Ping Identity™

PingFederate®

PingID Registration Adapter v1.5.0

User Guide

PingFederate PingID Registration Adapter User Guide
Version 1.5.0
September 2019

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 PingID Registration Adapter helps register a user with PingID. The adapter allows a user to register by receiving and verifying a code delivered by Desktop App, Mobile App, YubiKey, OATH token, SMS, voice, or email.

Prerequisites

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

- A functional PingFederate environment, version 9.x+
- JDK version 8+
- A PingOne for Enterprise account that has PingID-Multiple Devices configuration settings
- A pre-configured first factor authentication adapter (e.g., HTML Form Adapter with LDAP PCV)
- A pre-configured PingID standard adapter that will be used as the third adapter within a composite adapter or the policies framework
- If passing in SMS or voice numbers, they are required to be in international format for processing with the PingID API (see pairingData in the Offline Pairing table - https://www.pingidentity.com/developer/en/api/pingid-api/user-management-api.html#OfflinePairing)
- If enabling the OATH token option as a device method, OATH token seed file will need to be imported into PingOne/PingID (see https://support.pingidentity.com/s/document-item?bundleId=pingid&topicId=npc1564020476379.html)

Installation

1. From the /dist folder in *pf-pingid-registration-adapter-1.5.0.zip*, copy the following files to the following directories in your PingFederate:

Source	Destination
/dist/ • gson-2.8.5.jar • javase-2.0.jar • jdbc-lookup-plugin-1.0.0.jar • ldap-lookup-plugin-1.0.0.jar • libphonenumber-8.9.6.jar • pf-pingid-registration-adapter-1.5.0.jar • pingid-api-1.2.4.jar	<PingFederateInstall>/pingfederate/server/default/deploy/
/dist/templates • *.html	<PingFederateInstall>/pingfederate/server/default/conf/template/
/dist/templates/assets/ • css/* • images/* • js/*	<PingFederateInstall>/pingfederate/server/default/conf/template/assets/

2. Go to <PingFederateInstall>/pingfederate/server/default/conf/template/assets/images/ and create a new folder called ‘temp’ if it is not already there.

3. Follow the steps under ***Modifying Content and Applying Localization*** under **Configuration**.
4. Repeat steps 1 through 3 on other clustered engine nodes.
5. Start or restart PingFederate.

Configuration

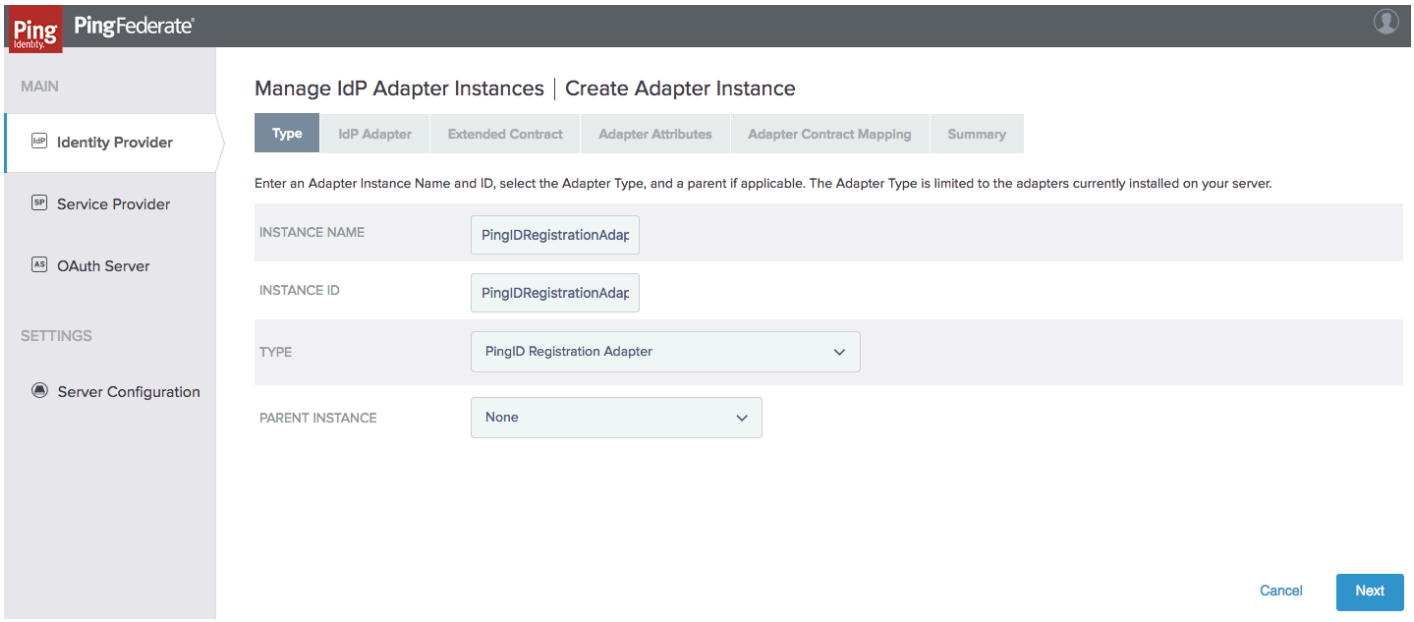
Modifying Content and Applying Localization

1. Go to <PingFederateInstall>/pingfederate/server/default/conf/language-packs/.
2. Make a backup copy of *pingfederate-messages.properties*.
3. Open up *pingfederate-messages.properties*, copy the contents from /dist/config/pingfederate-messages.propertes and append it to the bottom.
4. Modify the content as needed.
5. Save and close the file.
6. To localize content for PingFederate templates, do the following:
    a. Copy *pingfederate-messages.properties* and rename it *pingfederate-messages_[language code].properties* or *pingfederate-messages_[language code]_[region code].properties*. For example, *pingfederate-messages_es.properties* or *pingfederate-messages_fr_CA.properties*.
    b. Open up the localized copy and modify accordingly. Save and close it when completed.
    c. Move the file to the folder <PingFederateInstall>/pingfederate/server/default/conf/language-packs/.
    d. Repeat the process for additional localizations.

    For more information, refer to: https://documentation.pingidentity.com/pingfederate/pf90/index.shtml#adminGuide/pf_t_localizeMessagesForEndUsers.html

Configuring the PingID Registration Adapter

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** and **Instance Id**, choose **Ping ID Registration Adapter** and click **Next**.



4. Enter the required information, and click **Next**. Please note that a PingOne for Enterprise account with PingID-Multiple devices configuration settings will be needed to fill out the following fields: **PingID Base Endpoint**, **Use Base64 Key**, **Token**, **Org Alias**, **Domain**, **Origin**. The first four pieces of data can be taken from the Settings File (*pingid.properties*) that is downloaded from PingOne >> Setup >> PingID >> Client Integration.

Example of an OTP Verification Only PingID Registration 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.

PingID Registration Adapter

Field Name	Field Value	Description
ADAPTER METHOD TYPE	(•) OTP Verification ( ) Registration	The method type usage for the adapter; if 'OTP Verification' is selected, only the OTP is verified and the device will not be registered with the user for PingID (allowed options for OTP verification: phone, mobile, email, and secondary email); 'Registration' will register chosen devices
PINGID REGISTRATION TEMPLATE	pingid.registration.template.html	Name of the velocity template that will help the user verify OTP codes or register with PingID (default is pingid.registration.template.html)
PINGID NEXT STEPS TEMPLATE	pingid.registration.nextsteps.template.htm	Name of the velocity template that provides instructions on next steps after a user registers a device method (default is pingid.registration.nextsteps.template.html); pertains only to Adapter Method Type of 'Registration'
ALLOW DESKTOP APP REGISTRATION	☐	Allow Desktop App as an option in the PingID registration form; unavailable for 'OTP Verfication' adapter configurations
ALLOW MOBILE APP REGISTRATION	☐	Allow Mobile App as an option in the PingID registration form; unavailable for 'OTP Verfication' adapter configurations
ALLOW YUBIKEY REGISTRATION	☐	Allow Yubikey as an option in the PingID registration form; unavailable for 'OTP Verfication' adapter configurations
ALLOW OATH TOKEN REGISTRATION	☐	Allow OATH Token as an option in the PingID Registration form; unavailable for 'OTP Verification' adapter configurations
ALLOW SMS REGISTRATION	☑	Allow SMS as an option in the PingID registration form
ALLOW VOICE REGISTRATION	☑	Allow Voice as an option in the PingID registration form
ALLOW EMAIL REGISTRATION	☑	Allow Email as an option in the PingID registration form
ALLOW SECONDARY EMAIL REGISTRATION	☑	Allow Secondary Email as an option in the PingID registration form
PINGID BASE ENDPOINT	https://idpxnyl3m.pingidentity.com/pingid/	The PingID base endpoint (default is https://idpxnyl3m.pingidentity.com/pingid/rest/4/)
USE BASE 64 KEY	FbYVbTQML2LFKq6anu1ZykD9Hvy4oBgN	PingID property from PingOne 'use_base_64_key'
TOKEN	1c0b4526ba494ab69a95535b20ad5f6d	PingID property from PingOne 'token'
ORG ALIAS	4abbf497-4965-4a84-b15c-13bba6787ce	PingID property from PingOne 'org_alias'
DOMAIN	localhost	The domain of the service provider used for the PingID rpId (e.g., yourcompany.com)
ORIGIN	https://localhost	The scheme and domain of the URL that the user wants to access (e.g., https://yourcompany.com)

Advanced Fields:

ALWAYS ENABLE OTP VERIFICATION	☐	Always enable OTP verification even if the user has registered devices; works only if Adapter Method Type of 'OTP Verification' is selected
RESET USER ACCOUNT UPON OTP REVERIFY	☑	Reset the user's account and removes all associated device(s) when the user reverifies via OTP; please note that this option will also remove the user's account audit data in PingOne PingID; works only if Adapter Method Type of 'OTP Verification' is selected
ENABLE THE INTRODUCTION TEMPLATE	☑	Check to enable the PingID introduction template as the first step in the PingID registration flow
PINGID INTRODUCTION TEMPLATE	pingid.registration.introduction.template.ht	Name of the template that provides the user an introduction to PingID (default is pingid.registration.introduction.template.html)
RELY ON EXTERNAL QR IMAGE SERVICE	☐	Only check the box if 'Allow Mobile App Registration' is checked and if relying on an external QR image generator service suffices; unavailable for 'OTP Verfication' adapter configurations
MOBILE APP QR IMAGE URL	https://idpxnyl3m.pingidentity.com/pingid/(	The QR code image URL located externally for the Mobile App (i.e., https://idpxnyl3m.pingidentity.com/pingid/QRRedirection?); must keep 'Rely on External QR Image Service' checked if QR images are to be generated externally from the QR image service; unavailable for 'OTP Verfication' adapter configurations
MOBILE APP QR IMAGE PATH	/Users/schang/ping/pingfederate/server/de	The QR code image path located on the PingFederate server for the Mobile App (e.g., /apps/ping/pingfederate/server/default/conf/template/assets/images/temp/); must keep 'Rely on External QR Image Service' unchecked if QR images are to be generated internally on the PingFederate server; unavailable for 'OTP Verfication' adapter configurations
DISPLAY DEVICE METHOD DATA	☐	Enable to display and not mask device method data for allowed device methods (i.e., show entire SMS/voice number and email); available only to SMS, voice, email, and secondary email device methods
DISPLAY ALLOWED DEVICE METHOD TEXT FIELD	☑	Enable to display the text field that gathers contact information for allowed device methods; available only to SMS, voice, email, and secondary email device methods
ALWAYS DISPLAY ALLOWED DEVICE METHODS	☑	Always display allowed device methods regardless if the user's profile does not have the associated contact data; available only for SMS, voice, email, and secondary email device methods; if enabled, 'Display Allowed Device Method Text Field' must also be enabled
ALLOW ONLY ONE OF EACH DEVICE METHOD TYPE PER REGISTRATION	☐	Allow the user to register only one of each device method type per registration; the user can register multiple device methods, but only one of each device method type; available to all device methods except for secondary email; works only if Adapter Method Type of 'Registration' is selected
ENABLE CHANGE DEVICE BUTTON	☑	Enables the 'Change Device' button on the device registration code page
ENABLE FINISH REGISTRATION BUTTON	☐	Enables the 'Finish Registration' button on the choose device method page; unavailable for 'OTP Verfication' adapter configurations
FAIL IF ALREADY REGISTERED	☐	Fail adapter and redirect user to the 'PingID Registration Error Template' if user is already registered with PingID; will not work if 'Send to PingOne Override' is checked
ENABLE CANCEL BUTTON	☑	Enables the 'Cancel' button on the device method selection and registration code pages
CANCEL METHOD TYPE	◉ Fail to Error Template ○ Fail to Next Adapter	The cancel method type if the user presses the 'Cancel' button; 'Fail to Error Template' will fail the user to the 'PingID Registration Error Template'; 'Fail to Next Adapter' will fail the user to the next adapter (e.g., user account reset adapter); will only work when 'Enable Cancel Button' is checked

RESET USER ACCOUNT UPON CANCEL	☐	Reset the user's account and removes all associated device(s) when the user presses the Cancel button; please note that this option will also remove the user's account audit data in PingOne PingID
PINGID REGISTRATION ERROR TEMPLATE	pingid.registration.error.template.html	Name of the velocity template that will display various error messages; for example, if the user is already registered with PingID, reaches the maximum limit of OTP code resends, or cancels out of the registration process (default is pingid.registration.error.template.html)
ENABLE THE REGISTRATION COMPLETED TEMPLATE	☐	Check to enable the PingID registration completed template as the last step in the PingID registration flow; pertains only to Adapter Method Type of 'Registration'
PINGID REGISTRATION COMPLETED TEMPLATE	pingid.registration.completed.template.htm	Name of the template that provides the user registration completed information for PingID (default is pingid.registration.completed.template.html); pertains only to Adapter Method Type of 'Registration'
SEND TO PINGONE OVERRIDE	☐	Check to override the authentication flow and send the user directly to PingOne's manage devices page once the adapter is finished
MAXIMUM NUMBER OF OTP VERIFICATIONS	2	The maximum number of devices that a user can verify by OTP; required if the Adapter Method Type of 'OTP Verification' is selected, otherwise default to '0'
MAXIMUM NUMBER OF REGISTRATIONS	3	The maximum number of devices that a user can register (registrations must match the max allowed in PingOne: Setup >> PingID >> Maximum Allowed Devices)
DISPLAY NUMBER OF REGISTRATIONS IN PINGONE	☐	Enable the feature to display the number of registrations in PingOne to the user during the registration process
ENABLE OTP CODES RESEND LIMIT	☑	Enable the feature to check the maximum number of times an OTP code can be resent before failure occurs
OTP CODES RESEND LIMIT	5	The maximum limit for how many times an OTP code can be resent before failure occurs; will only work when 'Enable OTP Codes Resend Limit' is checked
OTP CODES RESEND FAILURE METHOD TYPE	◉ Fail to Error Template ○ Fail to Next Adapter	The failure method type once the maximum limit for resending OTP codes has been reached; 'Fail to Error Template' will fail the user to the 'PingID Registration Error Template'; 'Fail to Next Adapter' will fail the user to the next adapter (e.g., user account lockout adapter); will only work when 'Enable OTP Codes Resend Limit' is checked
ENABLE OTP CODES RETRY LIMIT	☑	Enable the feature to check the maximum number of times an OTP code can be tried before failure occurs
OTP CODES RETRY LIMIT	8	The maximum limit for how many times an OTP code can be tried before failure occurs; will only work when 'Enable OTP Codes Retry Limit' is checked
OTP CODES RETRY FAILURE METHOD TYPE	◉ Fail to Error Template ○ Fail to Next Adapter	The failure method type once the maximum limit for trying OTP codes has been reached; 'Fail to Error Template' will fail the user to the 'PingID Registration Error Template'; 'Fail to Next Adapter' will fail the user to the next adapter (e.g., user account lockout adapter); will only work when 'Enable OTP Codes Retry Limit' is checked
ENABLE TRACKING OTP RESEND/RETRY LIMITS IN SESSION	☑	Enable the feature to track the OTP resend/retry limits in the browser session; if this feature is disabled, the user can restart the registration process and not receive an OTP resend/retry error in the same browser session
ENABLE BYPASS MODE	☑	Enable the feature to bypass the user to the next adapter when the PingID service is down

Example of a standard PingID Registration 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.

