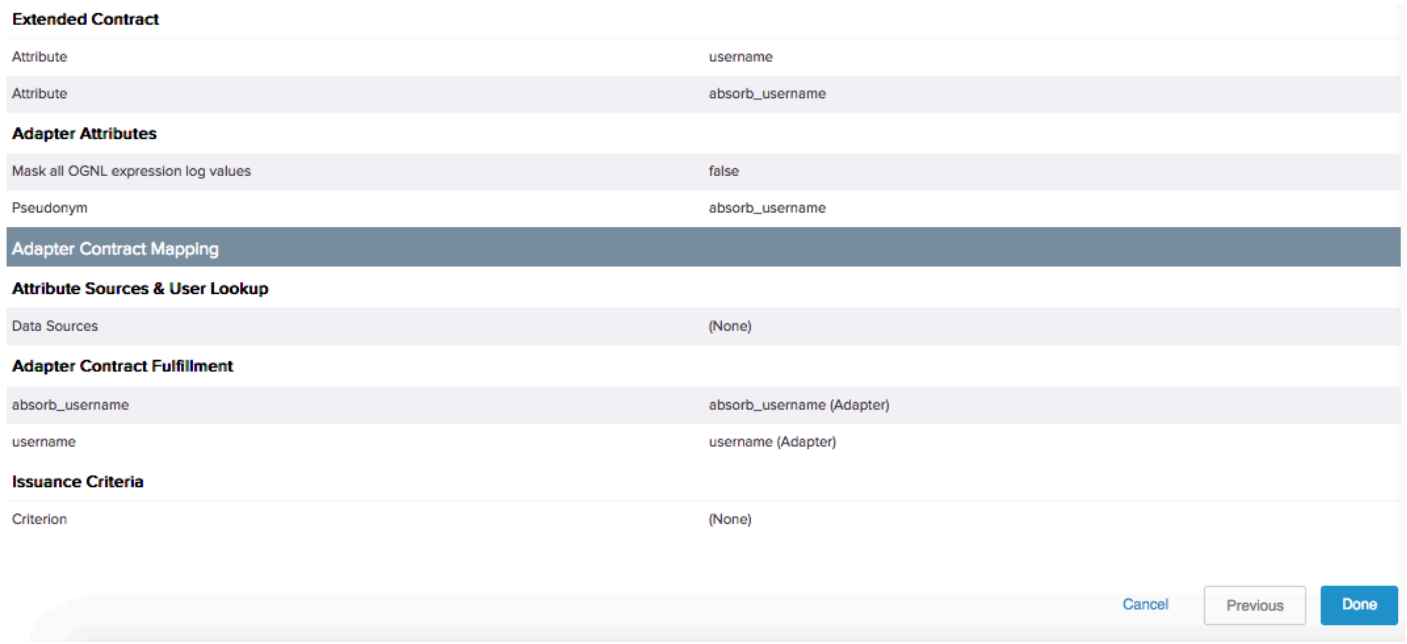
□ MASK ALL OGNL-EXPRESSION GENERATED LOG VALUES

9. Click **Next**.
10. Review the configuration on the summary page, and click **Done**.



Create Adapter Instance

Type	
Instance Name	HTMLFormIdPAdapterAbsorb
Instance Id	HTMLFormIdPAdapterAbsorb
Type	HTML Form IdP Adapter
Class Name	com.pingidentity.adapters.htmlform.idp.HtmlFormIdpAuthnAdapter
Parent Instance Name	None
IdP Adapter	
Credential Validators	AbsorbPCV
Challenge Retries	3
Session State	Per Adapter
Session Timeout	60
Session Max Timeout	480
Allow Password Changes	false
Password Management System	
Enable 'Remember My Username'	false
Change Password Email Notification	false
Show Password Expiring Warning	false
Password Reset Type	None
Login Template	html.form.login.template.html
Logout Path	
Logout Redirect	
Logout Template	idp.logout.success.page.template.html
Change Password Template	html.form.change.password.template.html
Change Password Message Template	html.form.message.template.html
Password Management System Message Template	html.form.message.template.html
Change Password Email Template	message-template-end-user-password-change.html
Expiring Password Warning Template	html.form.password.expiring.notification.template.html
Threshold for Expiring Password Warning	7
Snooze Interval for Expiring Password Warning	24
Login Challenge Template	html.form.login.challenge.template.html
'Remember My Username' Lifetime	30
Allow Username Edits During Chaining	false
Track Authentication Time	true
Post-Password Change Re-Authentication Delay	0
Password Reset Username Template	forgot-password.html
Password Reset Code Template	forgot-password-resume.html
Password Reset Template	forgot-password-change.html
Password Reset Error Template	forgot-password-error.html
Password Reset Success Template	forgot-password-success.html
OTP Length	8
OTP Time to Live	10
PingID Properties	

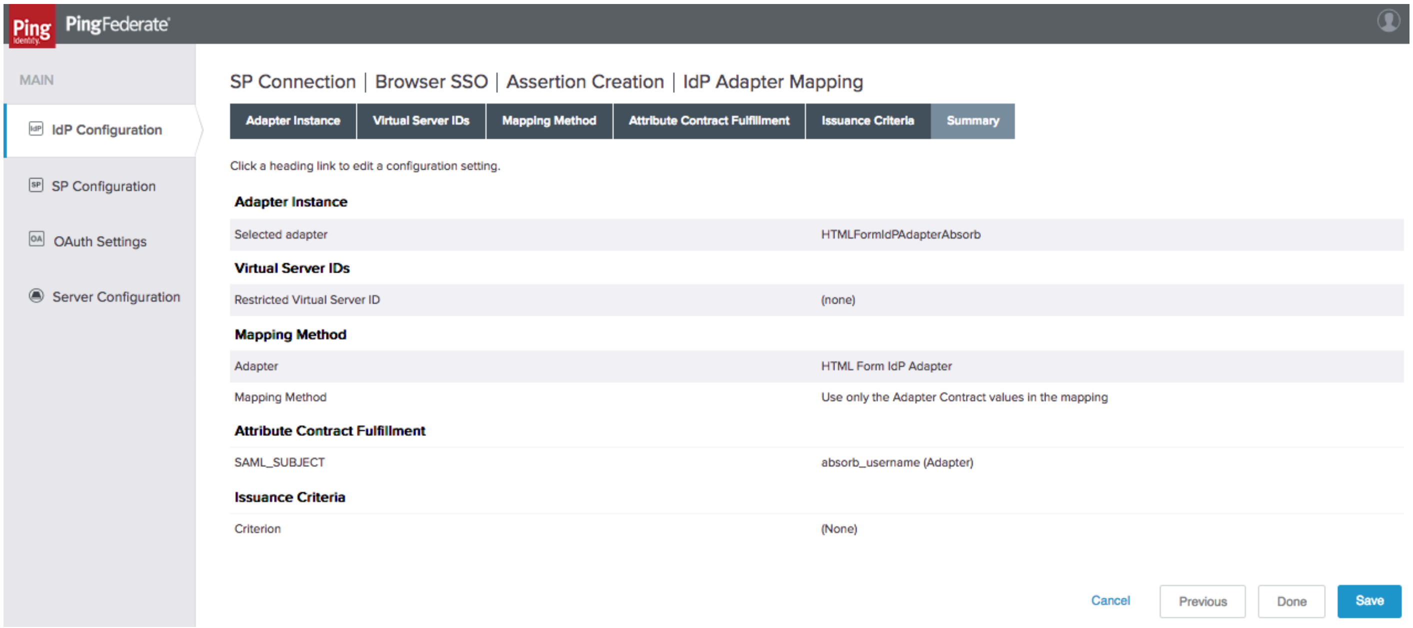


Extended Contract	
Attribute	username
Attribute	absorb_username
Adapter Attributes	
Mask all OGNL expression log values	false
Pseudonym	absorb_username
Adapter Contract Mapping	
Attribute Sources & User Lookup	
Data Sources	(None)
Adapter Contract Fulfillment	
absorb_username	absorb_username (Adapter)
username	username (Adapter)
Issuance Criteria	
Criterion	(None)