PingID Registration Adapter

Field Name	Field Value	Description
ADAPTER METHOD TYPE	○ OTP Verification ● Registration	The method type usage for the adapter; if 'OTP Verification' is selected, only the OTP is verified and the device will not be registered with the user for PingID (allowed options for OTP verification: phone, mobile, email, and secondary email); 'Registration' will register chosen devices
PINGID REGISTRATION TEMPLATE	pingid.registration.template.html	Name of the velocity template that will help the user verify OTP codes or register with PingID (default is pingid.registration.template.html)
PINGID NEXT STEPS TEMPLATE	pingid.registration.nextsteps.template.html	Name of the velocity template that provides instructions on next steps after a user registers a device method (default is pingid.registration.nextsteps.template.html); pertains only to Adapter Method Type of 'Registration'
ALLOW DESKTOP APP REGISTRATION	☑	Allow Desktop App as an option in the PingID registration form; unavailable for 'OTP Verfication' adapter configurations
ALLOW MOBILE APP REGISTRATION	☑	Allow Mobile App as an option in the PingID registration form; unavailable for 'OTP Verfication' adapter configurations
ALLOW YUBIKEY REGISTRATION	☑	Allow Yubikey as an option in the PingID registration form; unavailable for 'OTP Verfication' adapter configurations
ALLOW OATH TOKEN REGISTRATION	☑	Allow OATH Token as an option in the PingID Registration form; unavailable for 'OTP Verification' adapter configurations
ALLOW SMS REGISTRATION	☑	Allow SMS as an option in the PingID registration form
ALLOW VOICE REGISTRATION	☑	Allow Voice as an option in the PingID registration form
ALLOW EMAIL REGISTRATION	☑	Allow Email as an option in the PingID registration form
ALLOW SECONDARY EMAIL REGISTRATION	☑	Allow Secondary Email as an option in the PingID registration form
PINGID BASE ENDPOINT	https://idpxnyl3m.pingidentity.com/pingid/r	The PingID base endpoint (default is https://idpxnyl3m.pingidentity.com/pingid/rest/4/)
USE BASE 64 KEY	FbYVbTQML2LFKq6anu1ZykD9Hvy4oBgN8	PingID property from PingOne 'use_base_64_key'
TOKEN	1c0b4526ba494ab69a95535b20ad5f6d	PingID property from PingOne 'token'
ORG ALIAS	4abbf497-4965-4a84-b15c-13bba6787ce	PingID property from PingOne 'org_alias'
DOMAIN	localhost	The domain of the service provider used for the PingID rpId (e.g., yourcompany.com)
ORIGIN	https://localhost:9031	The scheme and domain of the URL that the user wants to access (e.g., https://yourcompany.com)

Advanced Fields:

ALWAYS ENABLE OTP VERIFICATION	☐	Always enable OTP verification even if the user has registered devices; works only if Adapter Method Type of 'OTP Verification' is selected
RESET USER ACCOUNT UPON OTP REVERIFY	☐	Reset the user's account and removes all associated device(s) when the user reverifies via OTP; please note that this option will also remove the user's account audit data in PingOne PingID; works only if Adapter Method Type of 'OTP Verification' is selected
ENABLE THE INTRODUCTION TEMPLATE	☐	Check to enable the PingID introduction template as the first step in the PingID registration flow
PINGID INTRODUCTION TEMPLATE	pingid.registration.introduction.template.ht	Name of the template that provides the user an introduction to PingID (default is pingid.registration.introduction.template.html)
RELY ON EXTERNAL QR IMAGE SERVICE	☑	Only check the box if 'Allow Mobile App Registration' is checked and if relying on an external QR image generator service suffices; unavailable for 'OTP Verfication' adapter configurations
MOBILE APP QR IMAGE URL	https://idpxnyl3m.pingidentity.com/pingid/(	The QR code image URL located externally for the Mobile App (i.e., https://idpxnyl3m.pingidentity.com/pingid/QRRedirection?); must keep 'Rely on External QR Image Service' checked if QR images are to be generated externally from the QR image service; unavailable for 'OTP Verfication' adapter configurations
MOBILE APP QR IMAGE PATH	/Users/schang/ping/pingfederate/server/de	The QR code image path located on the PingFederate server for the Mobile App (e.g., /apps/ping/pingfederate/server/default/conf/template/assets/images/temp/); must keep 'Rely on External QR Image Service' unchecked if QR images are to be generated internally on the PingFederate server; unavailable for 'OTP Verfication' adapter configurations
DISPLAY DEVICE METHOD DATA	☐	Enable to display and not mask device method data for allowed device methods (i.e., show entire SMS/voice number and email); available only to SMS, voice, email, and secondary email device methods
DISPLAY ALLOWED DEVICE METHOD TEXT FIELD	☑	Enable to display the text field that gathers contact information for allowed device methods; available only to SMS, voice, email, and secondary email device methods
ALWAYS DISPLAY ALLOWED DEVICE METHODS	☑	Always display allowed device methods regardless if the user's profile does not have the associated contact data; available only for SMS, voice, email, and secondary email device methods; if enabled, 'Display Allowed Device Method Text Field' must also be enabled
ALLOW ONLY ONE OF EACH DEVICE METHOD TYPE PER REGISTRATION	☐	Allow the user to register only one of each device method type per registration; the user can register multiple device methods, but only one of each device method type; available to all device methods except for secondary email; works only if Adapter Method Type of 'Registration' is selected
ENABLE CHANGE DEVICE BUTTON	☑	Enables the 'Change Device' button on the device registration code page
ENABLE FINISH REGISTRATION BUTTON	☑	Enables the 'Finish Registration' button on the choose device method page; unavailable for 'OTP Verfication' adapter configurations
FAIL IF ALREADY REGISTERED	☐	Fail adapter and redirect user to the 'PingID Registration Error Template' if user is already registered with PingID; will not work if 'Send to PingOne Override' is checked
ENABLE CANCEL BUTTON	☑	Enables the 'Cancel' button on the device method selection and registration code pages
CANCEL METHOD TYPE	◉ Fail to Error Template ○ Fail to Next Adapter	The cancel method type if the user presses the 'Cancel' button; 'Fail to Error Template' will fail the user to the 'PingID Registration Error Template'; 'Fail to Next Adapter' will fail the user to the next adapter (e.g., user account reset adapter); will only work when 'Enable Cancel Button' is checked

RESET USER ACCOUNT UPON CANCEL	☑	Reset the user's account and removes all associated device(s) when the user presses the Cancel button; please note that this option will also remove the user's account audit data in PingOne PingID
PINGID REGISTRATION ERROR TEMPLATE	pingid.registration.error.template.html	Name of the velocity template that will display various error messages; for example, if the user is already registered with PingID, reaches the maximum limit of OTP code resends, or cancels out of the registration process (default is pingid.registration.error.template.html)
ENABLE THE REGISTRATION COMPLETED TEMPLATE	☑	Check to enable the PingID registration completed template as the last step in the PingID registration flow; pertains only to Adapter Method Type of 'Registration'
PINGID REGISTRATION COMPLETED TEMPLATE	pingid.registration.completed.template.htn	Name of the template that provides the user registration completed information for PingID (default is pingid.registration.completed.template.html); pertains only to Adapter Method Type of 'Registration'
SEND TO PINGONE OVERRIDE	☐	Check to override the authentication flow and send the user directly to PingOne's manage devices page once the adapter is finished
MAXIMUM NUMBER OF OTP VERIFICATIONS	0	The maximum number of devices that a user can verify by OTP; required if the Adapter Method Type of 'OTP Verification' is selected, otherwise default to '0'
MAXIMUM NUMBER OF REGISTRATIONS	7	The maximum number of devices that a user can register (registrations must match the max allowed in PingOne: Setup >> PingID >> Maximum Allowed Devices)
DISPLAY NUMBER OF REGISTRATIONS IN PINGONE	☑	Enable the feature to display the number of registrations in PingOne to the user during the registration process
ENABLE OTP CODES RESEND LIMIT	☑	Enable the feature to check the maximum number of times an OTP code can be resent before failure occurs
OTP CODES RESEND LIMIT	5	The maximum limit for how many times an OTP code can be resent before failure occurs; will only work when 'Enable OTP Codes Resend Limit' is checked
OTP CODES RESEND FAILURE METHOD TYPE	◉ Fail to Error Template ○ Fail to Next Adapter	The failure method type once the maximum limit for resending OTP codes has been reached; 'Fail to Error Template' will fail the user to the 'PingID Registration Error Template'; 'Fail to Next Adapter' will fail the user to the next adapter (e.g., user account lockout adapter); will only work when 'Enable OTP Codes Resend Limit' is checked
ENABLE OTP CODES RETRY LIMIT	☑	Enable the feature to check the maximum number of times an OTP code can be tried before failure occurs
OTP CODES RETRY LIMIT	3	The maximum limit for how many times an OTP code can be tried before failure occurs; will only work when 'Enable OTP Codes Retry Limit' is checked
OTP CODES RETRY FAILURE METHOD TYPE	◉ Fail to Error Template ○ Fail to Next Adapter	The failure method type once the maximum limit for trying OTP codes has been reached; 'Fail to Error Template' will fail the user to the 'PingID Registration Error Template'; 'Fail to Next Adapter' will fail the user to the next adapter (e.g., user account lockout adapter); will only work when 'Enable OTP Codes Retry Limit' is checked
ENABLE TRACKING OTP RESEND/RETRY LIMITS IN SESSION	☑	Enable the feature to track the OTP resend/retry limits in the browser session; if this feature is disabled, the user can restart the registration process and not receive an OTP resend/retry error in the same browser session
ENABLE BYPASS MODE	☑	Enable the feature to bypass the user to the next adapter when the PingID service is down

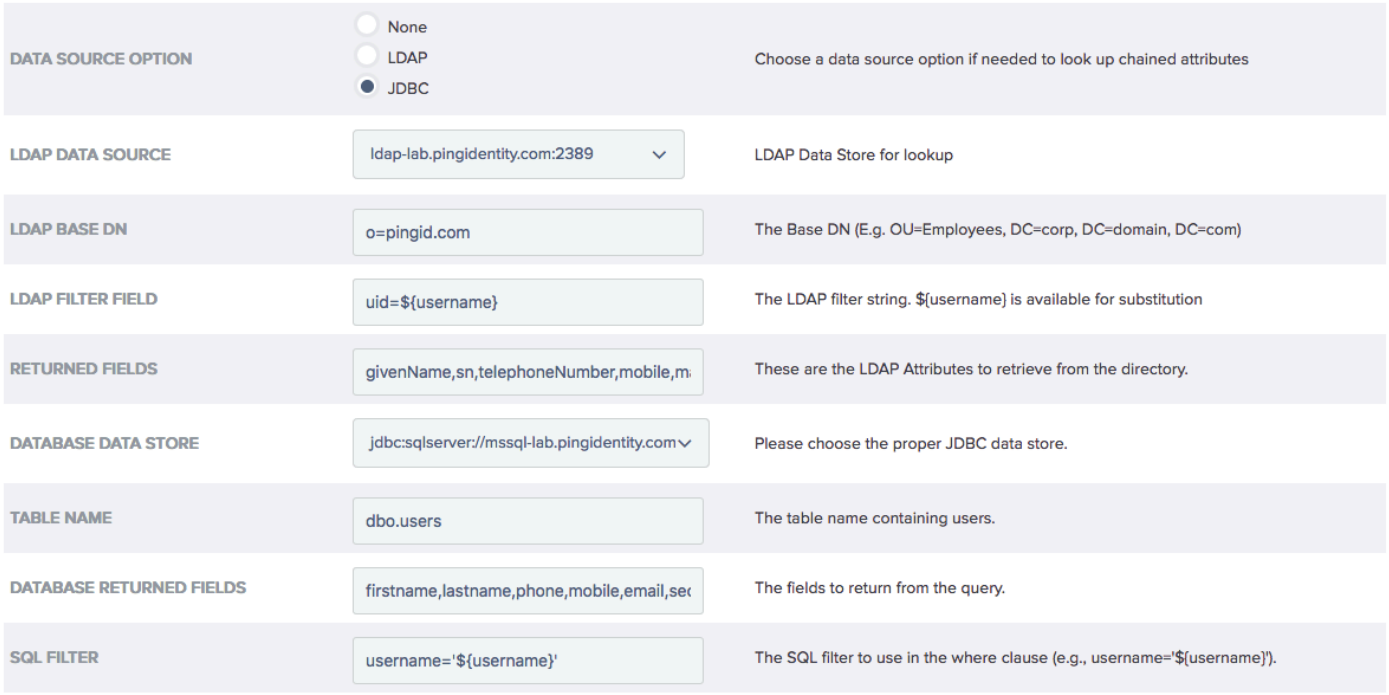
Example of an LDAP datastore configuration:

DATA SOURCE OPTION	None LDAP JDBC	Choose a data source option if needed to look up chained attributes
LDAP DATA SOURCE	ldap-lab.pingidentity.com:2389	LDAP Data Store for lookup
LDAP BASE DN	o=pingid.com	The Base DN (E.g. OU=Employees, DC=corp, DC=domain, DC=com)
LDAP FILTER FIELD	uid=${username}	The LDAP filter string. ${username} is available for substitution
RETURNED FIELDS	givenName,sn,telephoneNumber,mobile,m	These are the LDAP Attributes to retrieve from the directory.
DATABASE DATA STORE	jdbc:sqlserver://mssql-lab.pingidentity.com	Please choose the proper JDBC data store.
TABLE NAME	dbo.users	The table name containing users.
DATABASE RETURNED FIELDS	firstname,lastname,phone,mobile,email,se	The fields to return from the query.
SQL FILTER	username='${username}'	The SQL filter to use in the where clause (e.g., username='${username}').

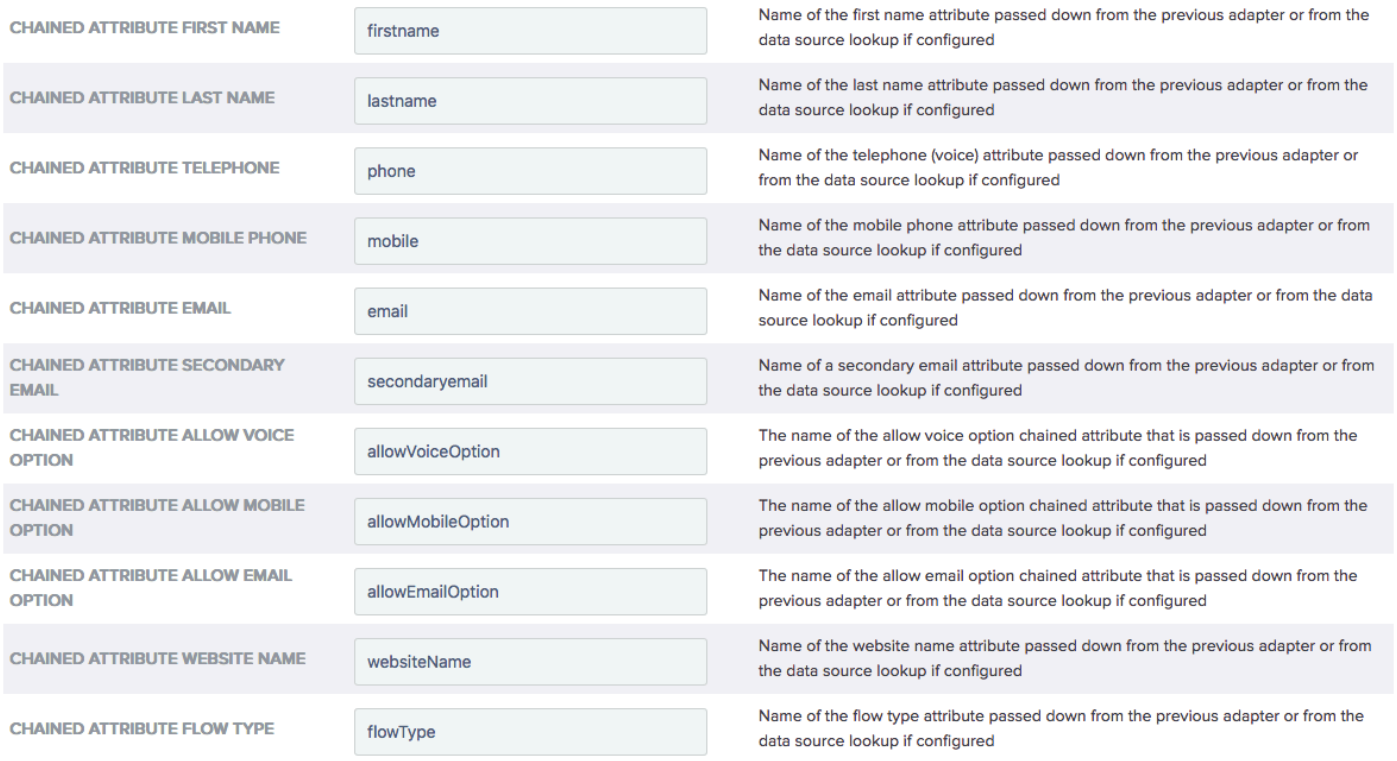
And associated chained attributes:

CHAINED ATTRIBUTE FIRST NAME	givenName	Name of the first name attribute passed down from the previous adapter or from the data source lookup if configured
CHAINED ATTRIBUTE LAST NAME	sn	Name of the last name attribute passed down from the previous adapter or from the data source lookup if configured
CHAINED ATTRIBUTE TELEPHONE	telephoneNumber	Name of the telephone (voice) attribute passed down from the previous adapter or from the data source lookup if configured
CHAINED ATTRIBUTE MOBILE PHONE	mobile	Name of the mobile phone attribute passed down from the previous adapter or from the data source lookup if configured
CHAINED ATTRIBUTE EMAIL	mail	Name of the email attribute passed down from the previous adapter or from the data source lookup if configured
CHAINED ATTRIBUTE SECONDARY EMAIL	destinationIndicator	Name of a secondary email attribute passed down from the previous adapter or from the data source lookup if configured
CHAINED ATTRIBUTE ALLOW VOICE OPTION	allowVoiceOption	The name of the allow voice option chained attribute that is passed down from the previous adapter or from the data source lookup if configured
CHAINED ATTRIBUTE ALLOW MOBILE OPTION	allowMobileOption	The name of the allow mobile option chained attribute that is passed down from the previous adapter or from the data source lookup if configured
CHAINED ATTRIBUTE ALLOW EMAIL OPTION	allowEmailOption	The name of the allow email option chained attribute that is passed down from the previous adapter or from the data source lookup if configured
CHAINED ATTRIBUTE WEBSITE NAME	websiteName	Name of the website name attribute passed down from the previous adapter or from the data source lookup if configured
CHAINED ATTRIBUTE FLOW TYPE	flowType	Name of the flow type attribute passed down from the previous adapter or from the data source lookup if configured

Example of a JDBC datastore configuration:



And associated chained attributes:

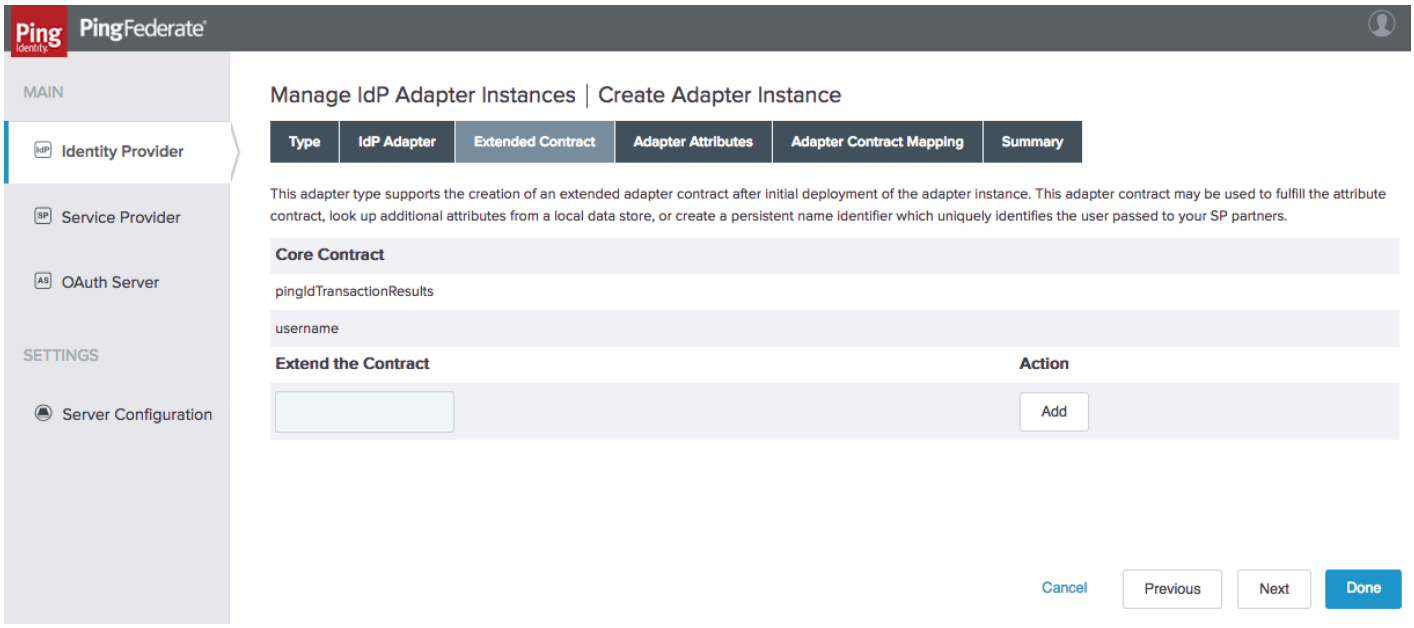


Please note on how to configure chained attributes (i.e., first name, last name, telephone, mobile, email, secondary email) – these are **required** if these pieces of information are to be passed in the SSO flow and/or updated in the user's account in PingOne (e.g., email notifications/confirmations):

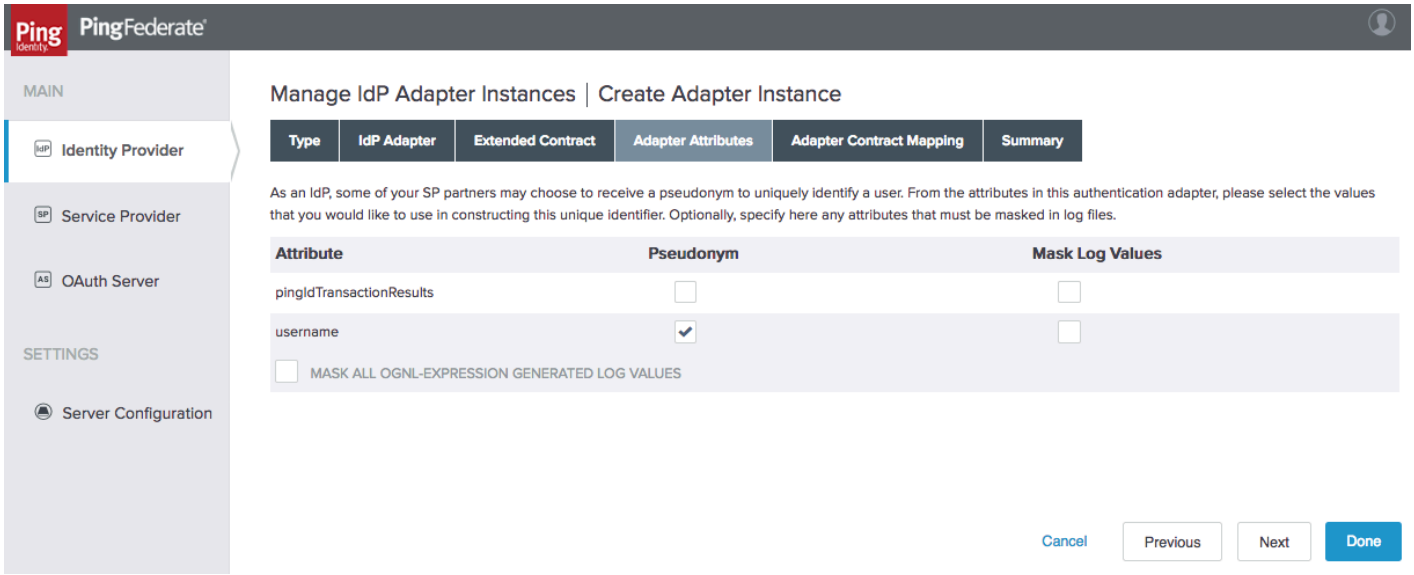
- If LDAP is chosen as a data source, enter the appropriate LDAP attribute name in the appropriate chained attribute field

- If JDBC is chosen as a data source, enter the appropriate JDBC field name in the appropriate chained attribute field
- If no data source is chosen, enter the appropriate attribute name passed from the first factor in the appropriate chained attribute field

5. Review and/or extend the attribute contract and click **Next**.



6. Select **username** as the **Pseudonym** and click **Next**.

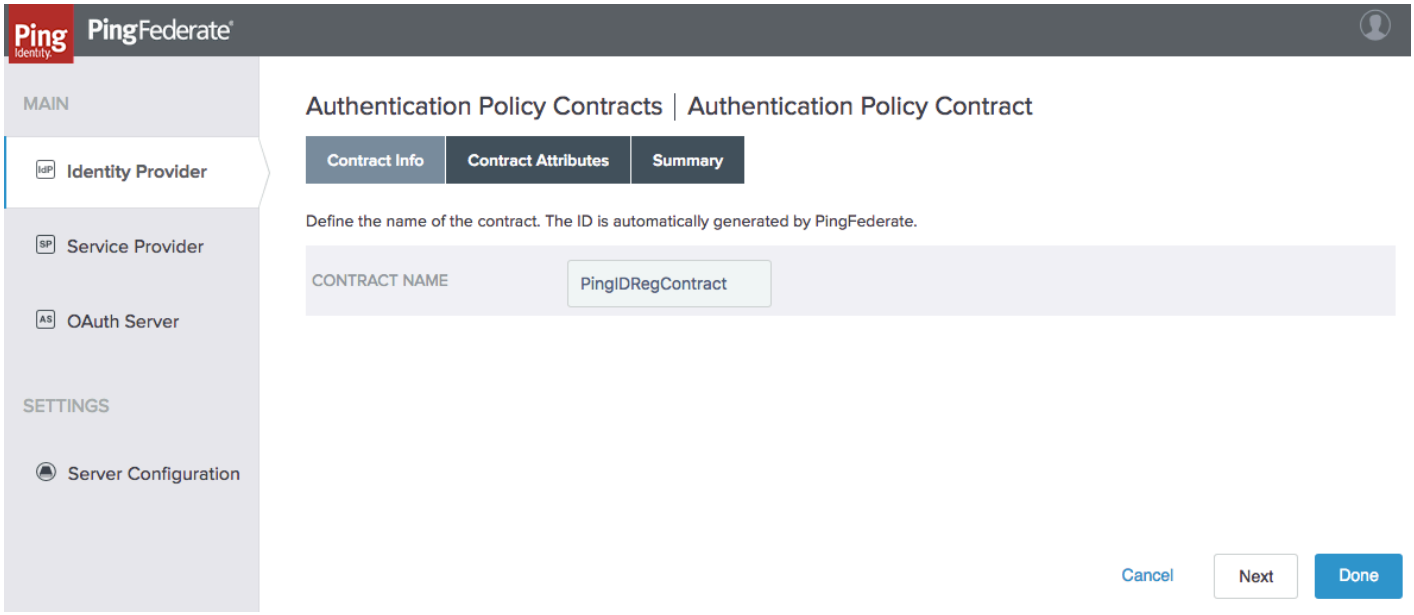


7. Click **Next**.
8. Review the configuration on the summary page and click **Done**.
9. Click **Save**.

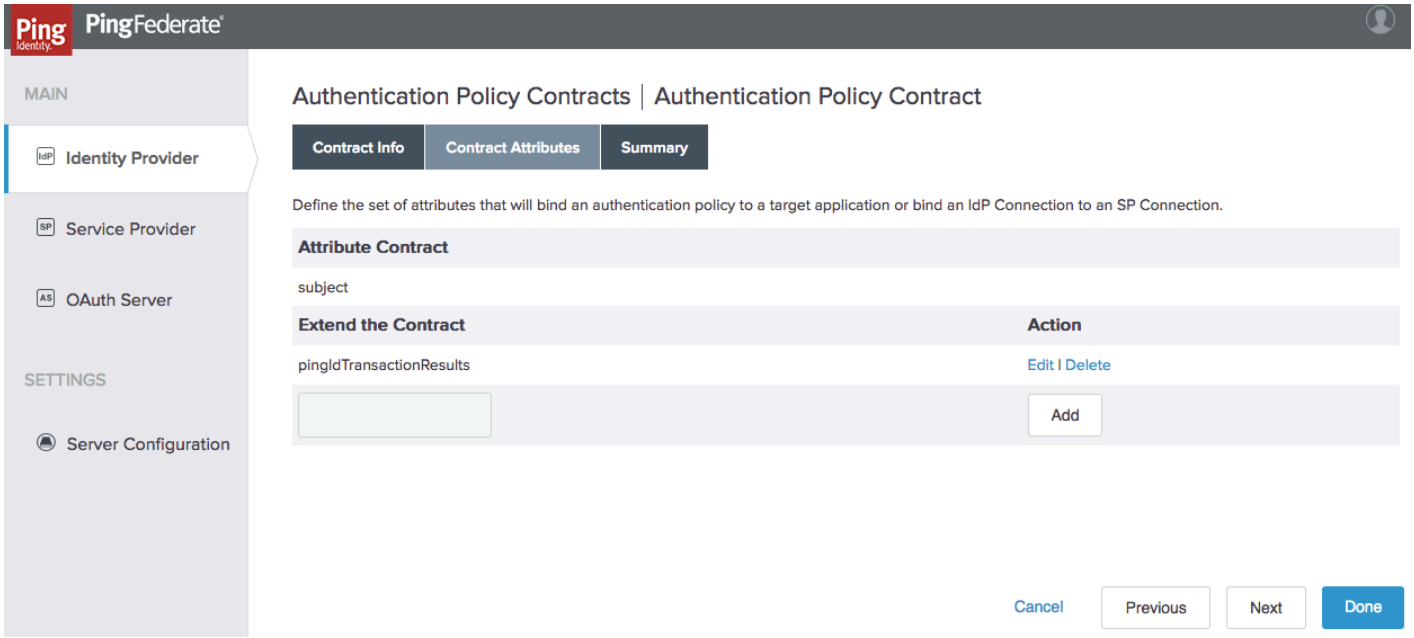
Configuring the PingID Registration Adapter in a Policy Tree

Note: If not configuring the PingID Registration Adapter in a composite adapter, use this method.

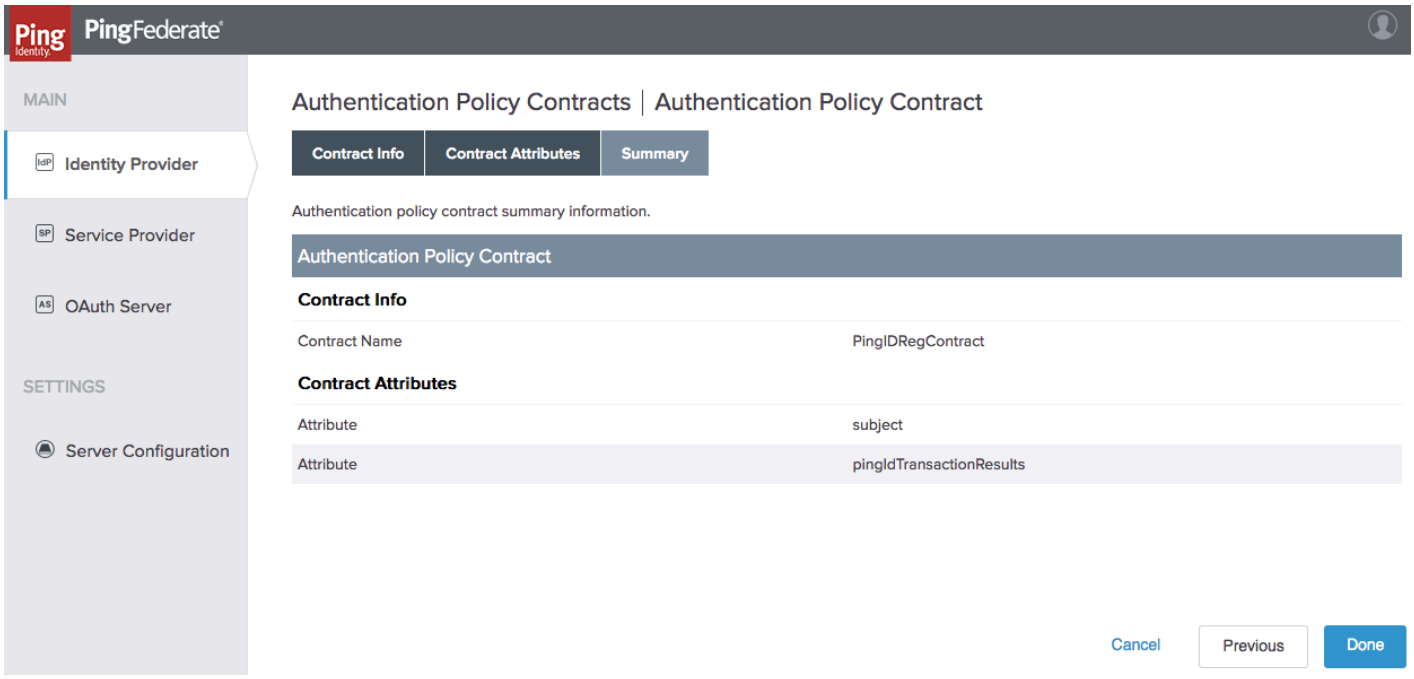
1. Log into the PingFederate admin console and click **Policy Contracts** under **Identity Provider** >> **Authentication Policies**.
2. Click **Create New Contract**.
3. Enter the **Contract Name** and click **Next**.