11. Click **Save**.

Configuring the SP Connection to Leverage the Absorb PCV-integrated Adapter

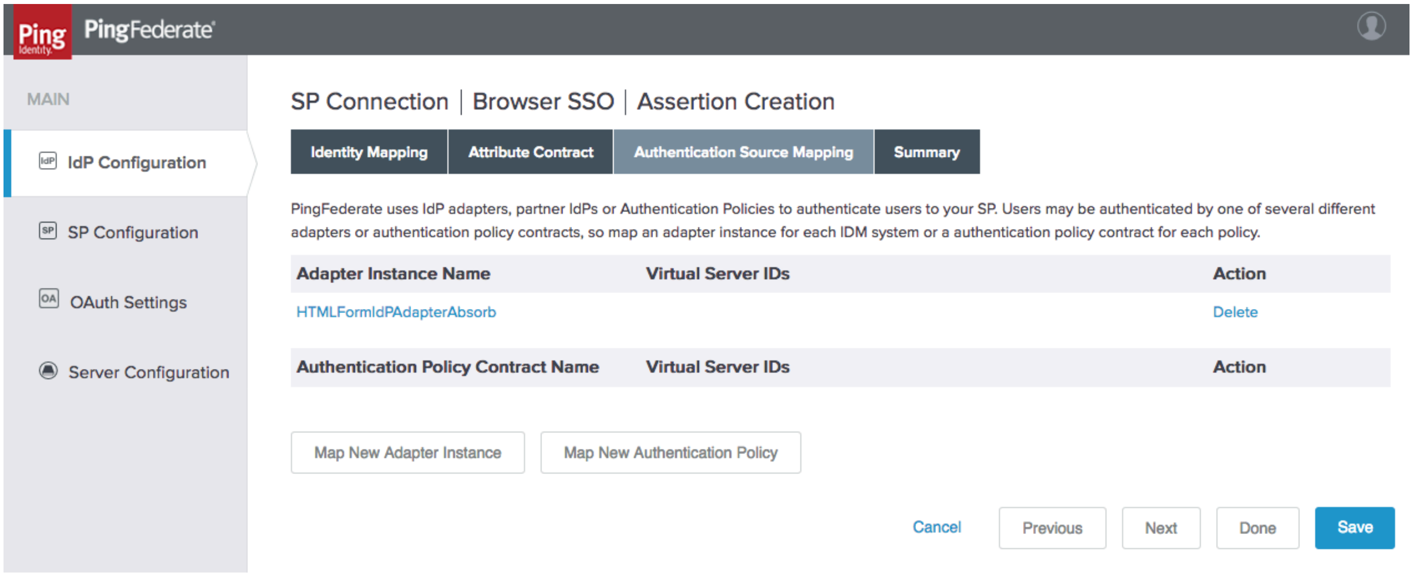
1. Click the SP connection to be modified or create a new SP connection, which should be located under **IdP Configuration** >> **SP Connections**.
2. Click **Authentication Source Mapping** and click **Map New Adapter Instance**.
3. Choose the adapter that was configured with the Absorb Password Credential Validator, and click **Next**.
4. Go through the rest of the configuration process. Make sure that the **SAML_SUBJECT** (or whichever attribute is chosen) is mapped to **absorb_username**.
5. Review the configuration on the summary page, and click **Done**.



Click a heading link to edit a configuration setting.