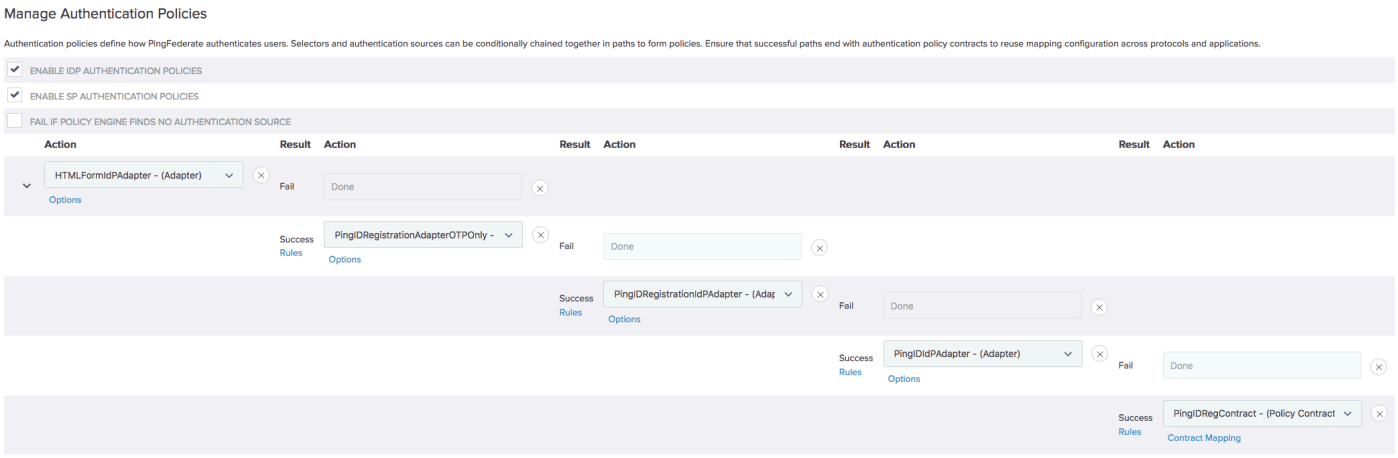
4. Extend the contract with **pingIdTransactionResults** and other attributes as needed and click **Next**.



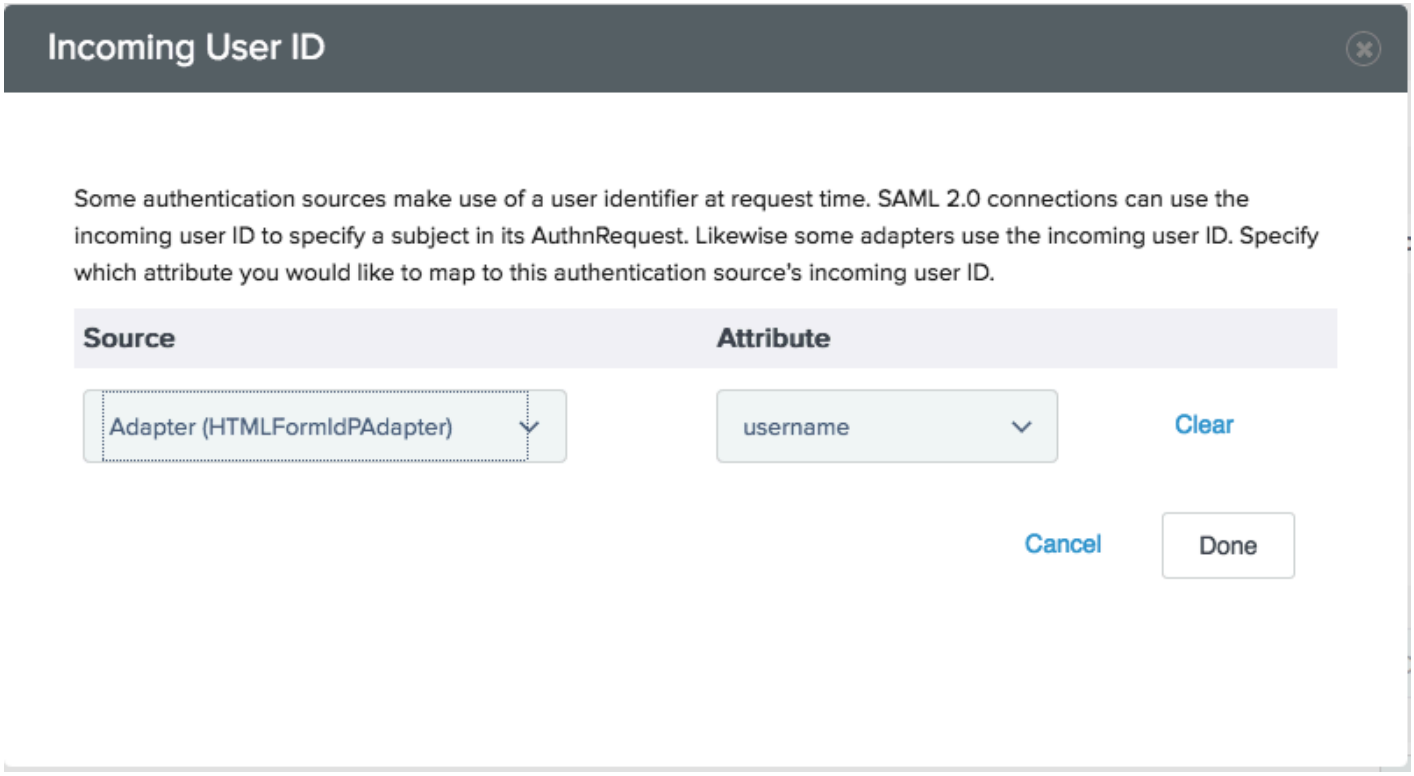
5. Click **Done**.



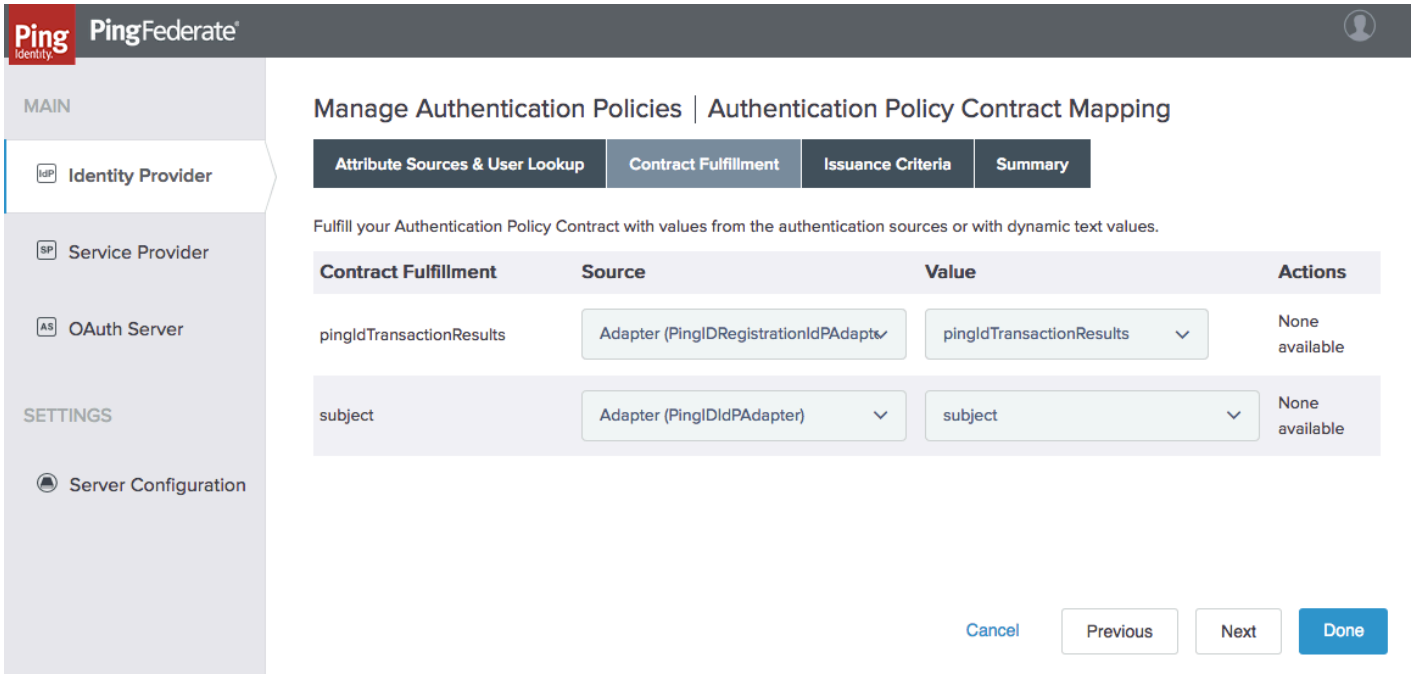
6. Click **Save**.
7. Click **Policies** under **Identity Provider** >> **Authentication Policies**.
8. Configure the policy tree. At the end of the policy tree, configure the policy contract that was previously configured. For example:



9. Click on **Options** under each adapter starting with the second configured adapter and configure the **Incoming User ID**. For example:



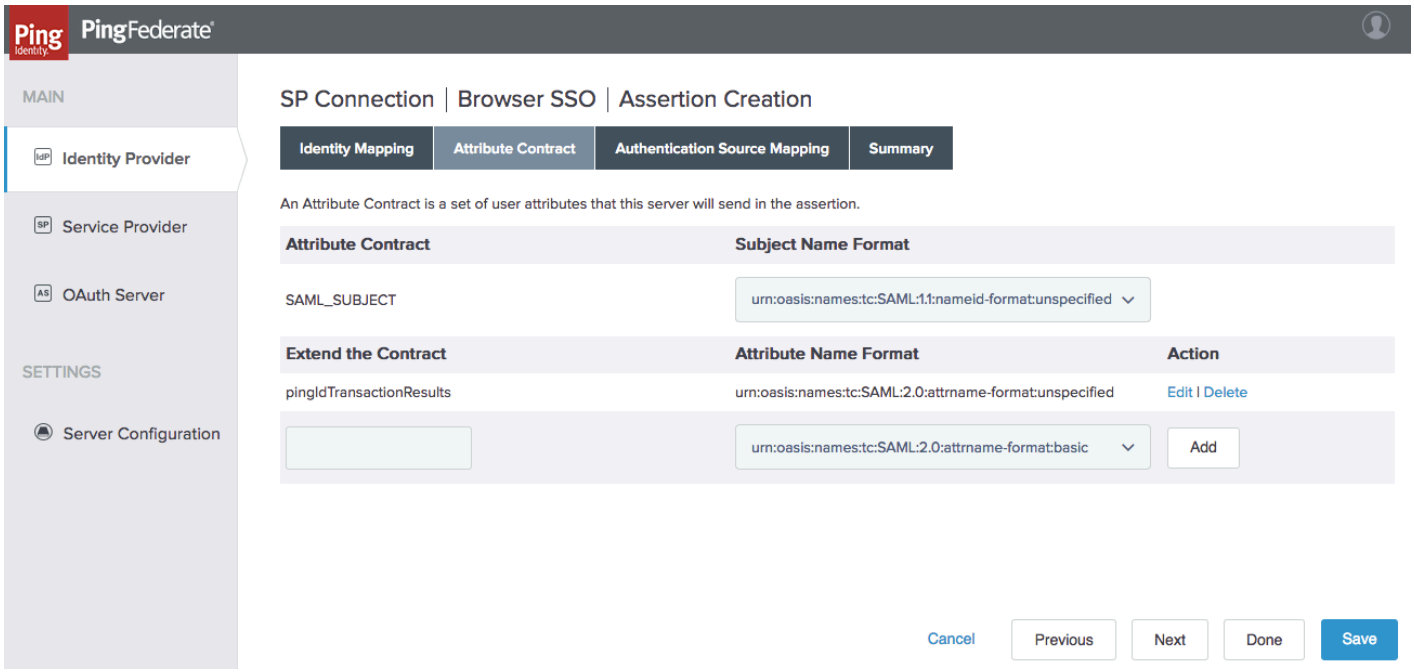
10. Click on **Contract Mapping** at the end of the policy tree and configure the **Contract Fulfillment**. For example:



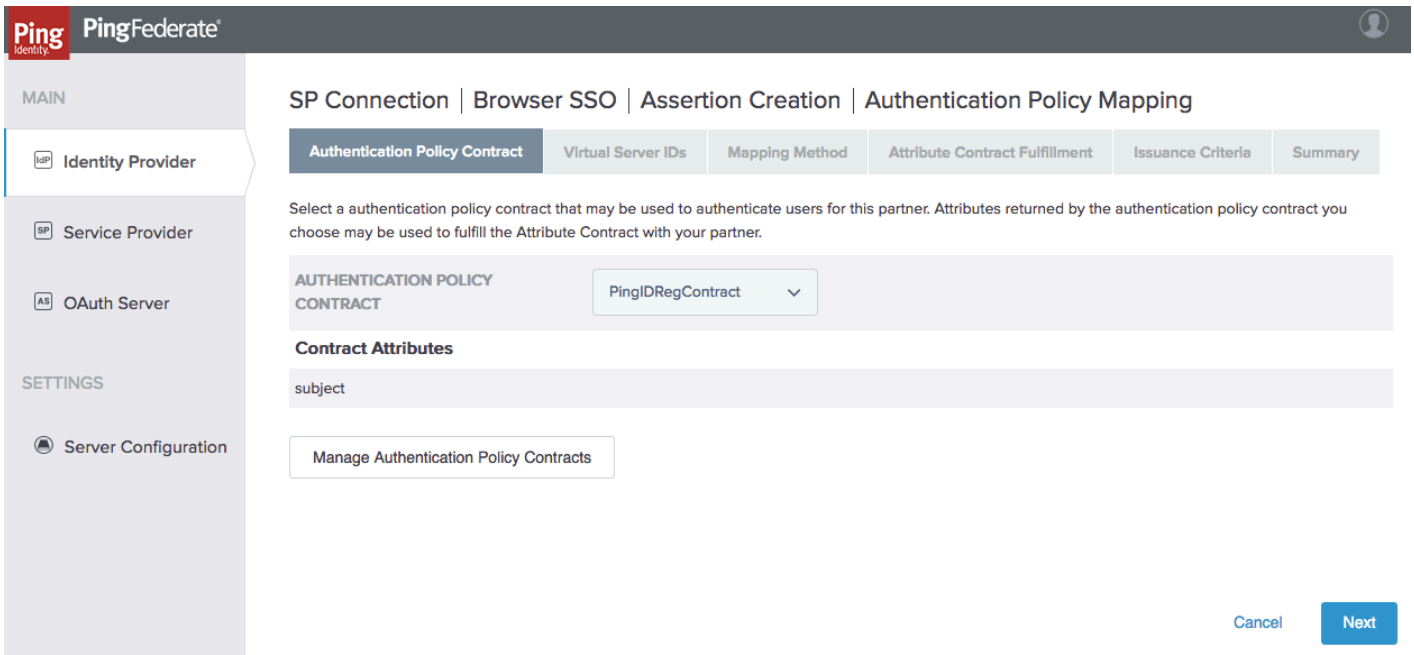
11. Click **Next**.
12. Click **Next**.
13. Click **Done**.
14. Click **Save.**

Configuring the SP Connection to Leverage the Policy Tree

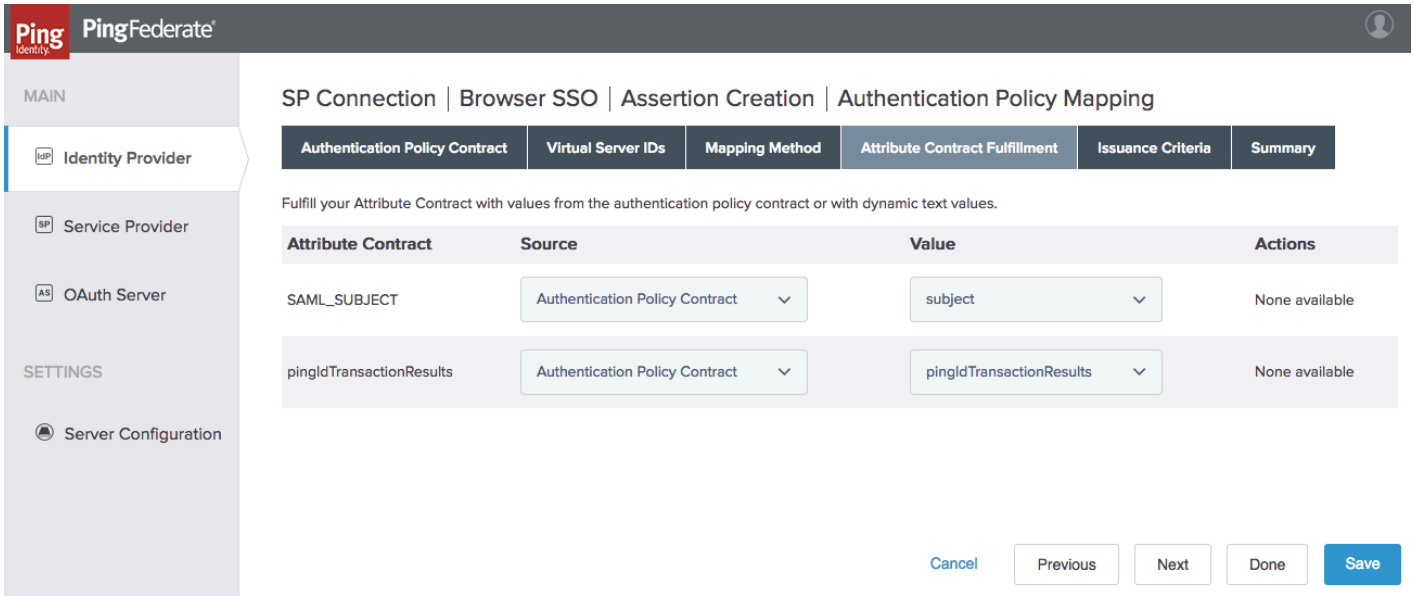
1. Click the SP connection to be modified or create a new SP connection, which should be located under **Identity Provider** >> **SP Connections**.
2. Under **Assertion Creation**, click on **Attribute Contract**, extend the contract with **pingIdTransactionResults**, and click **Next**.



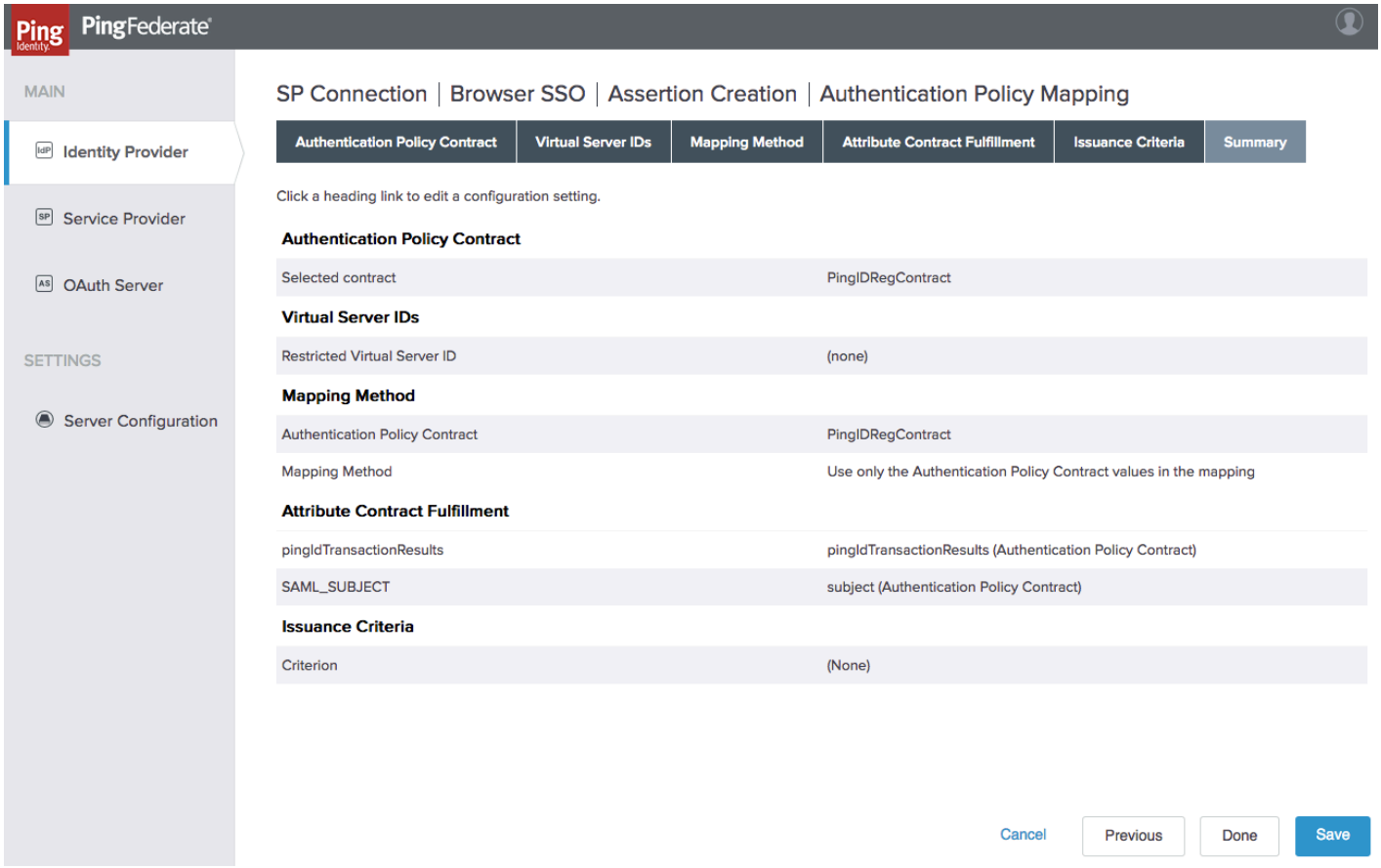
3. Click **Map New Authentication Policy**. Select the policy contract that contains the PingID Registration Adapter and click **Next**.



4. Click **Next**.
5. Select the appropriate **Adapter Contract** and click **Next**.
6. Configure the **Attribute Contract Fulfillment** and click **Next**.



7. Click **Next**.
8. Review the **Summary** and click **Done**.

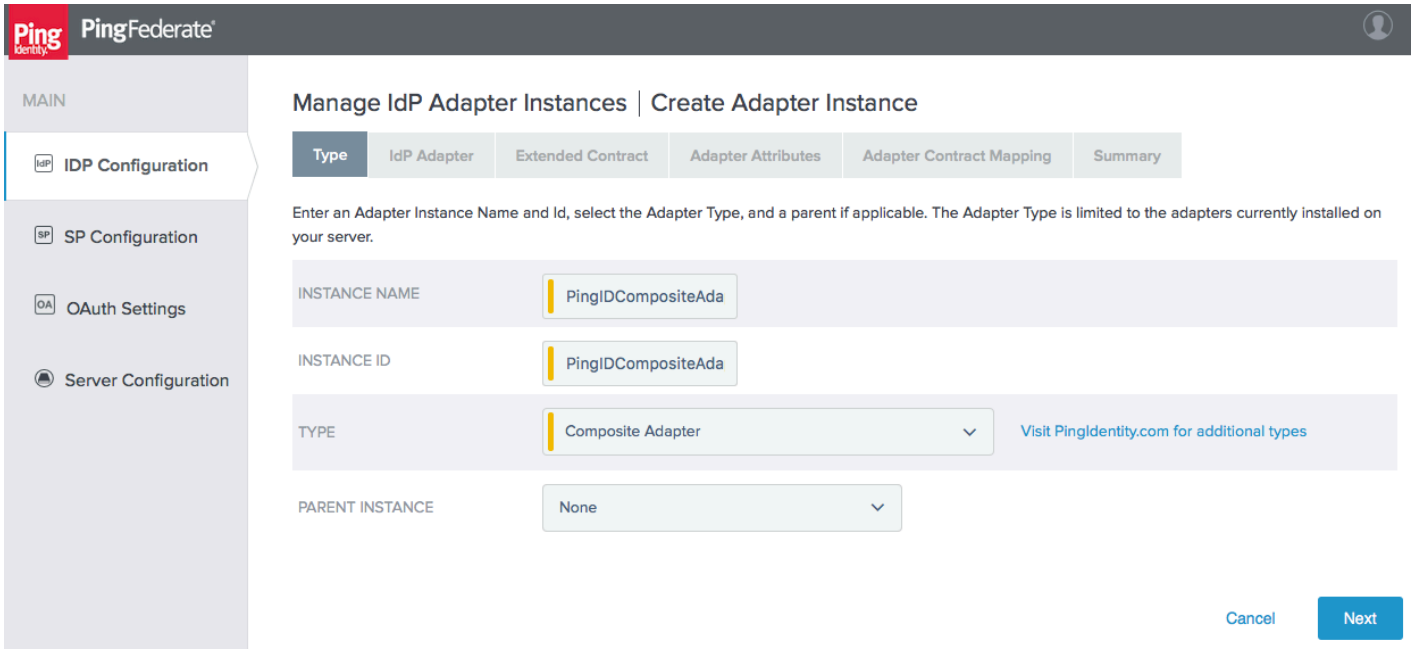


9. Continue with the rest of the SP connection configuration process.
10. Ensure that the SP connection is **Active**. Click **Save** as a final step to complete the SP connection configuration.

Configuring the PingID Registration Adapter in a Composite Adapter

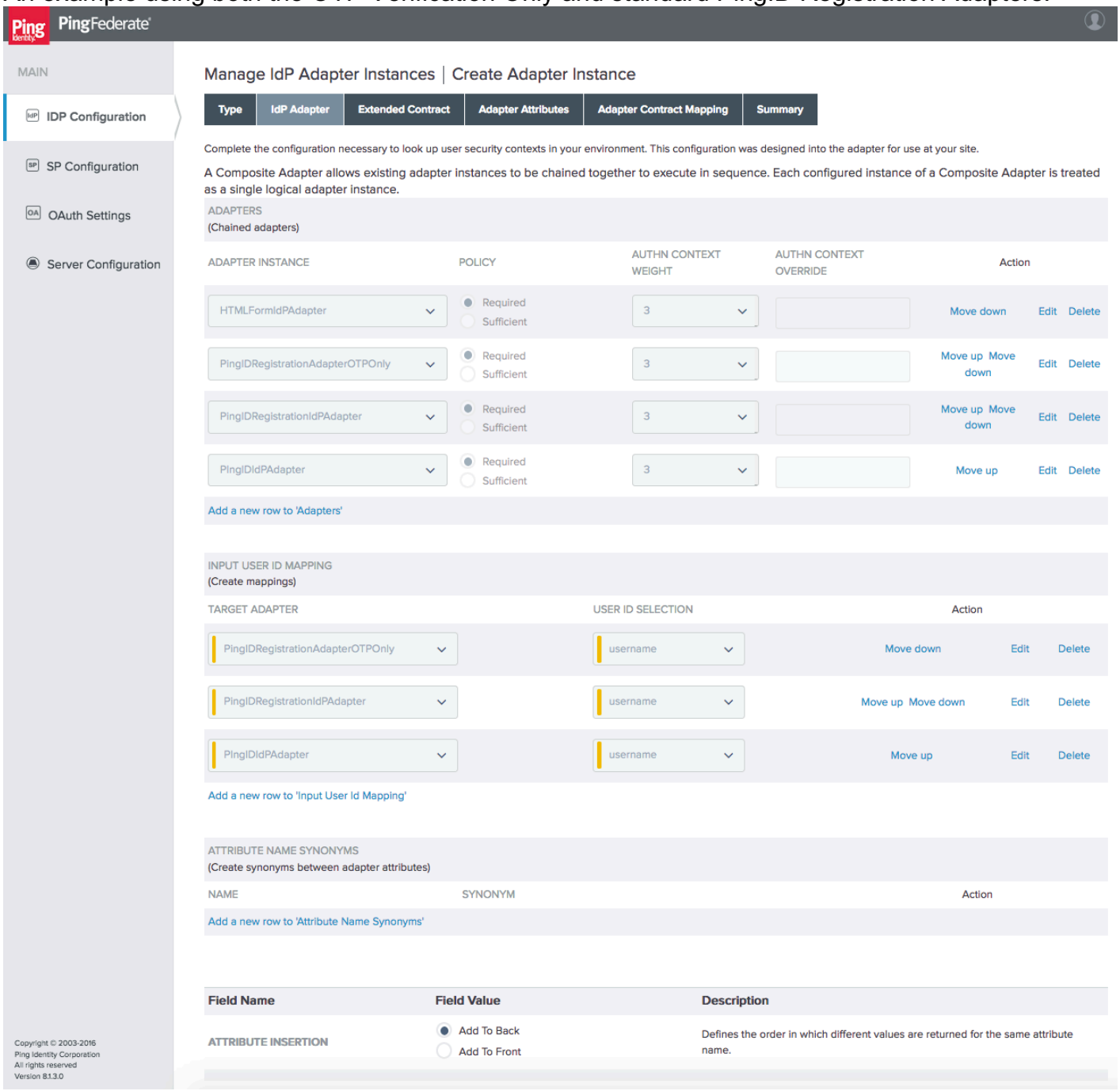
Note: If not configuring the PingID Registration Adapter in a policy tree, use this method.

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** and **Instance Id**, choose **Composite Adapter** and click **Next**.

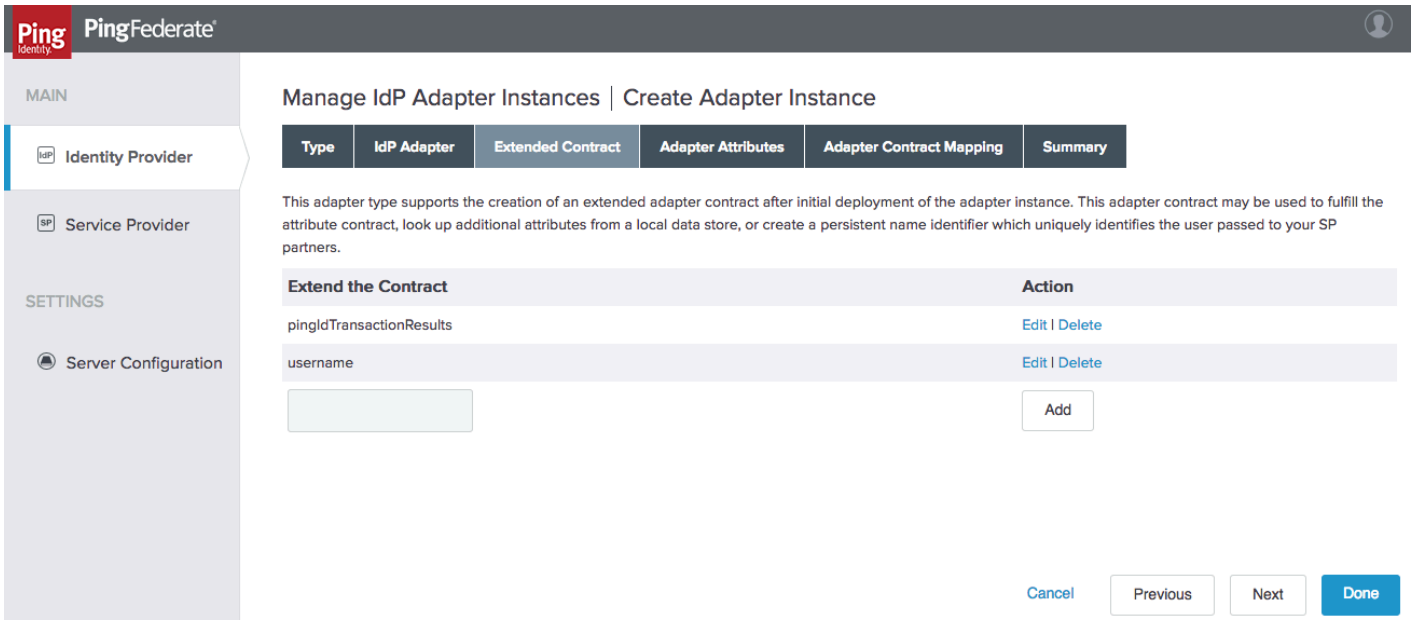


4. Click **Add a new row to 'Adapters,'** add an adapter as the first factor authentication adapter (e.g., the HTML Form Adapter was chosen for this example), and click **Update**. If leveraging an OTP Verification Only PingID Registration Adapter, add that as the second adapter. Otherwise, add the PingID Registration Adapter as the second adapter (or third adapter if the OTP Verification Only PingID Registration Adapter was indeed added as the second one), and click **Update**. Lastly, add the pre-configured PingID Adapter as the last adapter, and click **Update**. Click **Add a new row to 'Input User Id Mapping'** and add a mapping for the PingID Registration Adapter(s) and the PingID Adapter, and click **Update**. Then click **Next**.