Adapter Instance	
Selected adapter	HTMLFormIdPAdapterAbsorb
Virtual Server IDs	
Restricted Virtual Server ID	(none)
Mapping Method	
Adapter	HTML Form IdP Adapter
Mapping Method	Use only the Adapter Contract values in the mapping
Attribute Contract Fulfillment	
SAML_SUBJECT	absorb_username (Adapter)
Issuance Criteria	
Criterion	(None)

6. Review the **Authentication Source Mapping**, and click **Done**.



SP Connection | Browser SSO | Assertion Creation

PingFederate uses IdP adapters, partner IdPs or Authentication Policies to authenticate users to your SP. Users may be authenticated by one of several different adapters or authentication policy contracts, so map an adapter instance for each IDM system or a authentication policy contract for each policy.

Adapter Instance Name	Virtual Server IDs	Action
HTMLFormIdPAdapterAbsorb		Delete

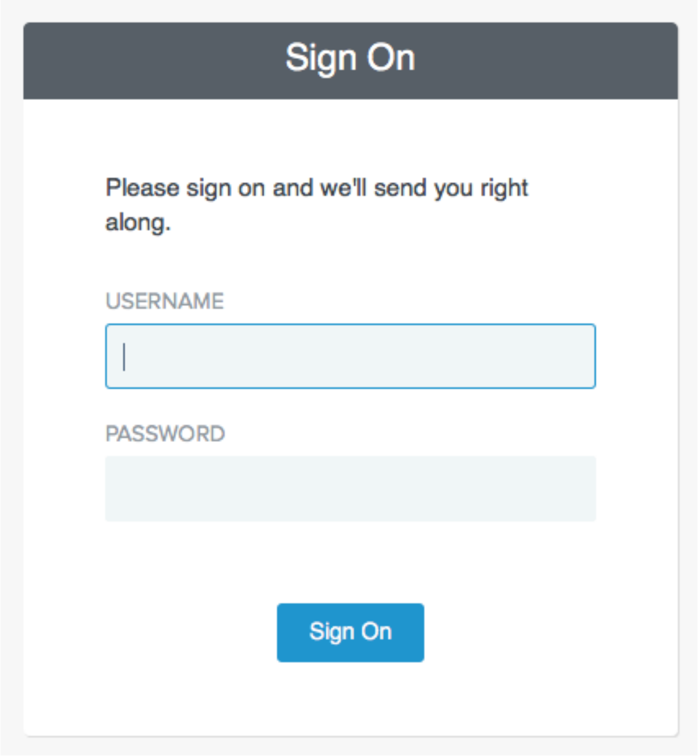
Authentication Policy Contract Name	Virtual Server IDs	Action

7. Click **Done**.
8. Click **Save**.

Testing

Primary Test Case

1. Open a browser and go to the IdP login form chosen as the primary form of authentication. In this example, the HTML Form IdP Adapter leveraging the Absorb PCV was chosen.



Sign On

Please sign on and we'll send you right along.

2. Log in using the test credentials.

   Results: If authorized into the target destination, authentication was a success. This means that the user authenticated successfully against the web service (verify by logs for details- ensure that DEBUG is enabled).

Other Test Cases

1. Log in with invalid credentials.

Logging

To enable various logging modes for the Absorb Password Credential Validator, add the following in the relevant sections in <PingFederateInstall>/pingfederate/server/default/conf/log4j2.xml.

```
<Logger name="com.pingidentity.clientservices.product.pcv.absorb" level="[ DEBUG | INFO
| WARN | ERROR ]" />
```

To enable logging for the Absorb Password Credential Validator in a separate file, add the following in the relevant sections in <PingFederateInstall>/pingfederate/server/default/conf/log4j2.xml.

```
<RollingFile name="AbsorbPCV" fileName="${sys:pf.log.dir}/absorbpcv.log"
 filePattern="${sys:pf.log.dir}/absorbpcv.%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.pcv.absorb"
level="[ DEBUG | INFO | WARN | ERROR ]" additivity="false" includeLocation="true"/>
        <appender-ref ref="AbsorbPCV" />
</Logger>
```

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