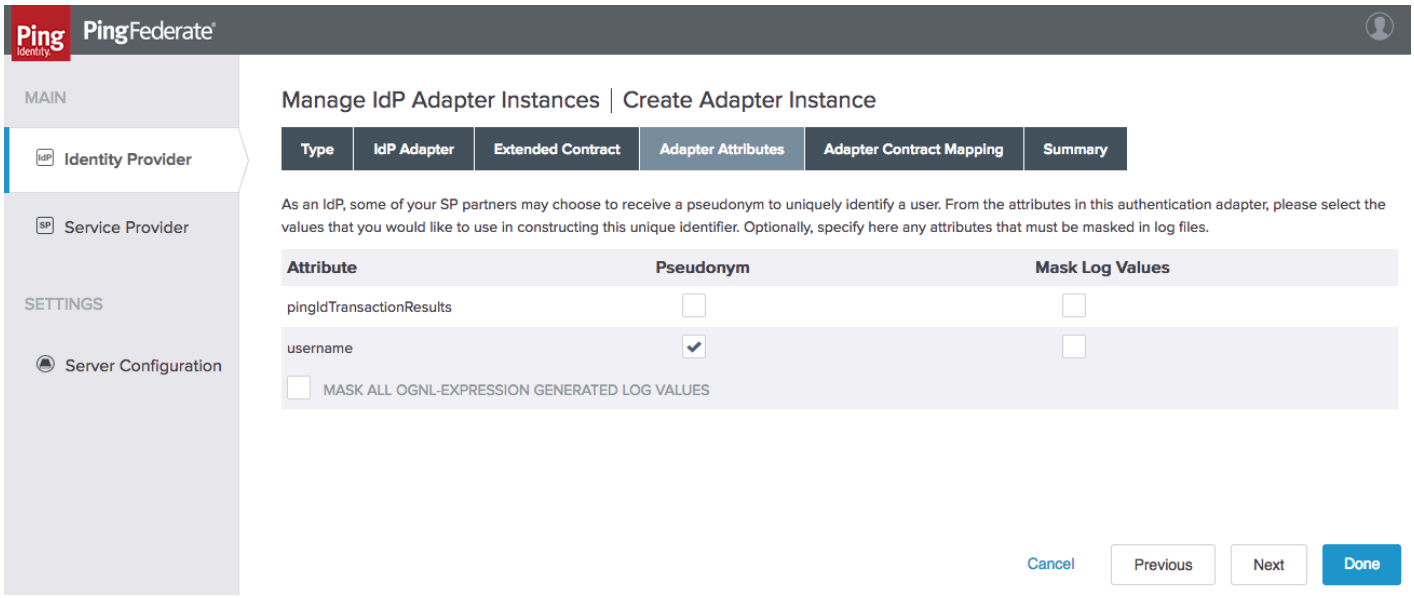
An example using both the OTP Verification Only and standard PingID Registration Adapters:



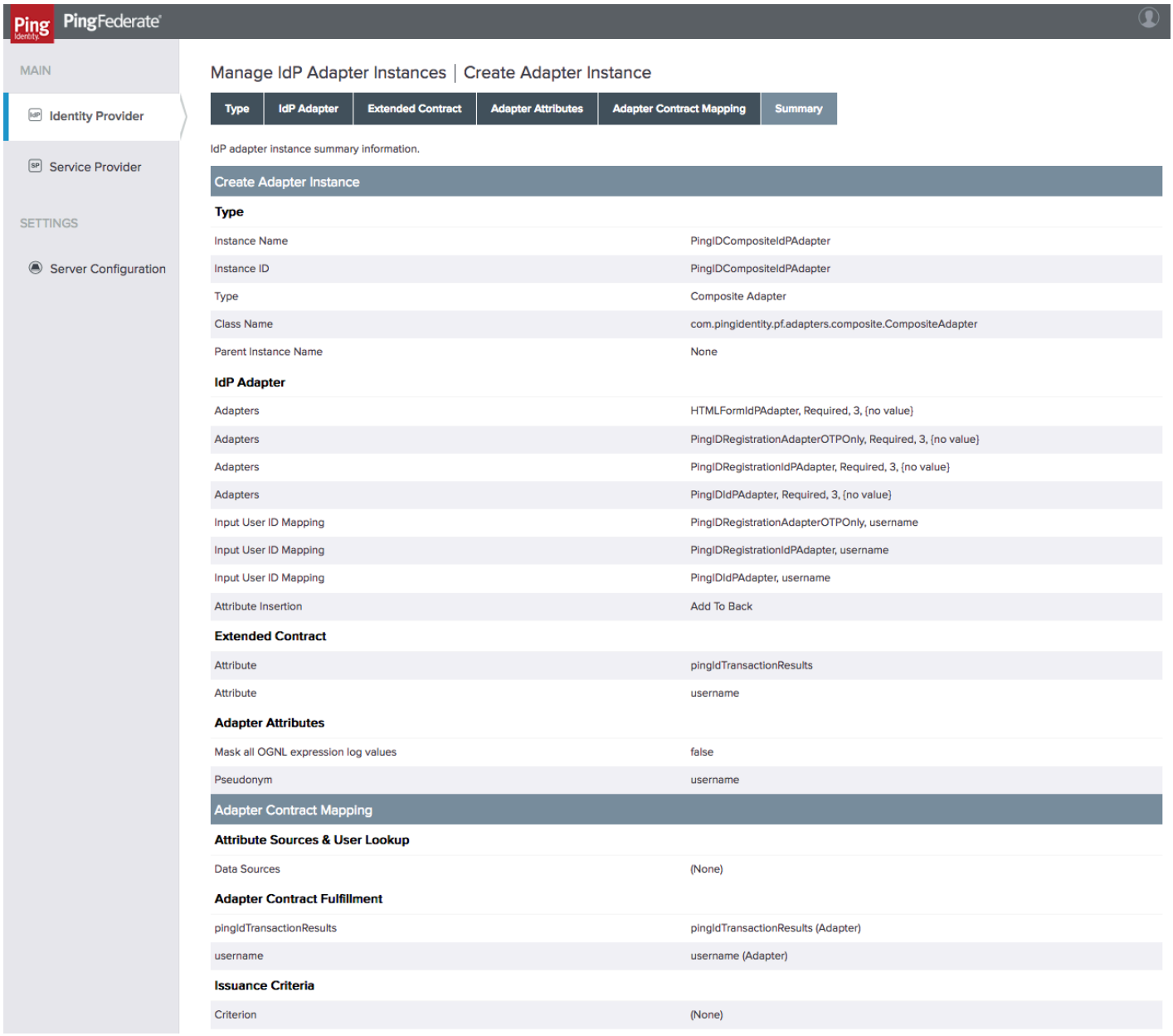
5. **Extend the Contract** by adding **username** and **pingIdTransactionResults**, and then click **Next**.



6. Select **username** as the **Pseudonym** and click **Next**.



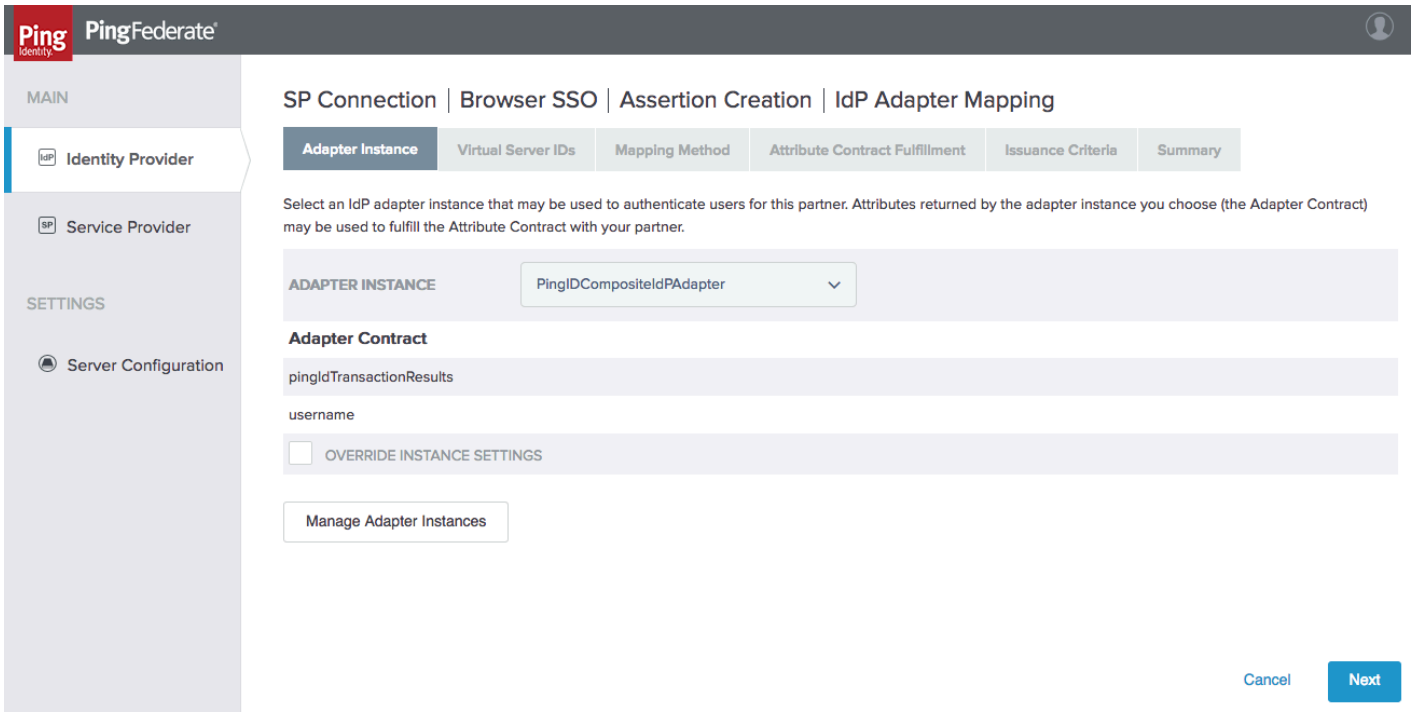
7. Click **Next**.
8. Review the **Summary** and click **Done**.



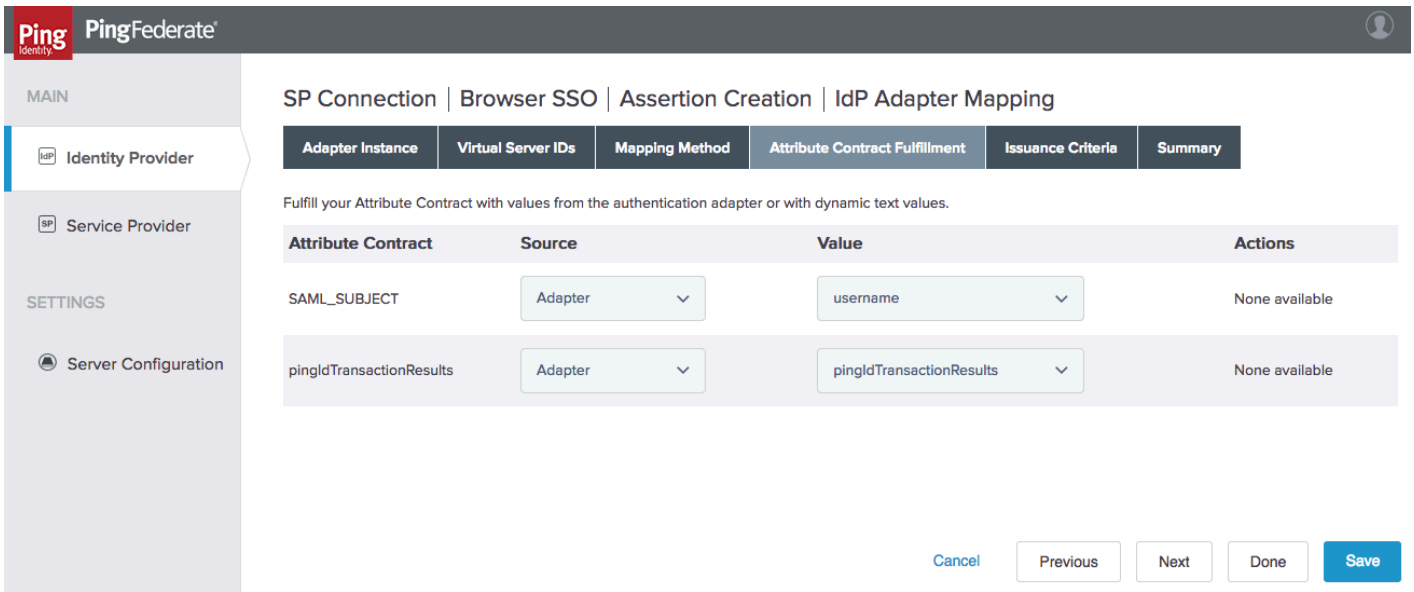
9. Click **Save**.

Configuring the SP Connection to Leverage the Composite Adapter

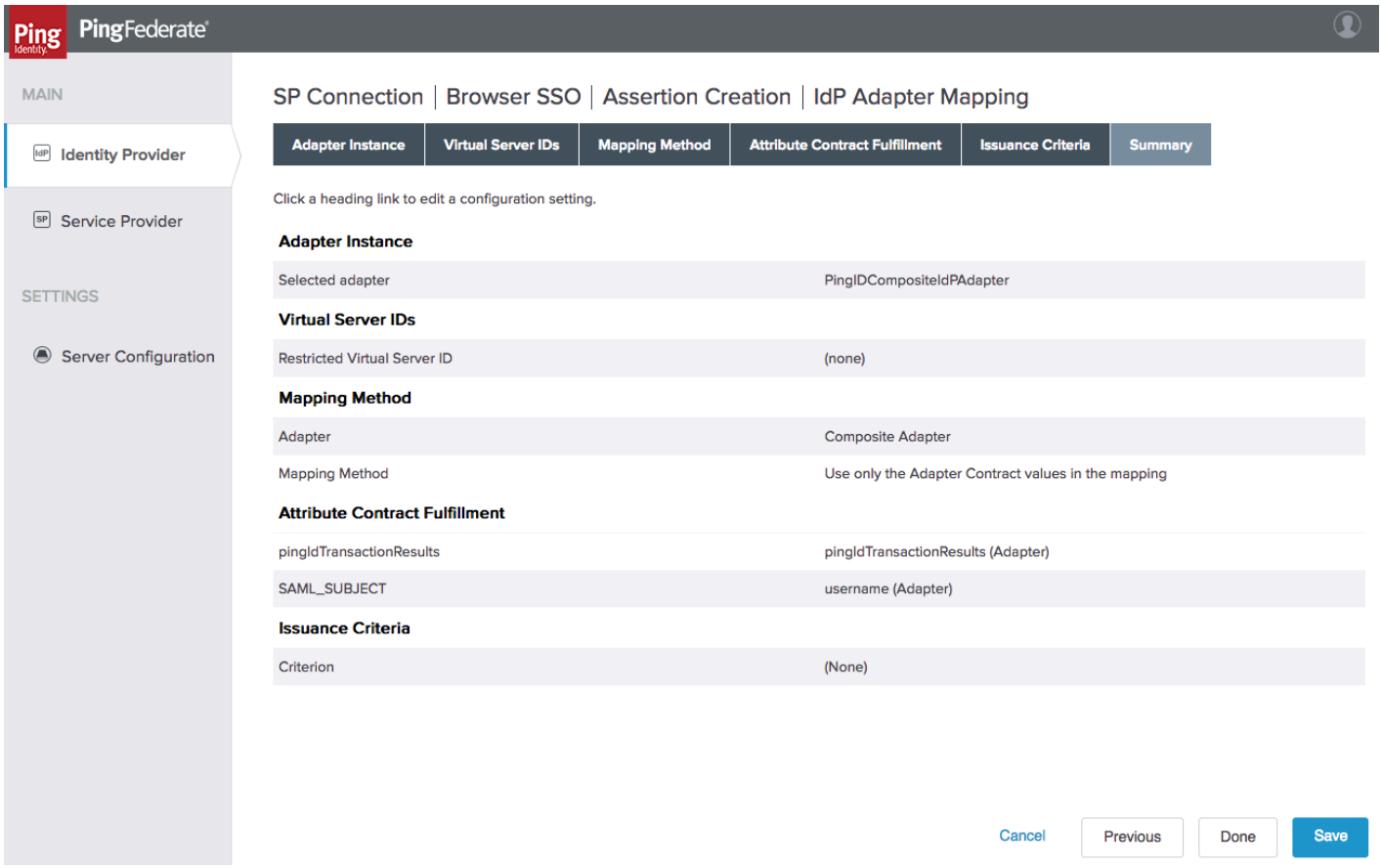
1. Click the SP connection to be modified or create a new SP connection, which should be located under **Identity Provider** >> **SP Connections**.
2. Under **Assertion Creation**, click on **Attribute Contract**, and extend the contract with **pingIdTransactionResults**, and click **Next**.
3. Click **Map New Adapter Instance**. Select the composite adapter that contains the PingID Registration Adapter and click **Next**.



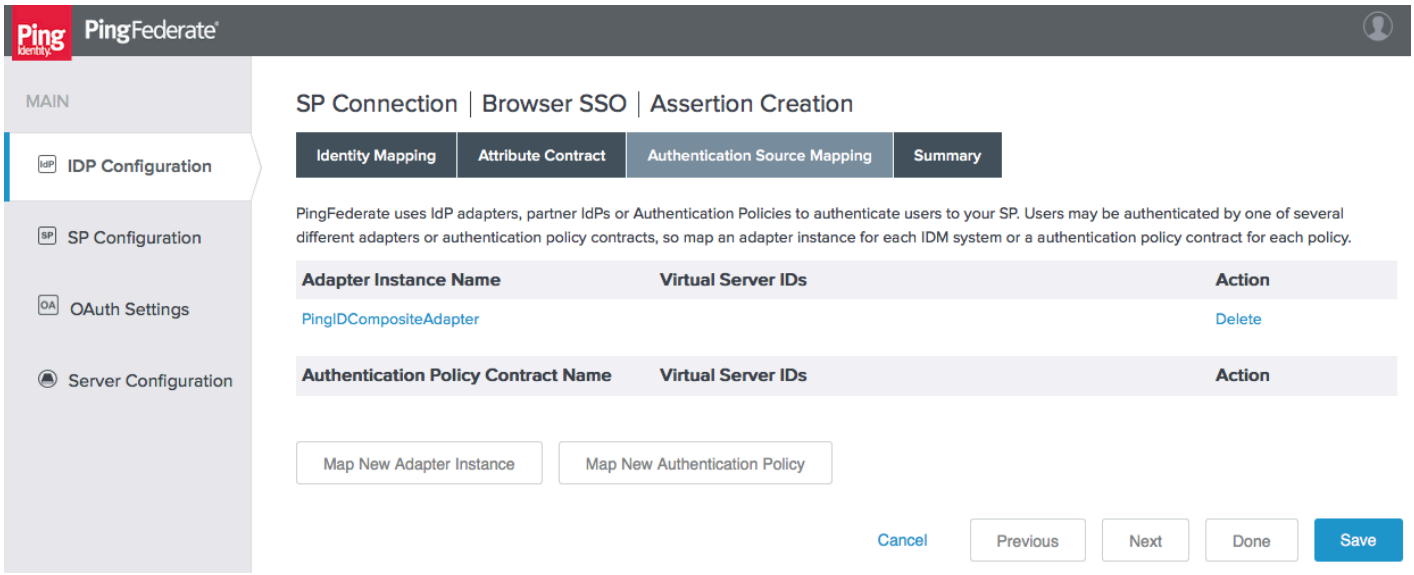
4. Click **Next**.
5. Select the appropriate **Adapter Contract** and click **Next**.
6. Configure the **Attribute Contract Fulfillment** and click **Next**.



7. Click **Next**.
8. Review the **Summary** and click **Done**.



9. Click **Done**.



10. Continue with the rest of the SP connection configuration process.
11. Ensure that the SP connection is **Active**. Click **Save** as a final step to complete the SP connection configuration.

Making an Endpoint Publically Accessible

If the registration adapter is set up to pair a mobile device or the desktop application, a polling process is then started up in the user's browser that checks with PingFederate and ultimately Ping ID. This is to see if the user has finished pairing from the mobile or desktop app. In order to get this functionally working, the following endpoint needs to be accessible to the outside world:

/ext/pingid/registration/status

Managing Old/Used QR Images

Note: This only applies if 'Rely on External QR image Service' is unchecked in the PingID Registration Adapter configuration in the PingFederate administration console.

If the PingID Registration Adapter is set up to generate QR images on the PingFederate server, a method to clean up old/used QR images is highly recommended. If there is no method to clean up old/used QR images, they may accumulate over time and exceed the disk space on the server.

One way to manage old/used QR images is to set up a nightly cron job to remove them if they are older than a certain allotted time (e.g., 24 hours).

A script named *pingid_qrimages_cleanup.sh* can be found in the /dist/scripts/ folder as an example Shell script to run as a cron job. The cron job can be set up as such (this example here says to run the script every day at 11:55 PM server time zone):

```
55 23 * * * /app/scripts/pingid_qrimages_cleanup.sh
```

Please note that it is recommended to test this in a pre-production environment for a week or so to make sure that the cron job and shell script are working properly.

Logging

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

```
<Logger name="com.pingidentity.clientservices.adapter.pingid.registration" level="[ DEBUG
| INFO | WARN | ERROR ]" />
```

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

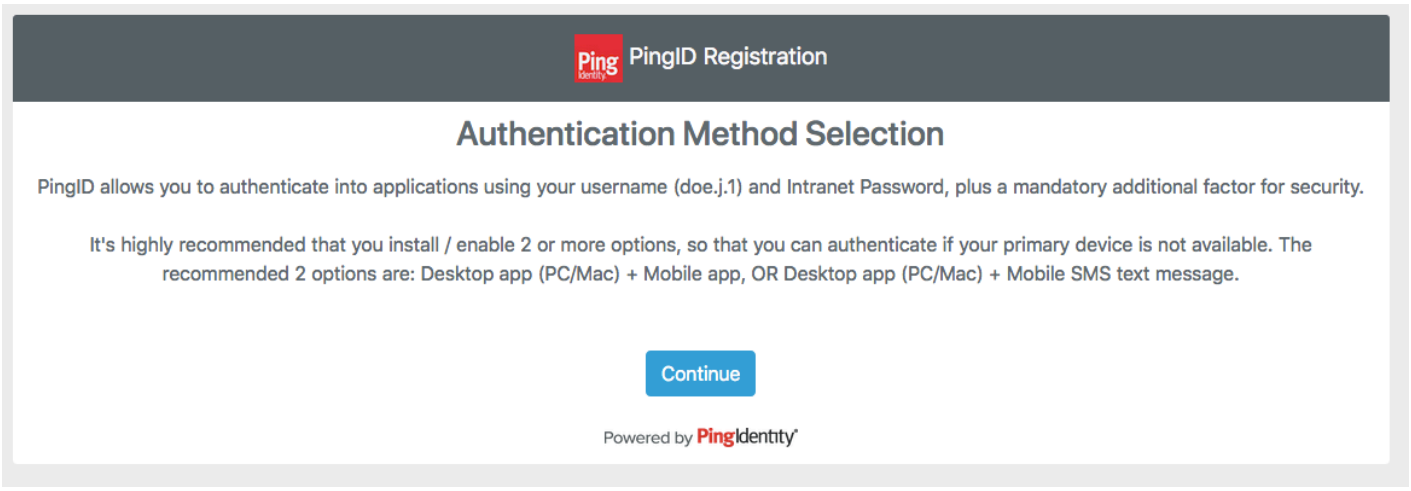
```
<RollingFile name="PingIDRegAdapter" fileName="${sys:pf.log.dir}/pingidregadapter.log"
 filePattern="${sys:pf.log.dir}/pingidregadapter.%d{yyyy-MM-dd}.log"
 ignoreExceptions="false">
        <PatternLayout>
                <!-- Uncomment this if you want to use UTF-8 encoding instead of system's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

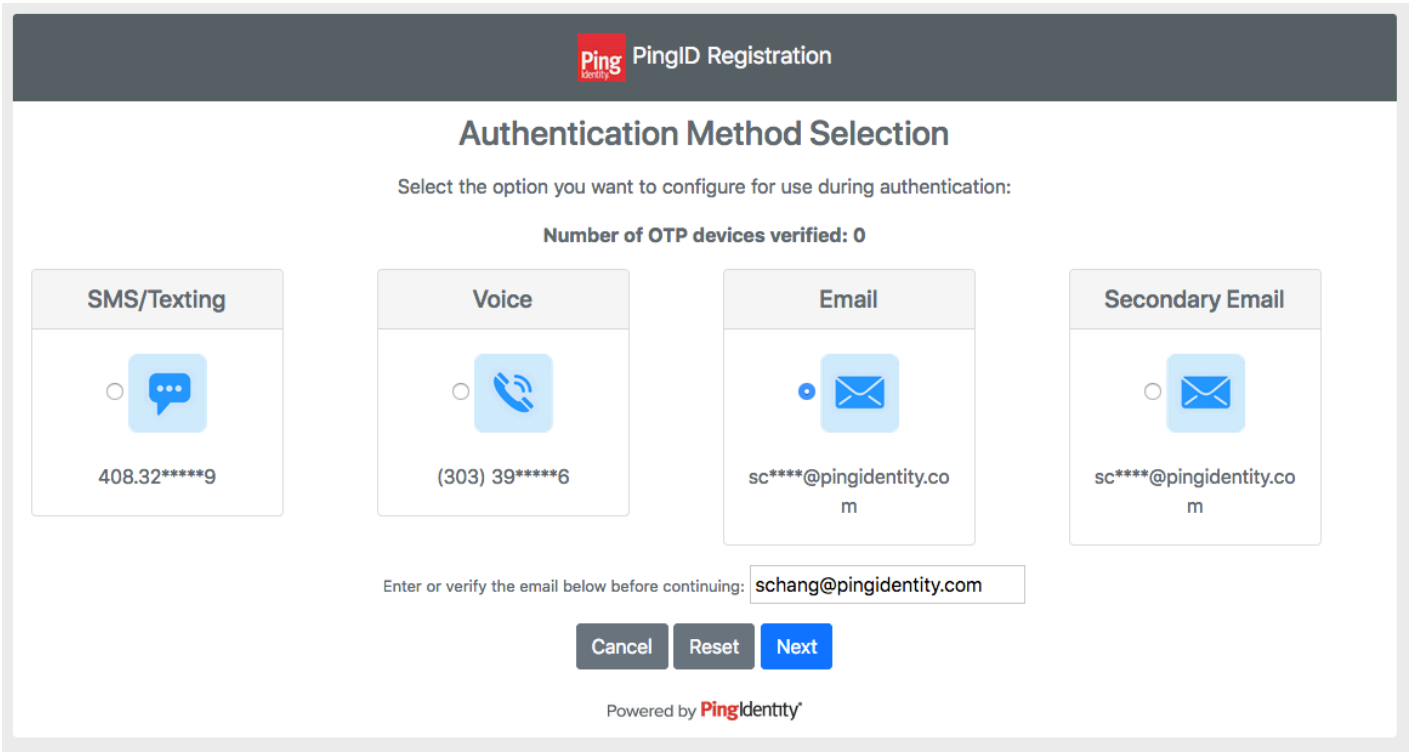
```
        </PatternLayout>
        <Policies>
            <TimeBasedTriggeringPolicy />
        </Policies>
    </RollingFile>

    <Logger name="com.pingidentity.clientservices.adapter.pingid.registration"
    level="[ DEBUG | INFO | WARN | ERROR ]" additivity="false" includeLocation="true">
        <appender-ref ref="PingIDRegAdapter" />
    </Logger>
```

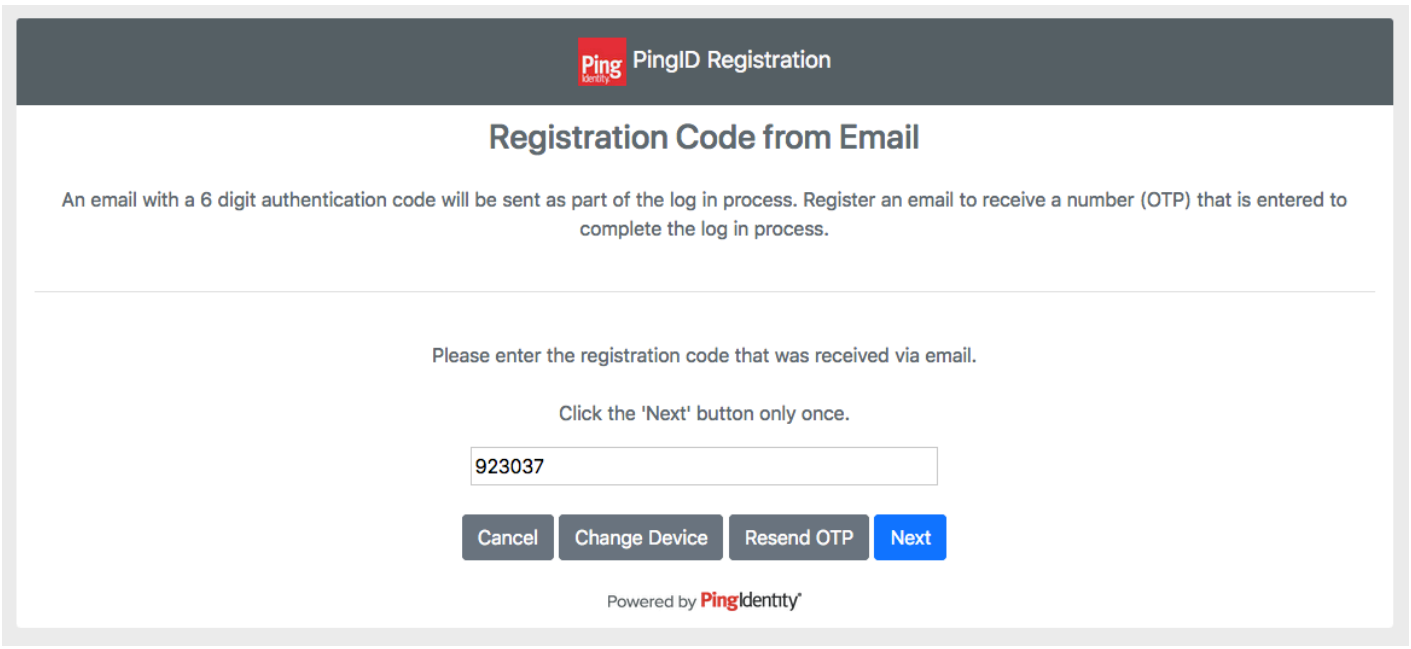
Detailed training on using Log4j in PingFederate can be found at:
https://ping.force.com/Support/PingIdentityKnbSearchHome?searchText=log4j

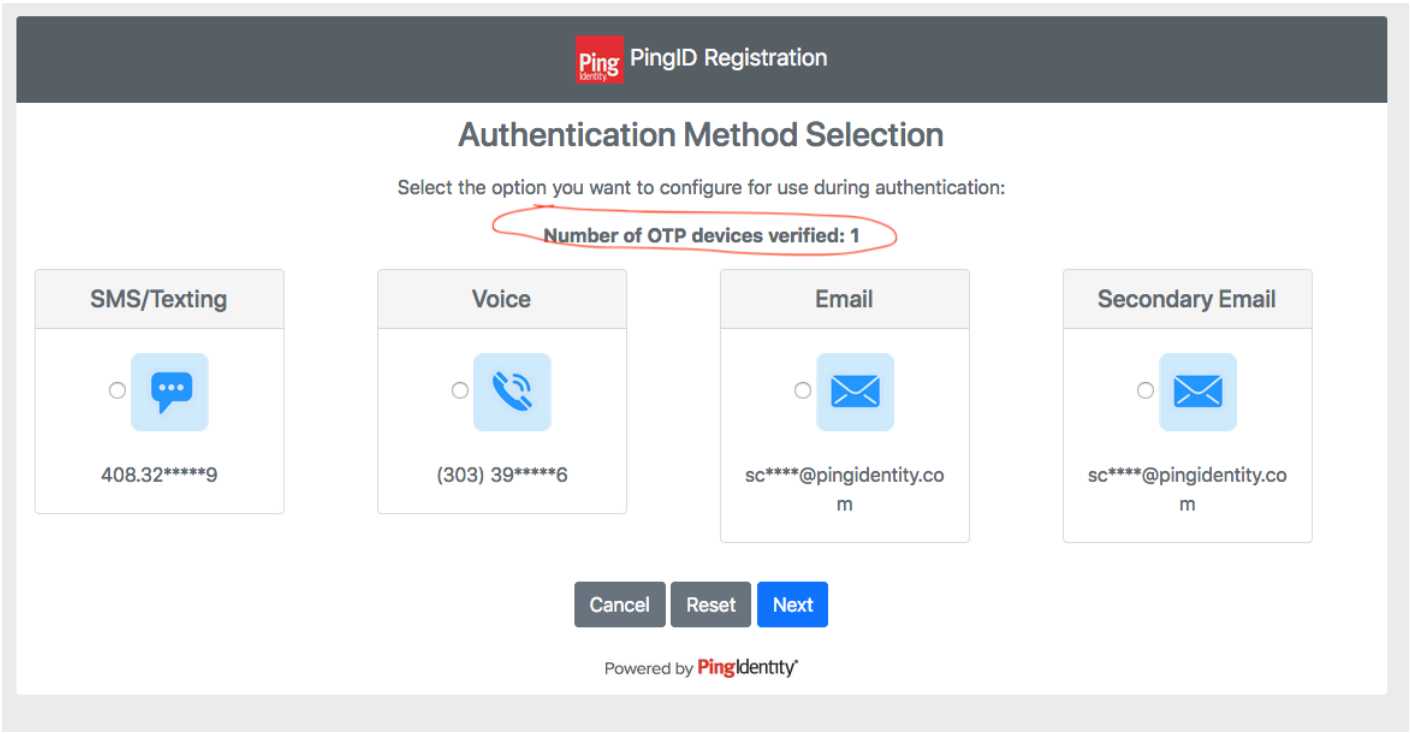
Example Flows

Example of an OTP Verification Only PingID Registration flow:

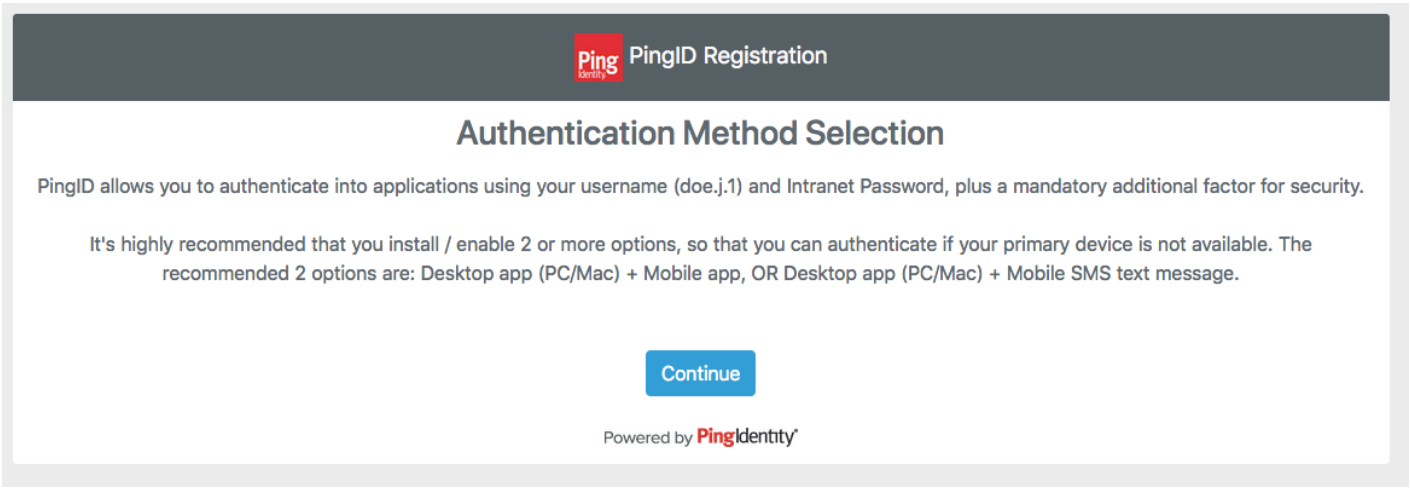


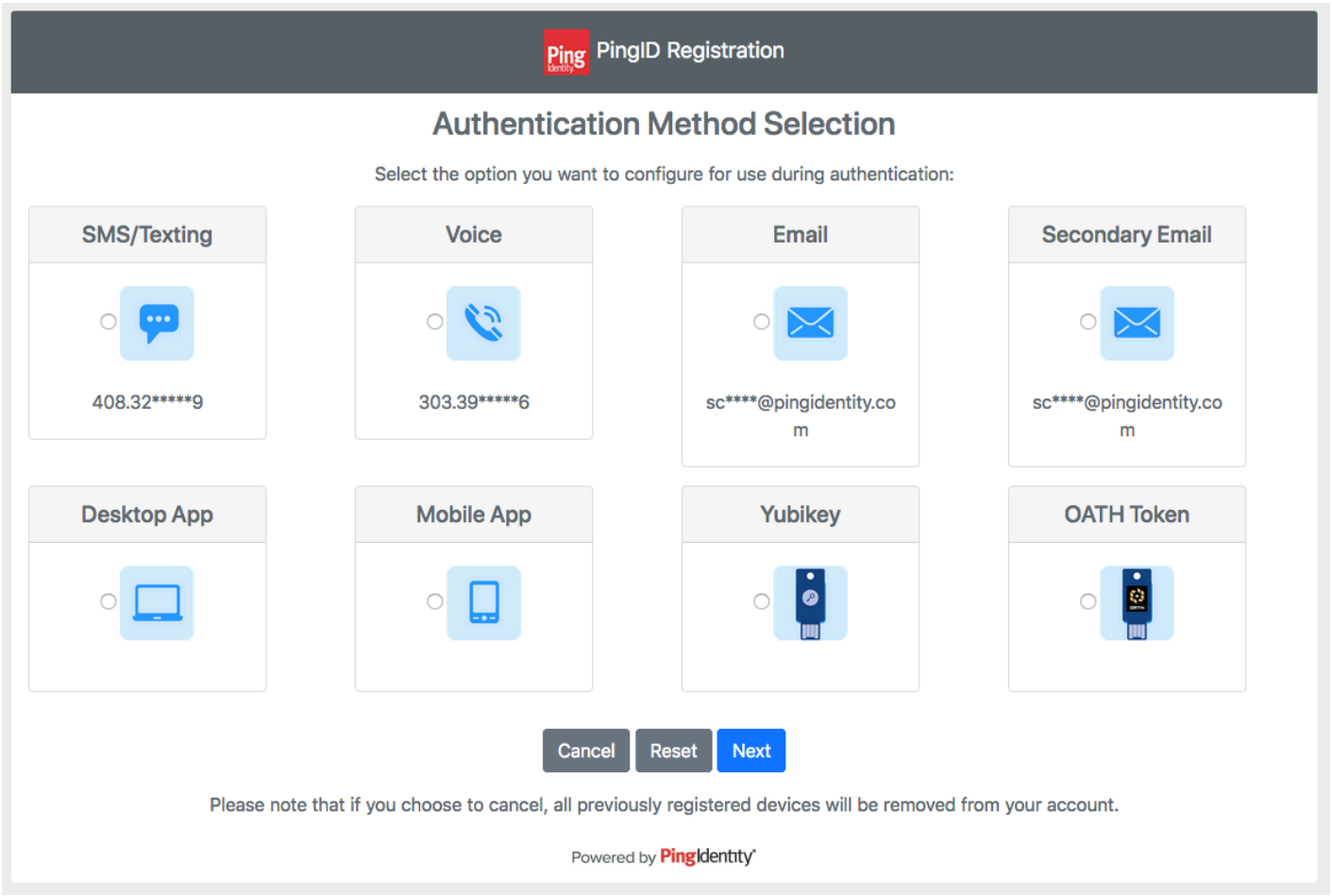

PingID Registration
Authentication Method Selection
Select the option you want to configure for use during authentication:
Number of OTP devices verified: 0
SMS/Texting
408.32*****9
Voice
(303) 39*****6
Email
sc****@pingidentity.com
Secondary Email
sc****@pingidentity.com
Enter or verify the email below before continuing:
schang@pingidentity.com
Cancel
Reset
Next
Powered by PingIdentity


PingID Registration
Registration Code from Email
An email with a 6 digit authentication code will be sent as part of the log in process. Register an email to receive a number (OTP) that is entered to complete the log in process.
Please enter the registration code that was received via email.
Click the 'Next' button only once.
923037
Cancel
Change Device
Resend OTP
Next
Powered by PingIdentity

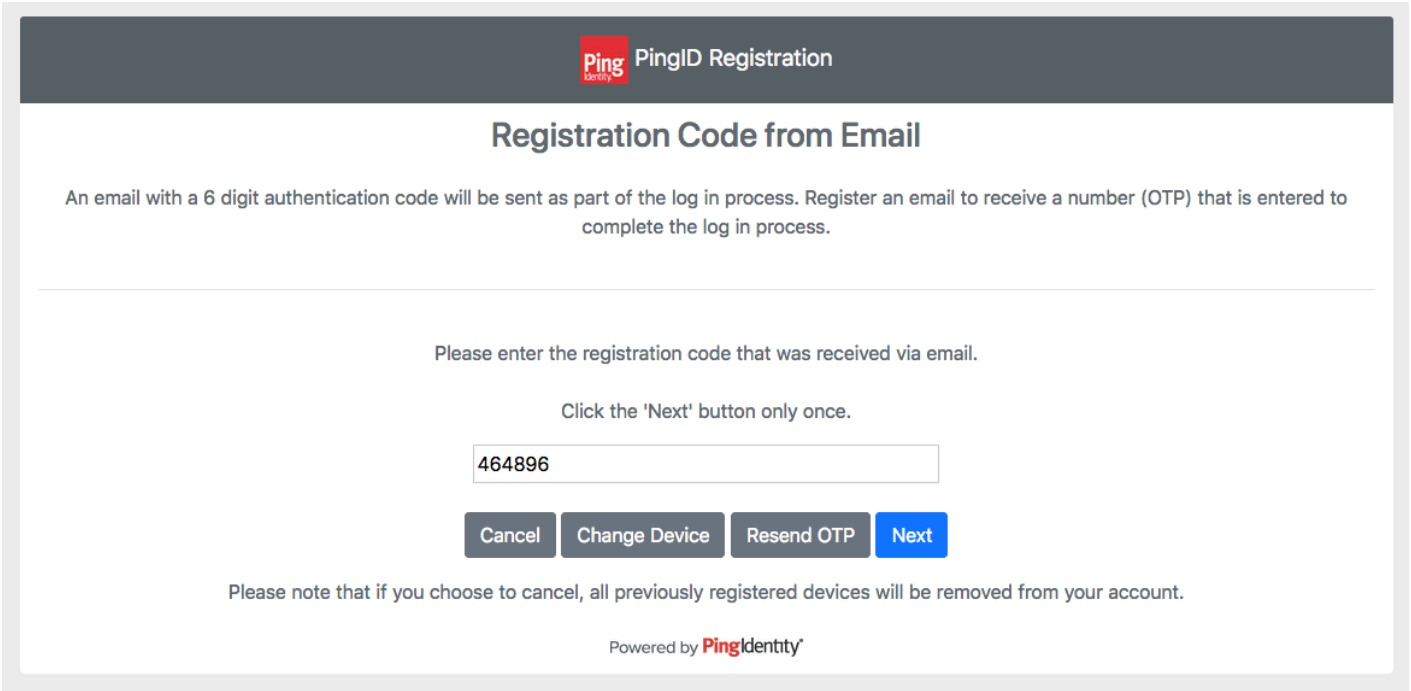


Example of a standard PingID Registration flow:

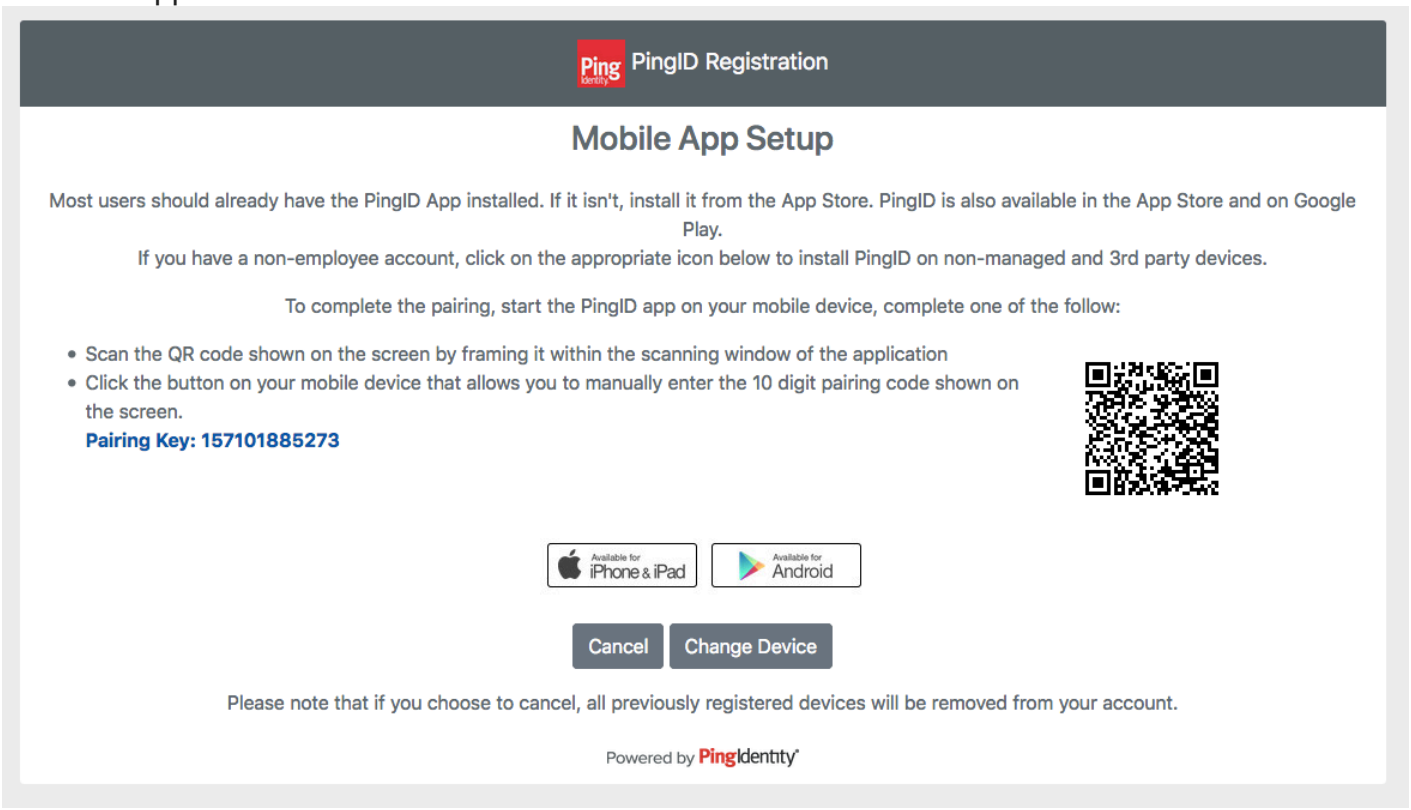




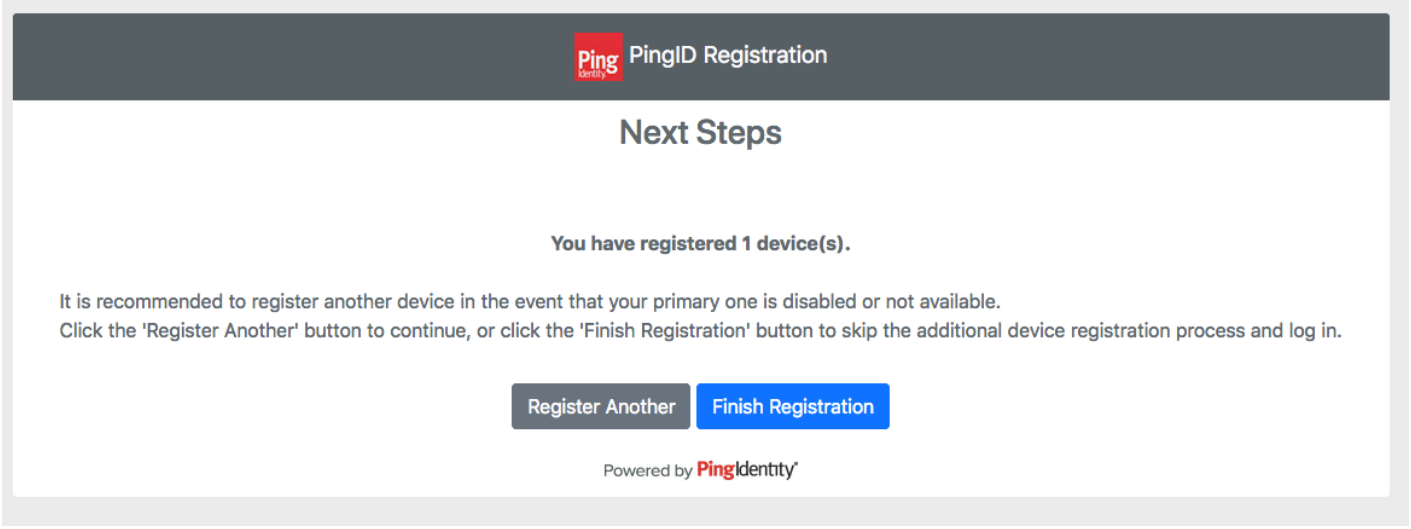
If Email is chosen:



If Mobile App is chosen:



After pairing with any device method:



If ‘Finish Registration’ button is clicked: