PingFederate®

Tomcat Integration Kit v1.1.0

User Guide

PingFederate Tomcat Integration Kit User Guide
Version 1.1.0
July 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

This user guide is intended for use by PingFederate clients, with the need to integrate SSO with applications leveraging the Apache Tomcat web server. The Tomcat Integration Kit provides the ability to pass headers to the consuming service provider application, after the user successfully authenticates.

Prerequisites

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

- A functional PingFederate environment, version 9.2.3.0+
- A functional Tomcat environment
- JDK version 8+
- An IdP adapter, such as an HTML form adapter
- Agentless Integration Kit V1.1

Installation

From *pf-tomcat-integration-kit-1.1.0.zip*:

1. Stop your Tomcat server
2. Copy /dist/pf-tomcat-integration-kit-1.1.0.jar to <YourTomcatInstall>/lib/
3. Copy /dist/apis/json-simple.jar to <YourTomcatInstall>/lib/
4. Modify catalina.sh or catalina.bat (depending on your Tomcat platform)
    a. Go to <YourTomcatInstall>/bin/
    b. Make a copy of catalina.sh or catalina.bat and append .orig to the end (i.e., catalina.sh.orig or catalina.bat.orig)
    c. Follow the instructions in /dist/bin/catalina.sh or /dist/bin/catalina.bat from the zip
    d. Save catalina.sh or catalina.bat
    e. When starting up Tomcat, this will be printed before the ‘Tomcat started.’:

    ```
    Using JAVA_OPTS:     -Djava.security.auth.login.config==<YourPath>/tomcat/conf/jaas.config
    Tomcat started.
    ```

5. Copy /dist/conf/jaas.config to <YourTomcatInstall>/conf/
6. Modify server.xml

    Note: An Agentless SP adapter must already be configured in PingFederate before going through this step. See ***Configuring the Agentless SP Adapter*** under ***Configuration***.

    a. Go to <YourTomcatInstall>/conf/
    b. Make a copy of server.xml and append .orig to the end (i.e., server.xml.orig)
    c. Append to server.xml within the <Host>…</Host> tags near the bottom of the file:
    Note: An example can be found in /dist/conf/server.xml.

    ```
    <Valve className="com.pingidentity.clientservices.product.tomcat.TomcatAdapter"
                    pfProto="[http protocol (https is recommended)]"
                    pfHost="[hostname]"
                    pfPort="[port]"
                    pfInstance="[Agentless SP adapter name from PingFederate]"
    ```

```
                    pfUser=”[Agentless SP adapter User Name]"
                    pfPass="[Agentless SP adapter Password]"
                    pfPrefix="[header prefix]"
                    pfSecurityLevel="[security level – see below for definitions]"
                    pfClientKeystoreAlias="[client keystore alias if security level is 3]"
                    pfSerialNumber="[serial number(s) if security level is 2]"
                    pfSecureHeader=”[true or false – if true, must go through https]”
                    pfEnableLogging=”[true or false]”/>
```

For example:

```
<Valve className="com.pingidentity.clientservices.product.tomcat.TomcatAdapter"
                    pfProto="https"
                    pfHost="localhost"
                    pfPort="9031"
                    pfInstance="TomcatAgentlessSPAdapter"
                    pfUser="admin"
                    pfPass="2Federate"
                    pfPrefix="PF_AUTH_"
                    pfSecurityLevel="1"
                    pfClientKeystoreAlias=""
                    pfSerialNumber=""
                    pfSecureHeader=”true”
                    pfEnableLogging=”true” />
```

d. Append to server.xml within the <Engine>…</Engine> tags near the bottom of the file:
   Note: This can be found in /dist/conf/server.xml.

```
<Realm className=”org.apache.catalina.realm.JAASRealm”
                    appName=”TomcatLogin”
                    userClassNames=”com.pingidentity.clientservices.product.tomcat.jaas.UserPrincipal”
                    roleClassNames=”com.pingidentity.clientservices.product.tomcat.jaas.RolePrincipal” />
```

e. Save server.xml

7. Copy /dist/conf/WEB-INF/* to <YourTomcatInstall>/webapps/<YourApp>/WEB-INF/
8. Modify web.xml
   a. Go to <YourTomcatInstall>/webapps/<YourApp>/WEB-INF/
   b. Open up web.xml
   c. Modify only the bolded between the following tags according to your resource protection policies:

```
<security-constraint>
        <display-name>protected</display-name>
        <web-resource-collection>
                <web-resource-name>[Main App Name] (protected)</web-resource-name>
                <url-pattern>/[Main App Folder if any or leave as wildcard]/*</url-pattern>
        </web-resource-collection>
        <auth-constraint>
                <role-name>standard</role-name>
        </auth-constraint>
</security-constraint>
```

For example:

```
<security-constraint>
        <web-resource-collection>
                <web-resource-name>MyApp (protected)</web-resource-name>
                <url-pattern>/MyApp/*</url-pattern>
        </web-resource-collection>
        <auth-constraint>
                <role-name>standard</role-name>
        </auth-constraint>
</security-constraint>
```

Or using just wildcard:

```
<security-constraint>
        <web-resource-collection>
                <web-resource-name>MyApp (protected)</web-resource-name>
                <url-pattern>/*</url-pattern>
        </web-resource-collection>
        <auth-constraint>
                <role-name>standard</role-name>
        </auth-constraint>
</security-constraint>
```

If additional applications need to be protected, make additional copies of <security-constraint>…</security-constraint> and modify accordingly.

Do not modify anything between the following tags:

- <auth-constraint>…</auth-constraint>*
- <security-role>…</security-role>*
- <security-constraint><display-name>unprotected</display-name>…</security-constraint>
- <login-config>…</login-config>

d. Save web.xml

Note: Role functionality is basic in this Tomcat Integration Kit version. The static role value is assigned to 'standard.'

9. Copy /dist/html/MyApp/pf/* to <YourTomcatInstall>/webapps/<YourApp>/pf/
10. Optional (for testing purposes only – see ***Testing*** section):
    a. Copy /dist/html/MyApp/* to <YourTomcatInstall>/webapps/MyApp/
        i. Follow steps in ***Modifying /pf/ JSP*** under ***Configuration***.
    b. Copy /dist/conf/WEB-INF/* to <YourTomcatInstall>/webapps/MyApp/WEB-INF/
        i. No changes to web.xml are needed
    c. Remember to remove these files when done using this example.
11. Repeat all above steps on all Tomcat web servers
12. Start Tomcat

Security Levels

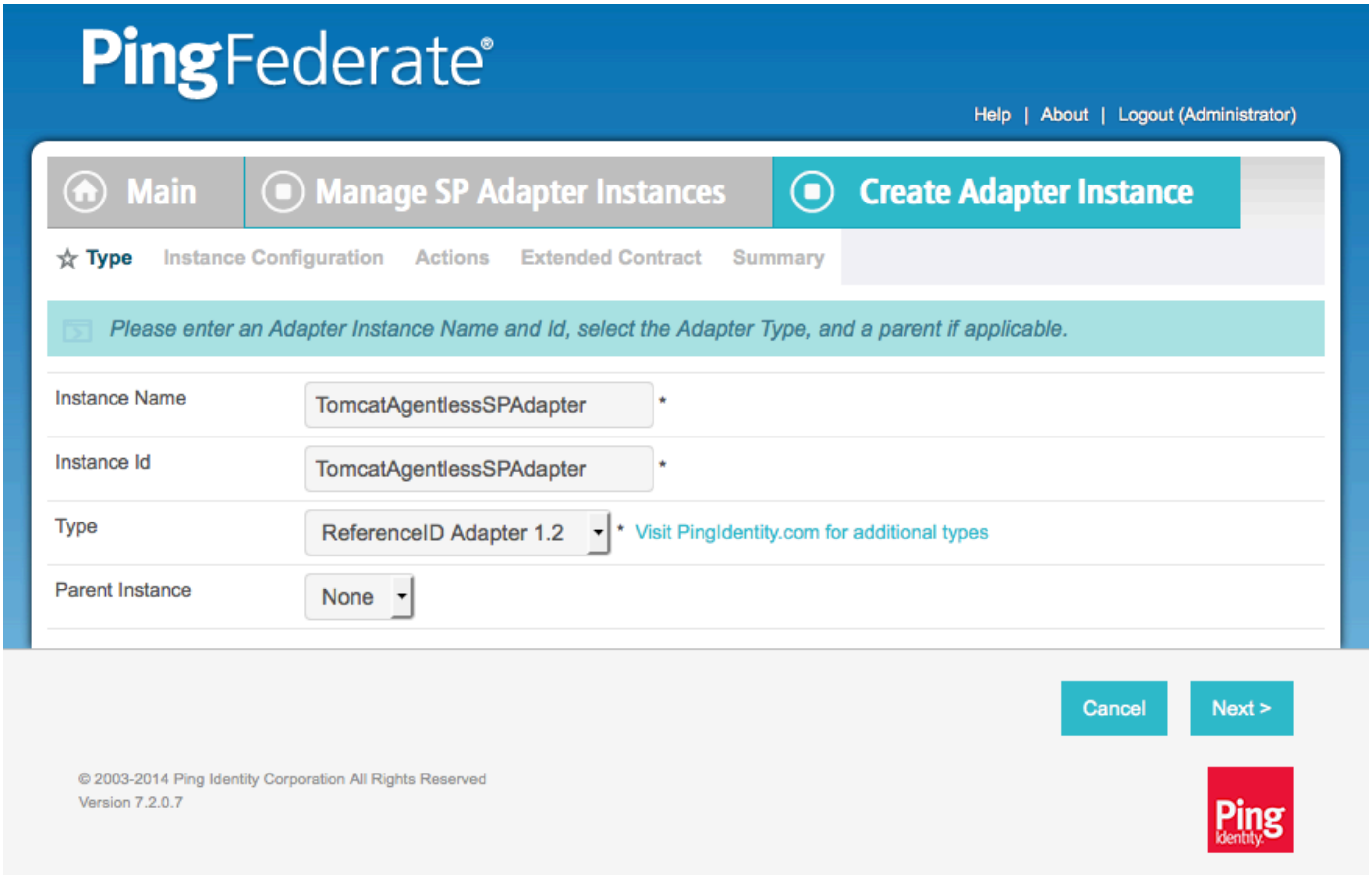
Security Level	**Type**	**Description**
1	Trust all certificates	All certificates will be accepted by default. This

		option bypasses certificate checks for agentless authentication transactions.
2	Trust specified certificate	Only the specified certificate is trusted and checked during agentless authentication transactions. To configure, enter the certificate’s serial number in *pfSerialNumber* in the Valve configuration (e.g., 01:44:BC:9B:84:A2). Add additional certificates with a pipe (‘|’) in between (e.g., 01:44:BC:9B:84:A2|01:44:BC:BA:7B:DD). The specified certificate’s serial number can be found under ***Security*** in PingFederate.
3	Mutual SSL authentication	Mutual SSL authentication will be used to secure agentless authentication transactions. To configure, the same trusted certificate must be installed on both client (Tomcat) and server (PingFederate). Enter the certificate’s client keystore alias in *pfClientKeystoreAlias* in the Valve configuration (e.g., 6s7tmxpno1vosapr4smfthtod). The trusted certificate’s client keystore alias can be found under ***Security*** in PingFederate.

Configuration

Configuring the Agentless SP Adapter

1. Log into the PingFederate admin console and click **Adapters** under **SP Configuration** >> **Application Integration Settings**.
2. Click **Create New Instance…**
3. Enter the **Instance Name** and **Instance ID**, choose **ReferenceID Adapter 1.2** as the **Type**, and click **Next**.

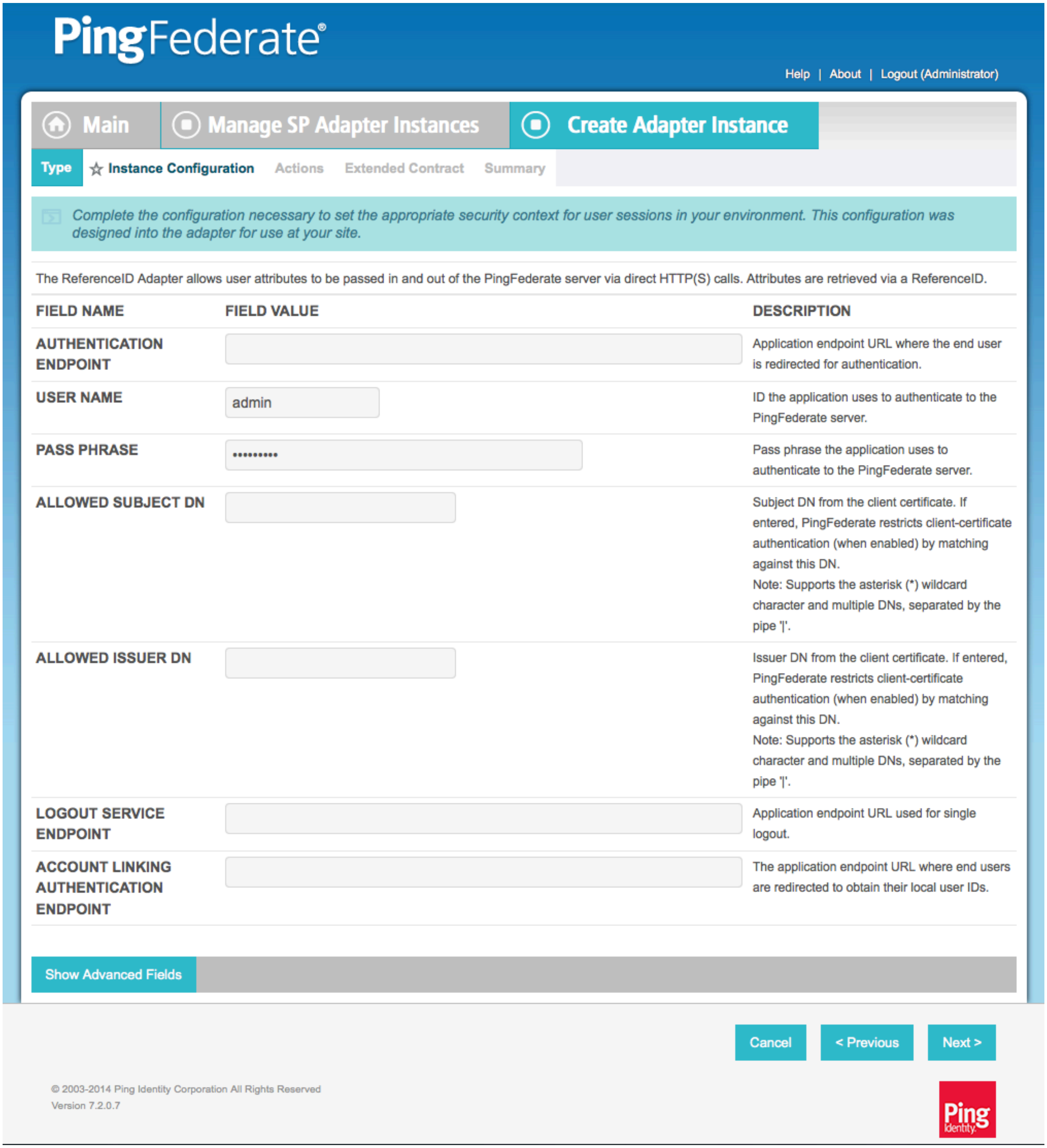


Please enter an Adapter Instance Name and Id, select the Adapter Type, and a parent if applicable.

Instance Name	TomcatAgentlessSPAdapter *
Instance Id	TomcatAgentlessSPAdapter *
Type	ReferenceID Adapter 1.2 * Visit PingIdentity.com for additional types
Parent Instance	None

© 2003-2014 Ping Identity Corporation All Rights Reserved
Version 7.2.0.7

4. Enter a **User Name** and **Pass Phrase**. Fill out or leave the rest as is, and click **Next**.

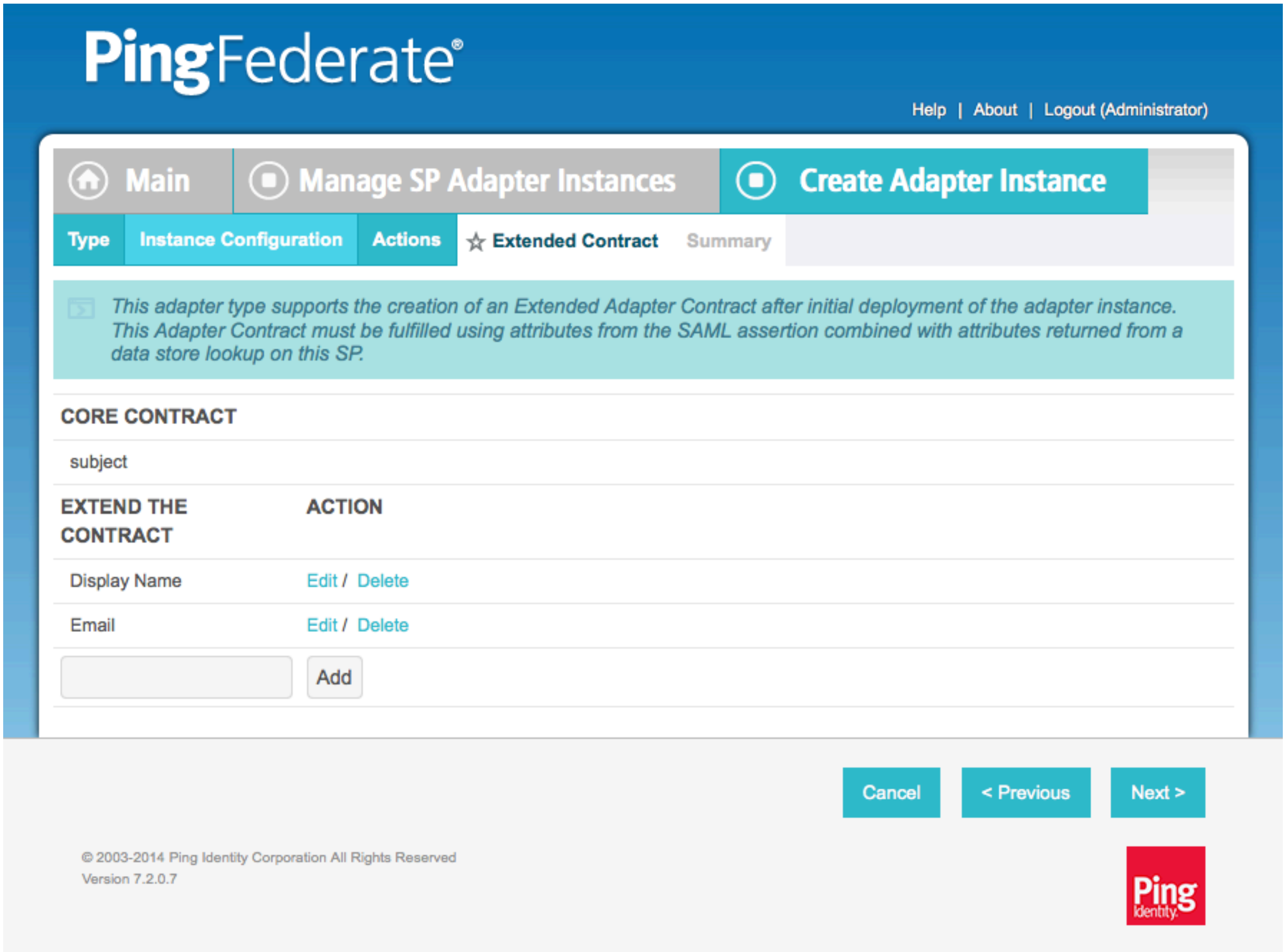


Complete the configuration necessary to set the appropriate security context for user sessions in your environment. This configuration was designed into the adapter for use at your site.

The ReferenceID Adapter allows user attributes to be passed in and out of the PingFederate server via direct HTTP(S) calls. Attributes are retrieved via a ReferenceID.

FIELD NAME	FIELD VALUE	DESCRIPTION
AUTHENTICATION ENDPOINT		Application endpoint URL where the end user is redirected for authentication.
USER NAME	admin	ID the application uses to authenticate to the PingFederate server.
PASS PHRASE	•••••••••	Pass phrase the application uses to authenticate to the PingFederate server.
ALLOWED SUBJECT DN		Subject DN from the client certificate. If entered, PingFederate restricts client-certificate authentication (when enabled) by matching against this DN. Note: Supports the asterisk (*) wildcard character and multiple DNs, separated by the pipe '|'.
ALLOWED ISSUER DN		Issuer DN from the client certificate. If entered, PingFederate restricts client-certificate authentication (when enabled) by matching against this DN. Note: Supports the asterisk (*) wildcard character and multiple DNs, separated by the pipe '|'.
LOGOUT SERVICE ENDPOINT		Application endpoint URL used for single logout.
ACCOUNT LINKING AUTHENTICATION ENDPOINT		The application endpoint URL where end users are redirected to obtain their local user IDs.

5. Click **Next**.
6. **Extend the Contract** if needed. Click **Next**.

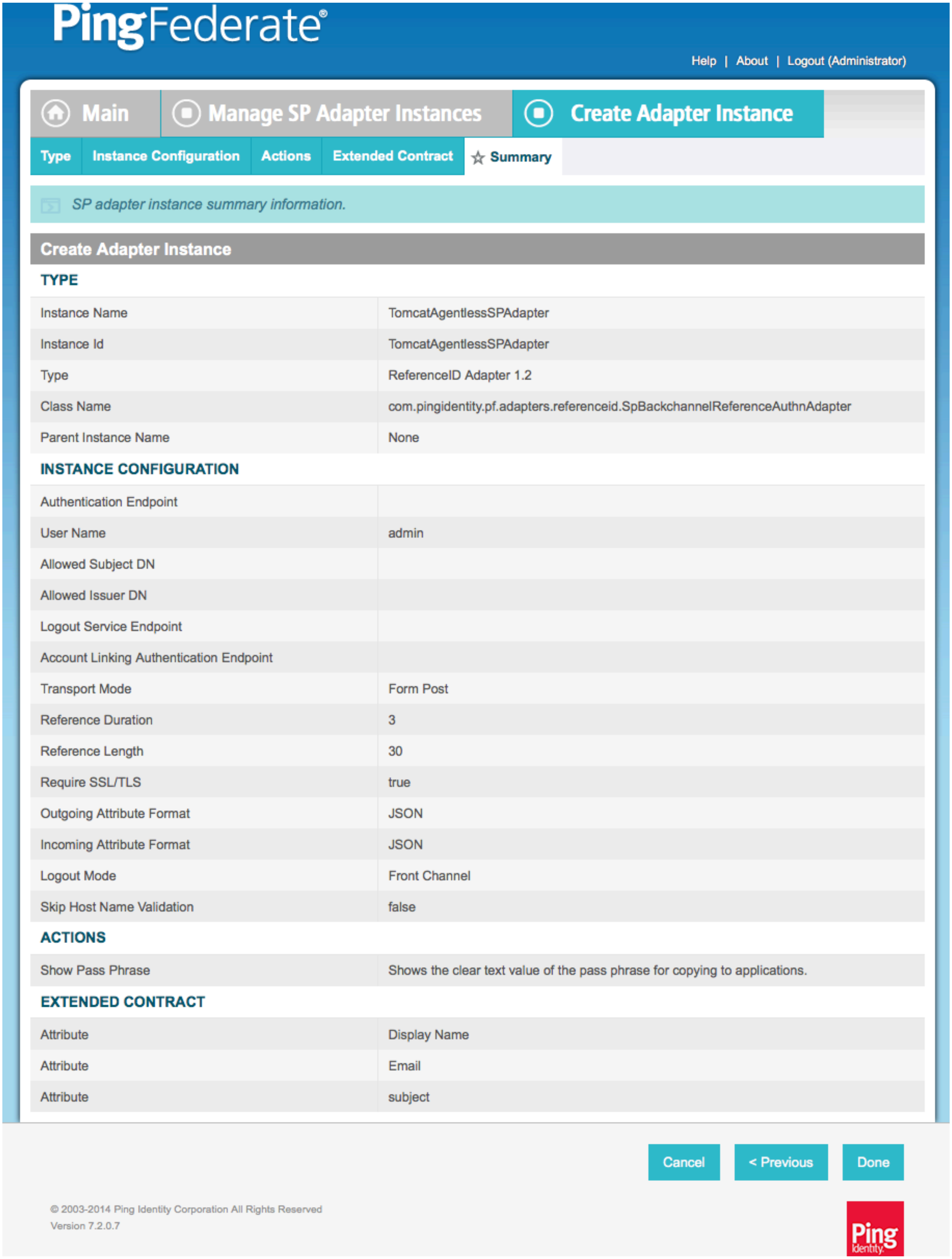


This adapter type supports the creation of an Extended Adapter Contract after initial deployment of the adapter instance. This Adapter Contract must be fulfilled using attributes from the SAML assertion combined with attributes returned from a data store lookup on this SP.

CORE CONTRACT	
subject	
EXTEND THE CONTRACT	**ACTION**
Display Name	Edit / Delete
Email	Edit / Delete
	Add

© 2003-2014 Ping Identity Corporation All Rights Reserved
Version 7.2.0.7

7. Confirm the **Summary** and click **Done**.



SP adapter instance summary information.

Create Adapter Instance

TYPE

Instance Name	TomcatAgentlessSPAdapter
Instance Id	TomcatAgentlessSPAdapter
Type	ReferenceID Adapter 1.2
Class Name	com.pingidentity.pf.adapters.referenceid.SpBackchannelReferenceAuthnAdapter
Parent Instance Name	None

INSTANCE CONFIGURATION

Authentication Endpoint	
User Name	admin
Allowed Subject DN	
Allowed Issuer DN	
Logout Service Endpoint	
Account Linking Authentication Endpoint	
Transport Mode	Form Post
Reference Duration	3
Reference Length	30
Require SSL/TLS	true
Outgoing Attribute Format	JSON
Incoming Attribute Format	JSON
Logout Mode	Front Channel
Skip Host Name Validation	false

ACTIONS

Show Pass Phrase	Shows the clear text value of the pass phrase for copying to applications.

EXTENDED CONTRACT

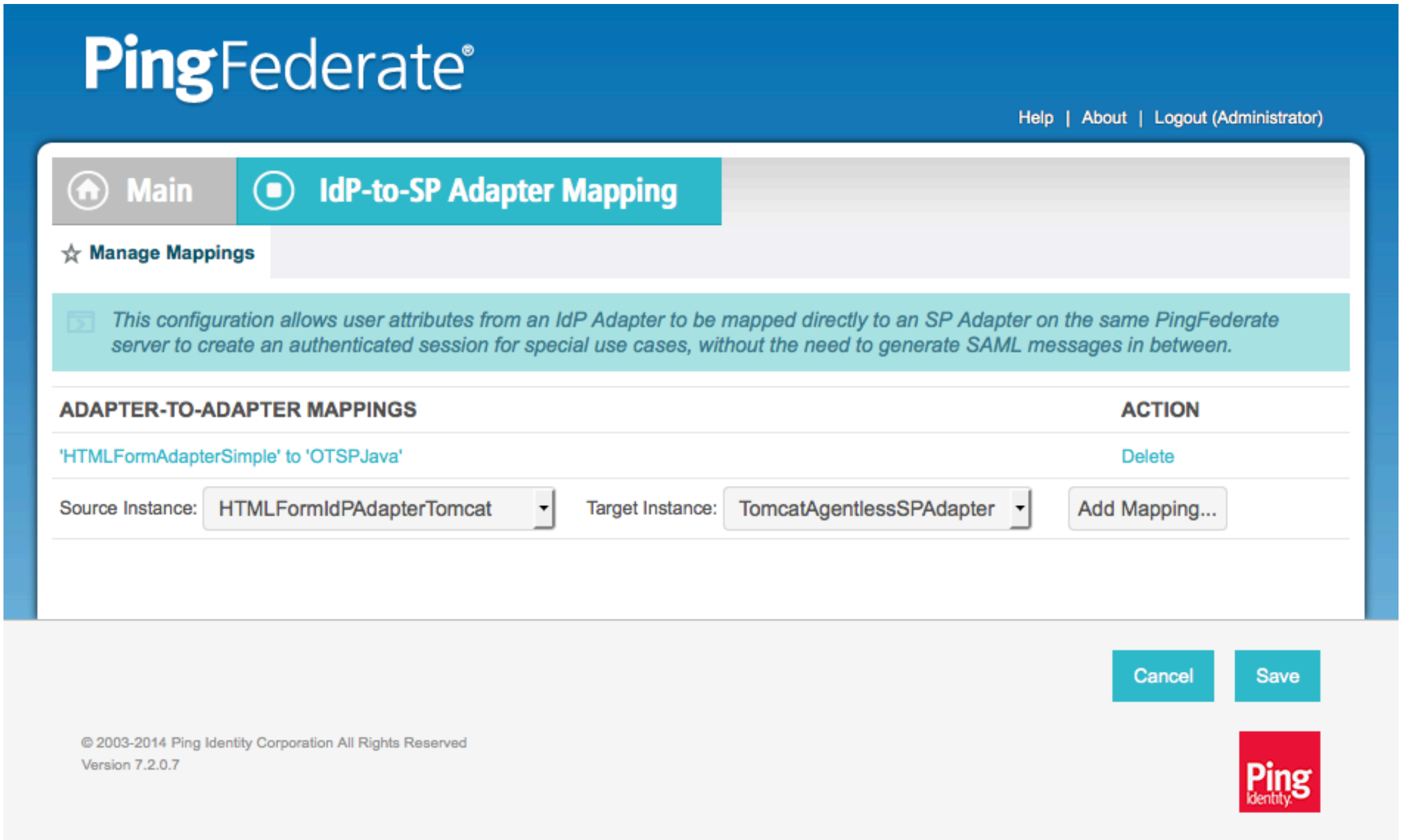
Attribute	Display Name
Attribute	Email
Attribute	subject

© 2003-2014 Ping Identity Corporation All Rights Reserved
Version 7.2.0.7

8. Click **Save**.

Configuring the Adapter-to-Adapter Mapping

1. Click **IdP-to-SP Adapter Mapping** under **System Settings** (in PingFederate 7.2 and below) or **Adapter-to-Adapter Mappings** under **IdP-To-SP Bridging** (in PingFederate 7.3 and above).
2. Select the IdP adapter that will be used for authentication as the **Source Instance**, and then the agentless SP adapter that was just configured as the **Target Instance**.



This configuration allows user attributes from an IdP Adapter to be mapped directly to an SP Adapter on the same PingFederate server to create an authenticated session for special use cases, without the need to generate SAML messages in between.

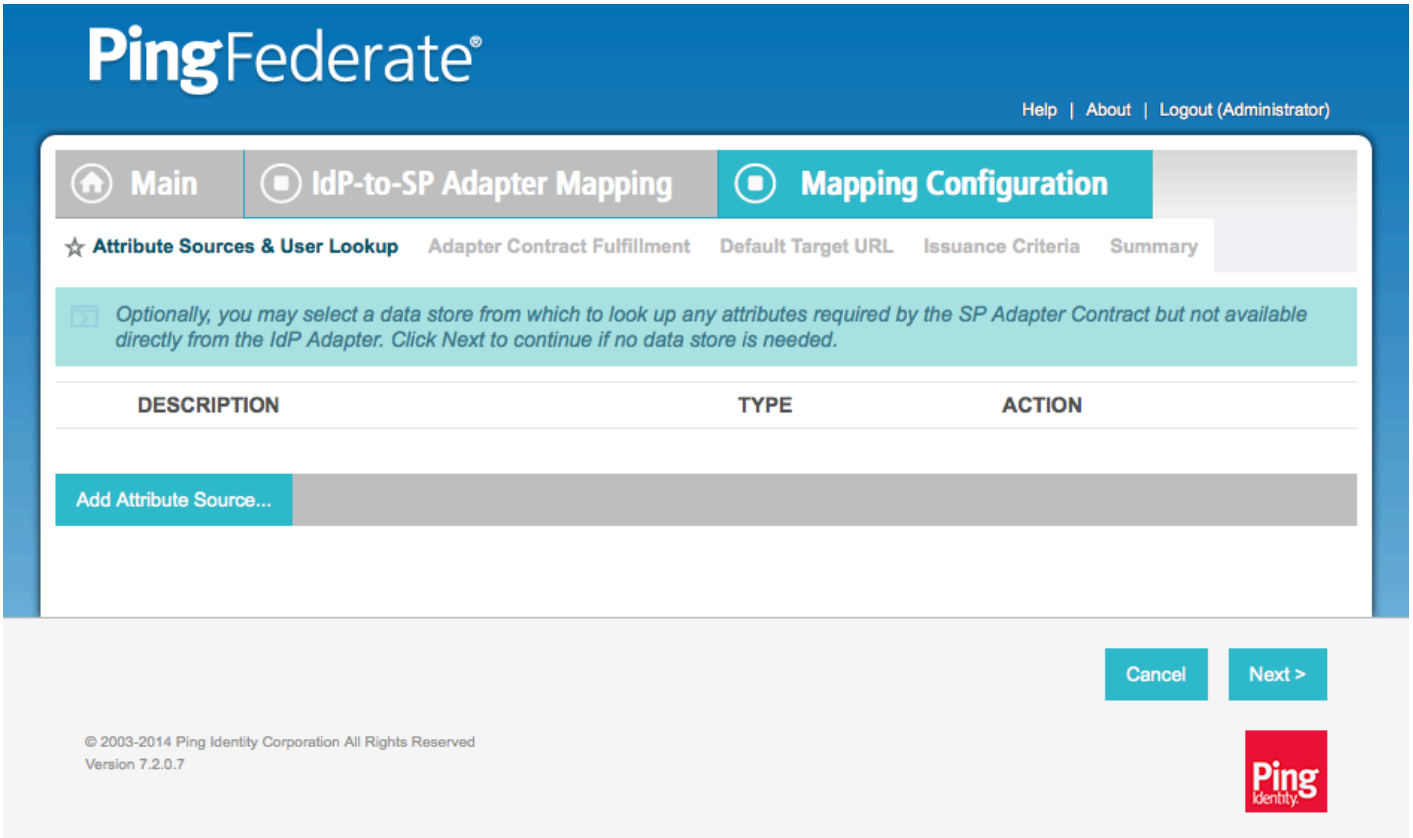
ADAPTER-TO-ADAPTER MAPPINGS	ACTION
'HTMLFormAdapterSimple' to 'OTSPJava'	Delete

Source Instance: HTMLFormIdPAdapterTomcat

Target Instance: TomcatAgentlessSPAdapter

© 2003-2014 Ping Identity Corporation All Rights Reserved
Version 7.2.0.7

3. Click the **Add Mapping…** button.
4. Click **Add Attribute Source…** if needed to lookup attributes from a datastore.

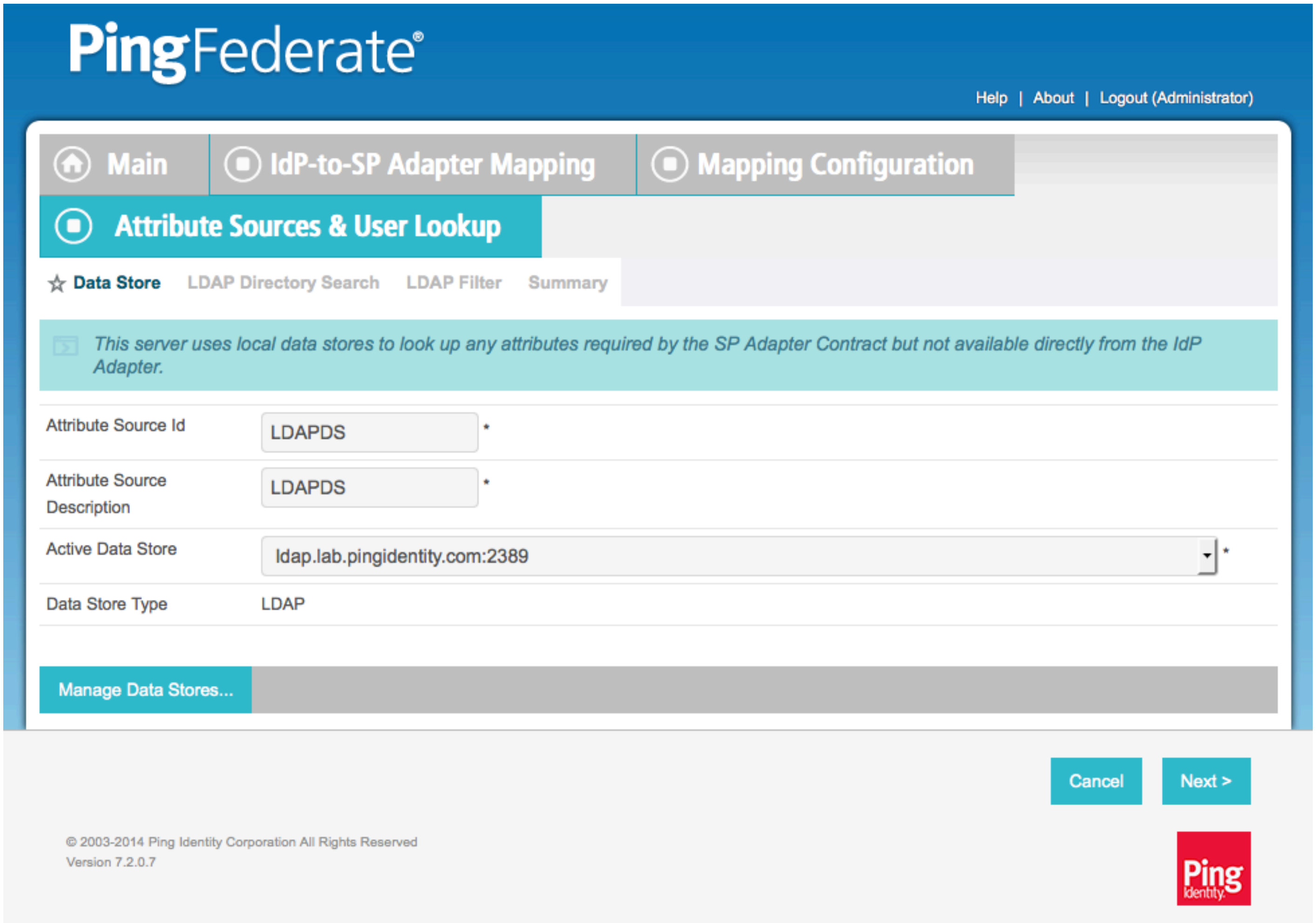


Optionally, you may select a data store from which to look up any attributes required by the SP Adapter Contract but not available directly from the IdP Adapter. Click Next to continue if no data store is needed.

DESCRIPTION	TYPE	ACTION

© 2003-2014 Ping Identity Corporation All Rights Reserved
Version 7.2.0.7

5. If adding an **Attribute Source**, proceed by entering the **Attribute Source Id**, **Attribute Source Description**, and selecting the Active **Data Store**. Then click **Next**.

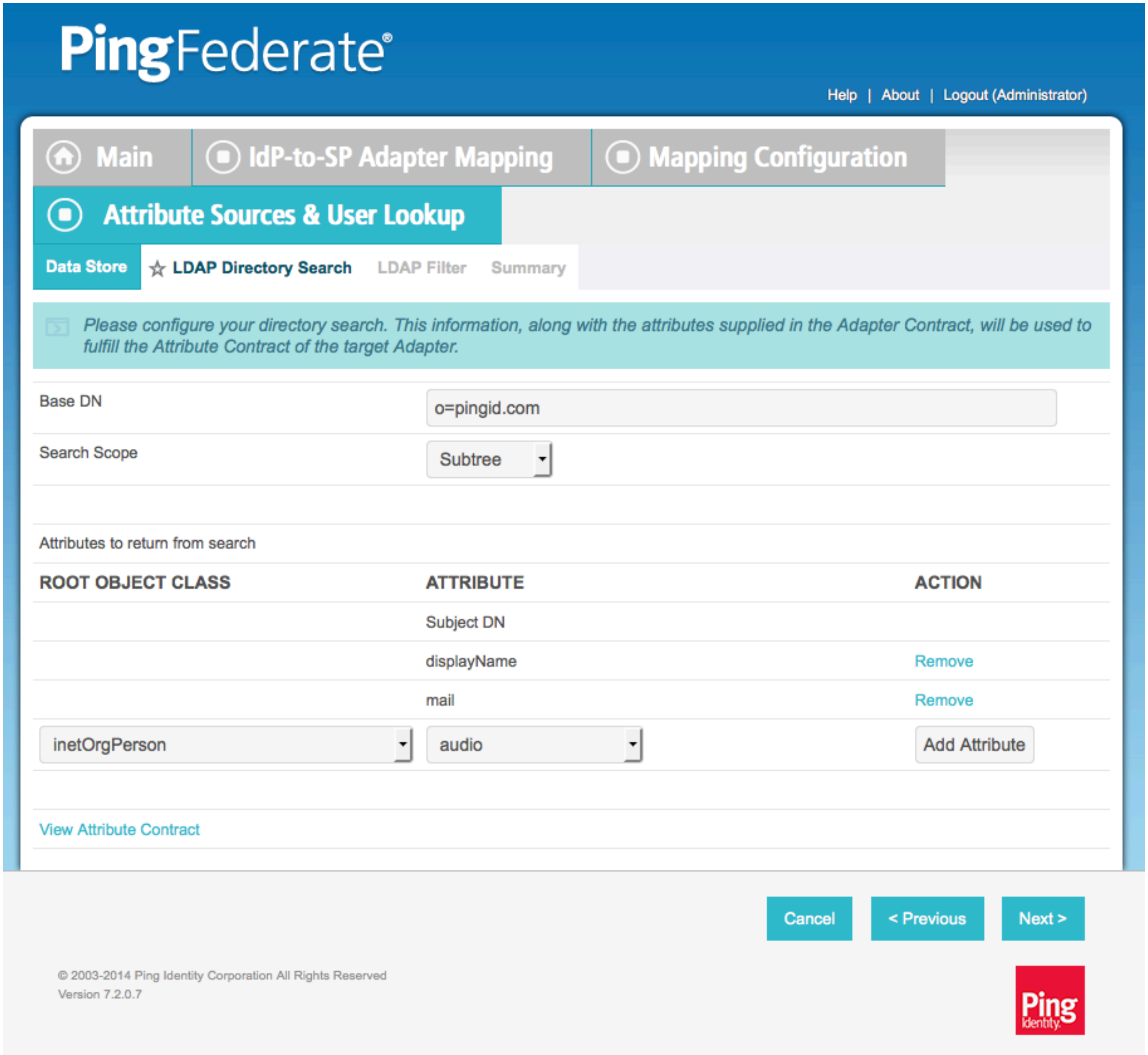


This server uses local data stores to look up any attributes required by the SP Adapter Contract but not available directly from the IdP Adapter.

Attribute Source Id	LDAPDS *
Attribute Source Description	LDAPDS *
Active Data Store	ldap.lab.pingidentity.com:2389 *
Data Store Type	LDAP

© 2003-2014 Ping Identity Corporation All Rights Reserved
Version 7.2.0.7

6. Enter the **Base DN**, add the necessary attributes, and click **Next**.


PingFederate®
Help | About | Logout (Administrator)
Main
IdP-to-SP Adapter Mapping
Mapping Configuration
Attribute Sources & User Lookup
Data Store
☆ LDAP Directory Search
LDAP Filter
Summary

Please configure your directory search. This information, along with the attributes supplied in the Adapter Contract, will be used to fulfill the Attribute Contract of the target Adapter.

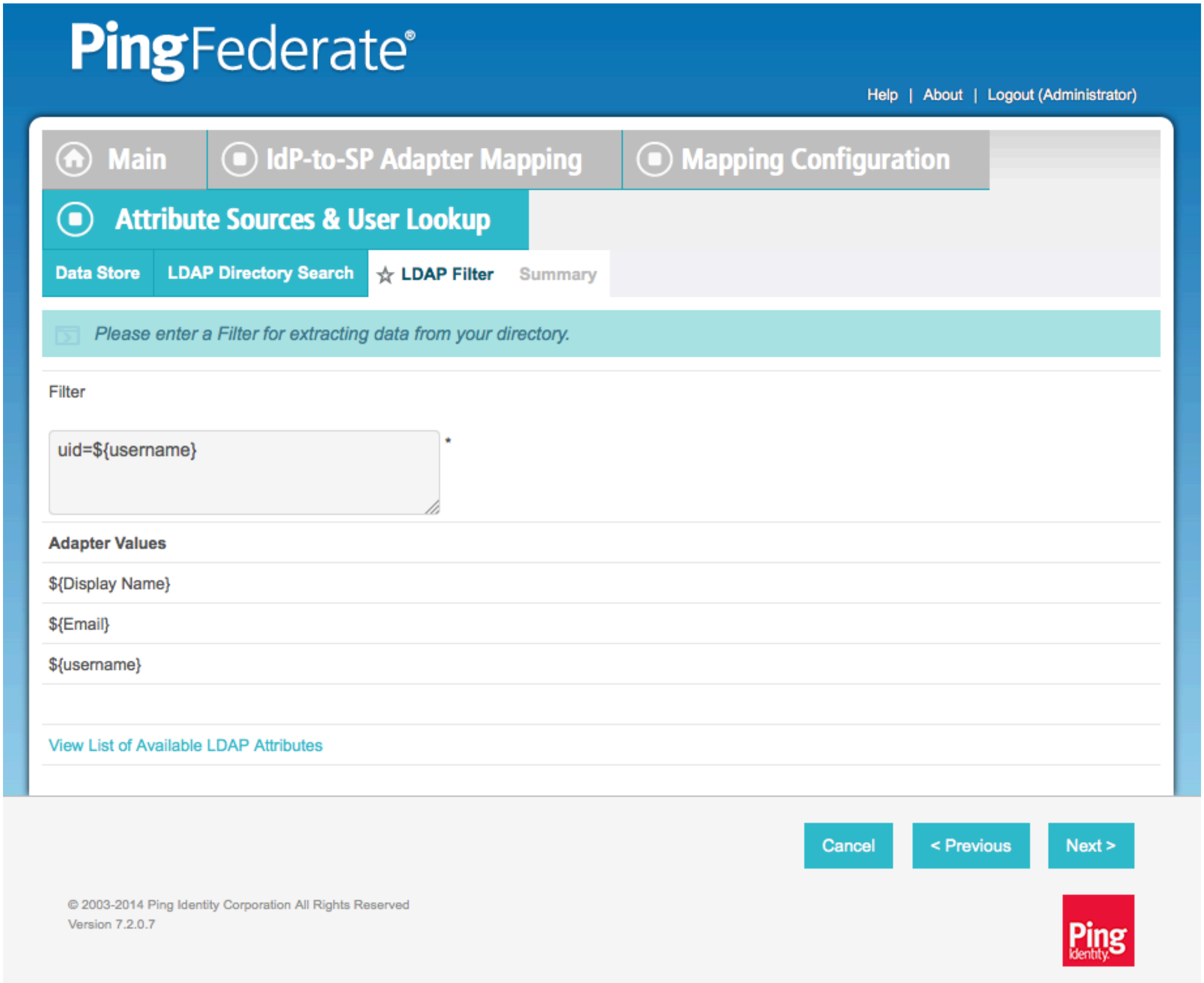
Base DN	o=pingid.com
Search Scope	Subtree

Attributes to return from search

ROOT OBJECT CLASS	ATTRIBUTE	ACTION
	Subject DN	
	displayName	Remove
	mail	Remove
inetOrgPerson	audio	Add Attribute

© 2003-2014 Ping Identity Corporation All Rights Reserved
Version 7.2.0.7

7. Enter the **Filter**, and click **Next**.



Please enter a Filter for extracting data from your directory.

Filter

uid=${username} *

Adapter Values

${Display Name}

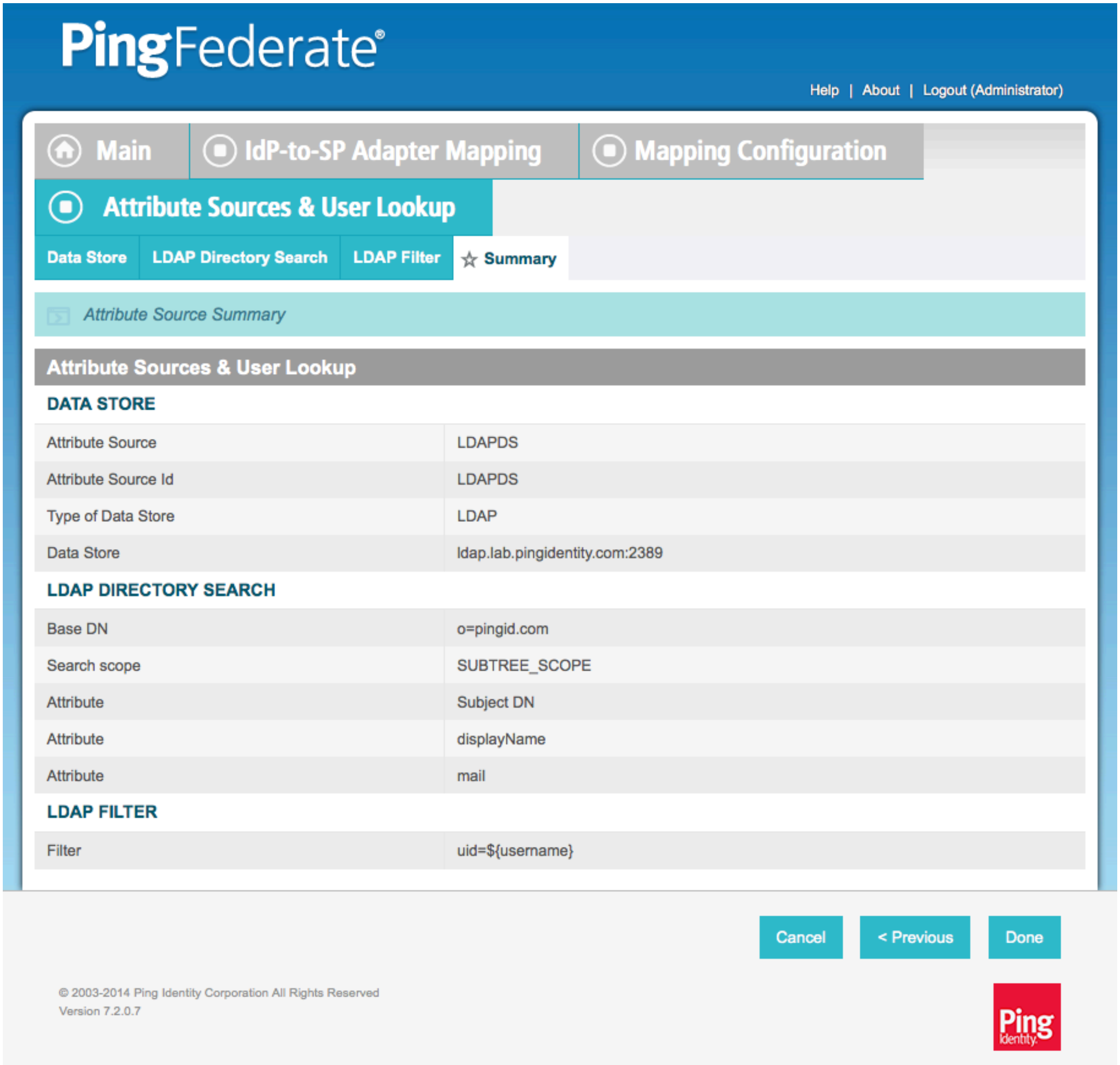
${Email}

${username}

View List of Available LDAP Attributes

© 2003-2014 Ping Identity Corporation All Rights Reserved
Version 7.2.0.7

8. Confirm the **Attribute Source Summary**, and click **Done**.


PingFederate
Help | About | Logout (Administrator)
Main
IdP-to-SP Adapter Mapping
Mapping Configuration
Attribute Sources & User Lookup
Data Store
LDAP Directory Search
LDAP Filter
☆ Summary

Attribute Source Summary

Attribute Sources & User Lookup

DATA STORE

Attribute Source	LDAPDS
Attribute Source Id	LDAPDS
Type of Data Store	LDAP
Data Store	ldap.lab.pingidentity.com:2389

LDAP DIRECTORY SEARCH

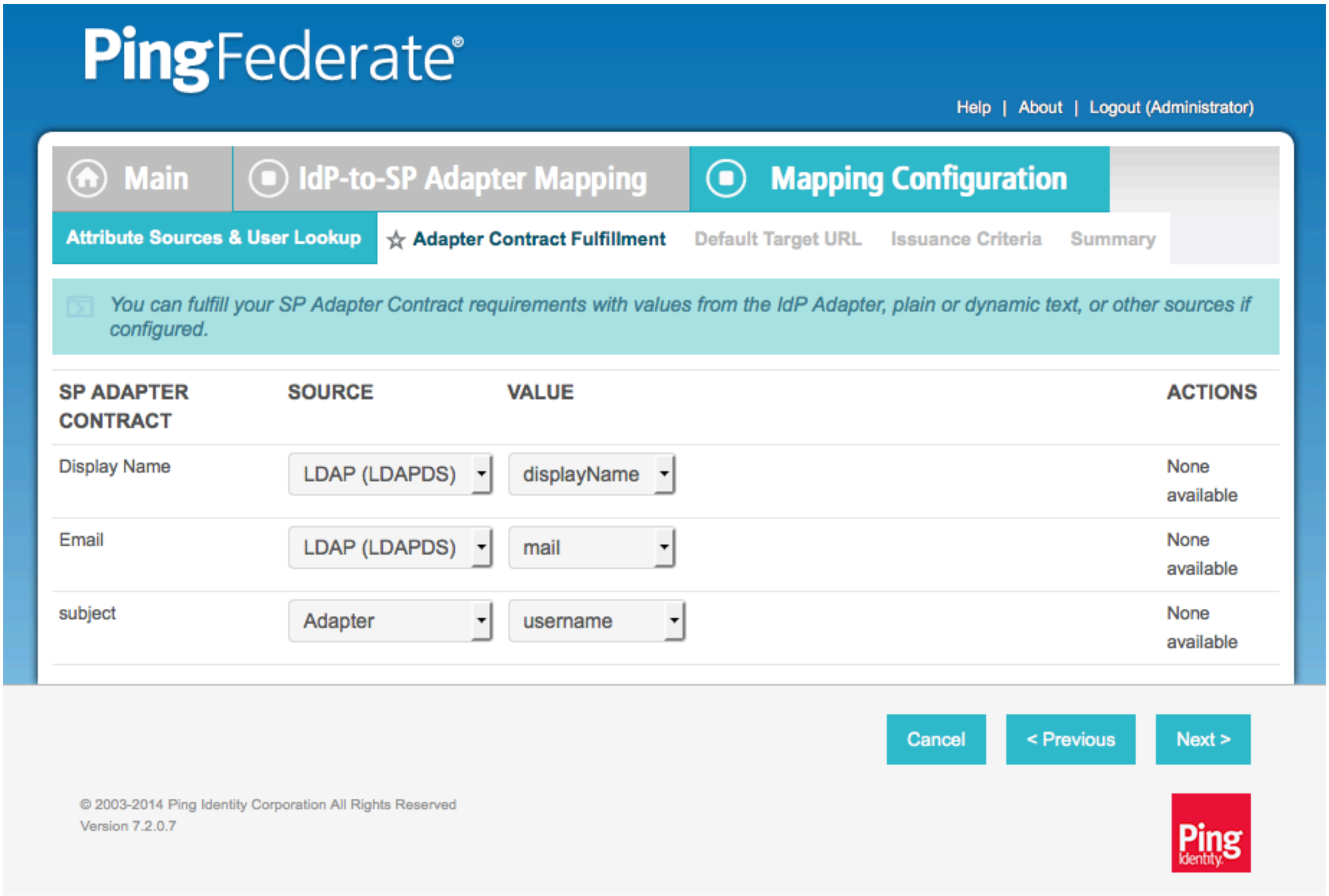
Base DN	o=pingid.com
Search scope	SUBTREE_SCOPE
Attribute	Subject DN
Attribute	displayName
Attribute	mail

LDAP FILTER

Filter	uid=${username}

Cancel
< Previous
Done
© 2003-2014 Ping Identity Corporation All Rights Reserved
Version 7.2.0.7
Ping Identity

9. Click **Next**.
10. Configure the **SP Adapter Contract**, and click **Next**.

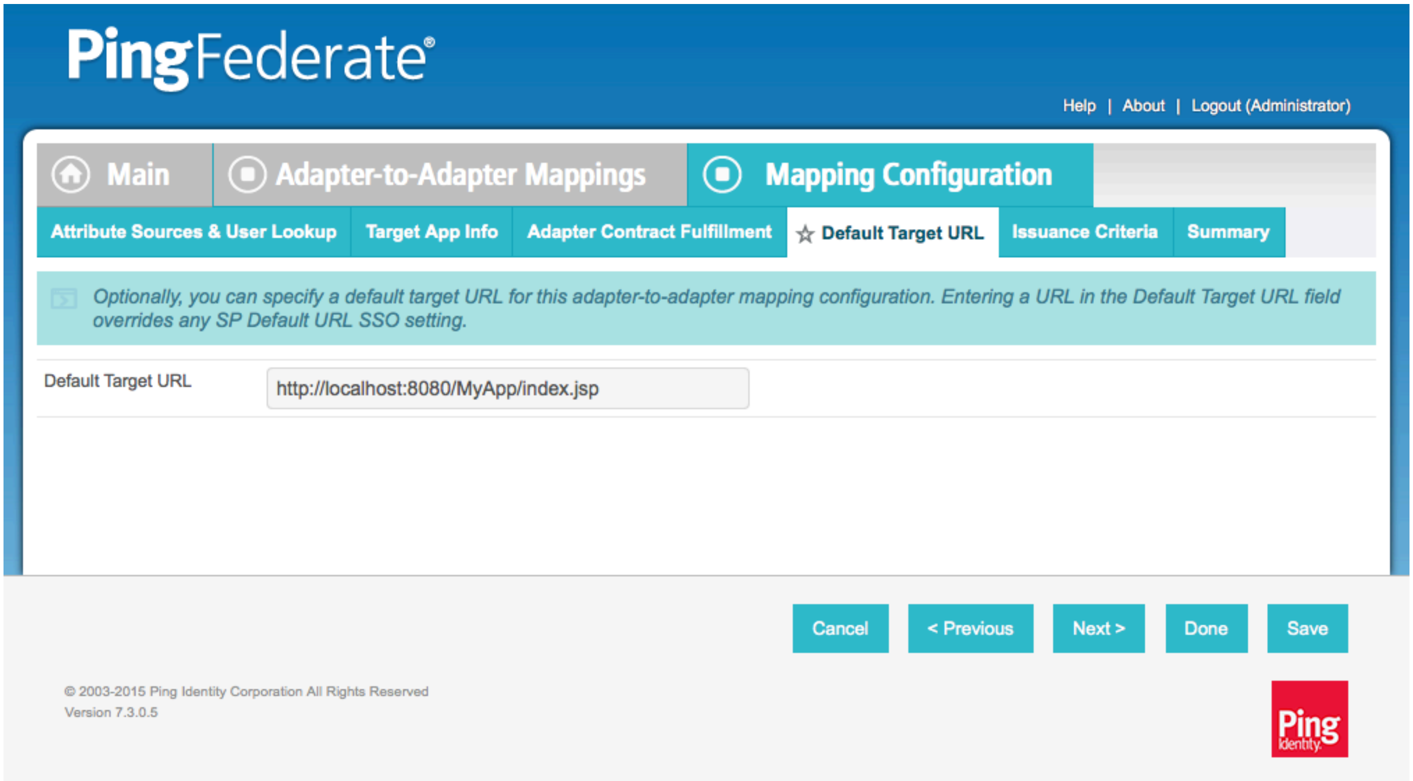


PingFederate®
Help | About | Logout (Administrator)
Main
IdP-to-SP Adapter Mapping
Mapping Configuration
Attribute Sources & User Lookup
☆ Adapter Contract Fulfillment
Default Target URL
Issuance Criteria
Summary

You can fulfill your SP Adapter Contract requirements with values from the IdP Adapter, plain or dynamic text, or other sources if configured.

SP ADAPTER CONTRACT	SOURCE	VALUE	ACTIONS
Display Name	LDAP (LDAPDS)	displayName	None available
Email	LDAP (LDAPDS)	mail	None available
subject	Adapter	username	None available

11. Enter the **Default Target URL** pertaining to your installation of where users should land if no referrer URL is present (i.e., https://<YourTomcatInstallUrl>/<YourApp>/index.jsp), and click **Next**.

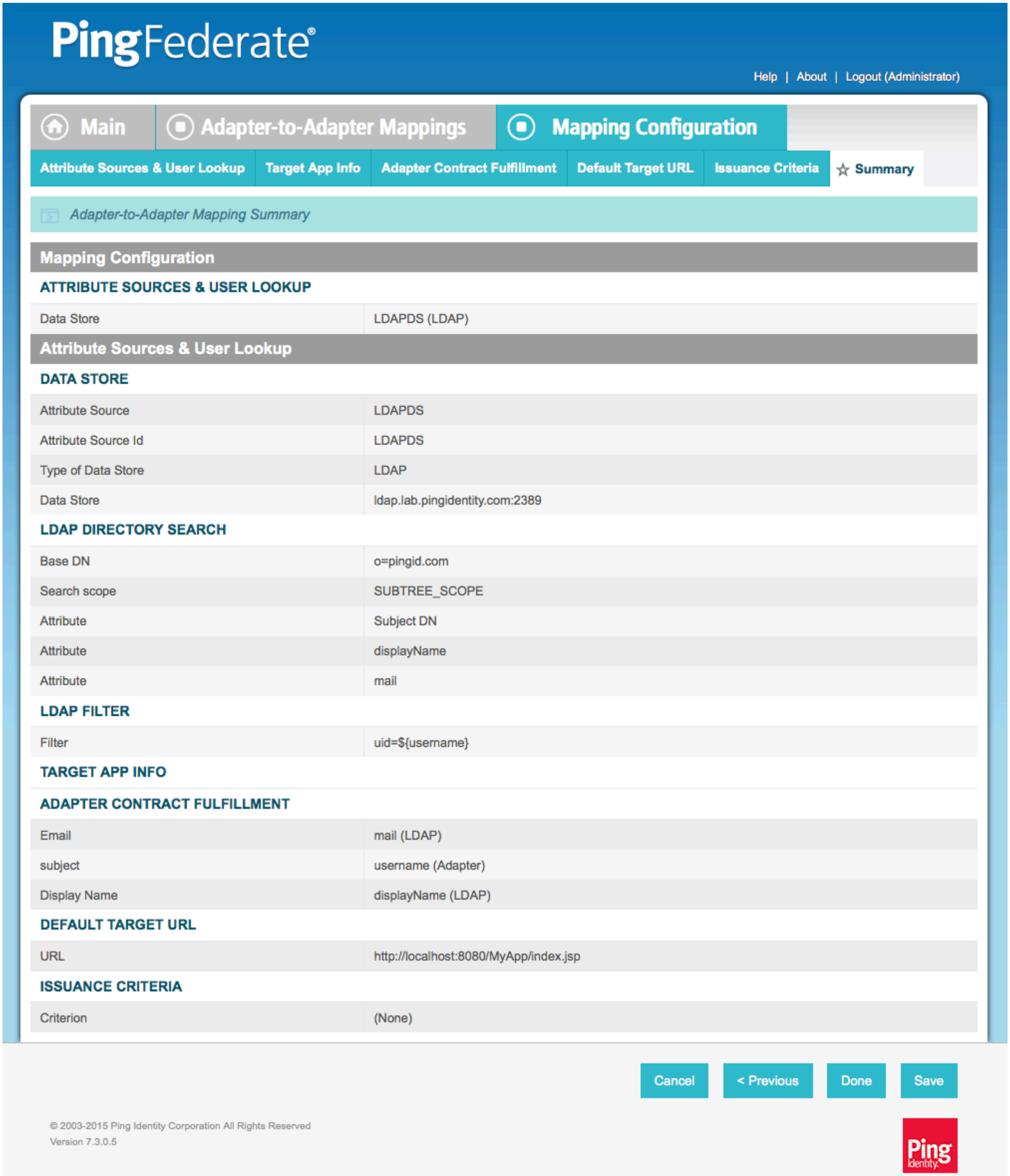

PingFederate®
Help | About | Logout (Administrator)
Main
Adapter-to-Adapter Mappings
Mapping Configuration
Attribute Sources & User Lookup
Target App Info
Adapter Contract Fulfillment
☆ Default Target URL
Issuance Criteria
Summary

Optionally, you can specify a default target URL for this adapter-to-adapter mapping configuration. Entering a URL in the Default Target URL field overrides any SP Default URL SSO setting.

Default Target URL: http://localhost:8080/MyApp/index.jsp

Cancel
< Previous
Next >
Done
Save
© 2003-2015 Ping Identity Corporation All Rights Reserved
Version 7.3.0.5
Ping Identity.

12. Click **Next**.
13. Confirm the **Adapter-to-Adapter Mapping Summary** and click **Done**.



Adapter-to-Adapter Mapping Summary

Mapping Configuration

ATTRIBUTE SOURCES & USER LOOKUP

Data Store	LDAPDS (LDAP)

Attribute Sources & User Lookup

DATA STORE

Attribute Source	LDAPDS
Attribute Source Id	LDAPDS
Type of Data Store	LDAP
Data Store	ldap.lab.pingidentity.com:2389

LDAP DIRECTORY SEARCH

Base DN	o=pingid.com
Search scope	SUBTREE_SCOPE
Attribute	Subject DN
Attribute	displayName
Attribute	mail

LDAP FILTER

Filter	uid=${username}

TARGET APP INFO

ADAPTER CONTRACT FULFILLMENT

Email	mail (LDAP)
subject	username (Adapter)
Display Name	displayName (LDAP)

DEFAULT TARGET URL

URL	http://localhost:8080/MyApp/index.jsp

ISSUANCE CRITERIA

Criterion	(None)

© 2003-2015 Ping Identity Corporation All Rights Reserved
Version 7.3.0.5

14. Click **Save**.

Modifying /pf/ JSP

1. Go to <YourTomcatInstall>/webapps/<YourApp>/pf/

2. Modify error.jsp
    a. Modify the following lines:

       Line 6: set the *loginUrl* to your equivalent PingFederate login URL - only modify the bolded:

       https://localhost:9031/pf/adapter2adapter.ping?IdpAdapterId=**HTMLFormIdPAdapterTomcat**&SpSessionAuthnAdapterId=**TomcatAgentlessSPAdapter**&TargetResource=**http://localhost:8080/MyApp**/pf/redirector.jsp

       Line 7: a valid email to send SSO issues to

    b. Save error.jsp.

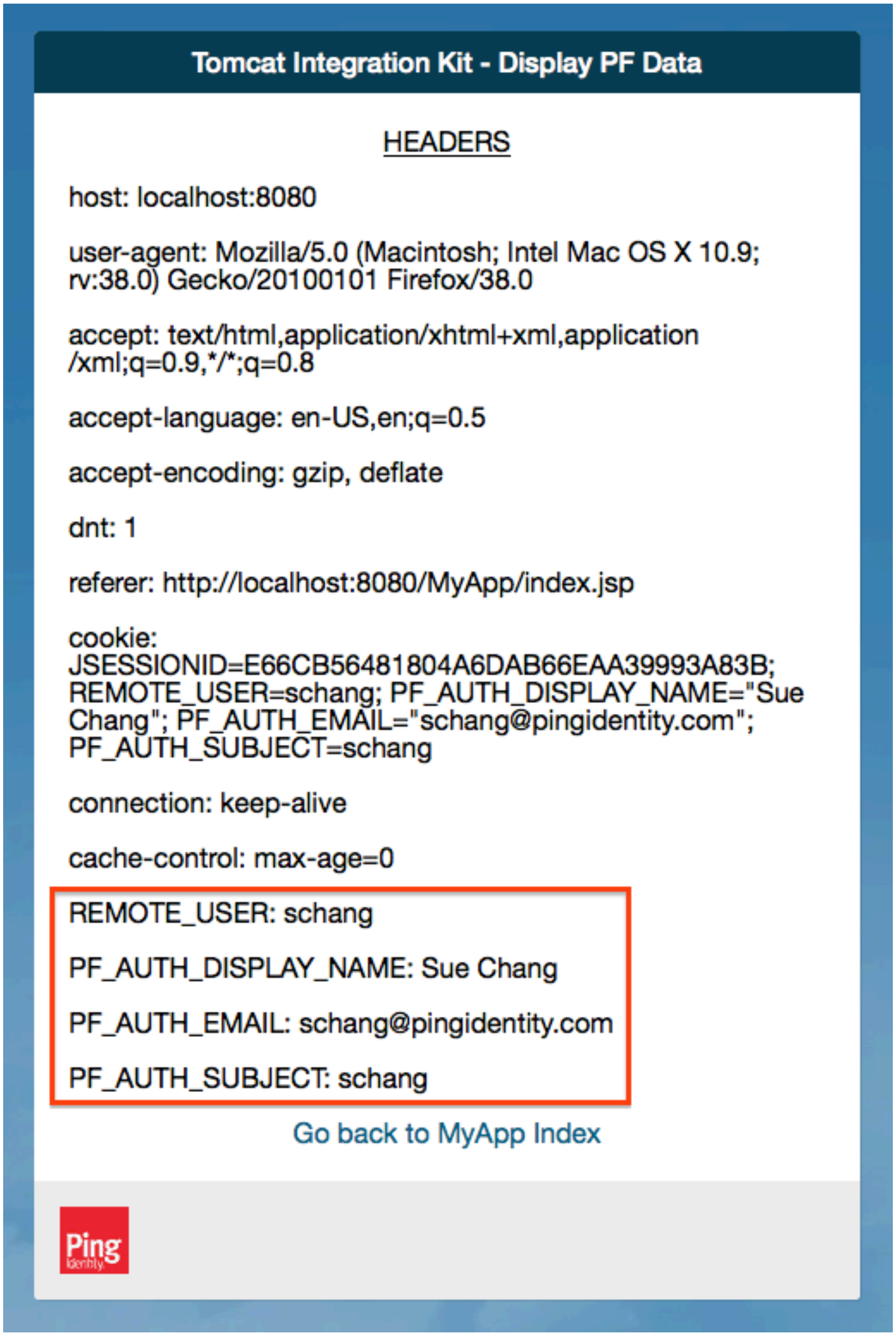
Testing

Please note: For all test cases below, please make sure to log out, clear the browser session, close and re-open the browser.

Testing with MyApp from the Kit

1. Direct Login Test
    a. Open a browser and go to the login link of the app to authenticate into (e.g., https://localhost:9031/pf/adapter2adapter.ping?IdpAdapterId=HTMLFormIdPAdapterTomcat&SpSessionAuthnAdapterId=TomcatAgentlessSPAdapter).
    b. Log in with correct credentials.

    Results: The user should be able to log in successfully, and be redirected to the default Target URL (the one configured in Step 11 under ***Configuration***). The expected headers should be passed from the PingFederate agentless adapter and displayed on *displaypfdata.jsp*.



Tomcat Integration Kit - Display PF Data

HEADERS

host: localhost:8080

user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:38.0) Gecko/20100101 Firefox/38.0

accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

accept-language: en-US,en;q=0.5

accept-encoding: gzip, deflate

dnt: 1

referer: http://localhost:8080/MyApp/index.jsp

cookie: JSESSIONID=E66CB56481804A6DAB66EAA39993A83B; REMOTE_USER=schang; PF_AUTH_DISPLAY_NAME="Sue Chang"; PF_AUTH_EMAIL="schang@pingidentity.com"; PF_AUTH_SUBJECT=schang

connection: keep-alive

cache-control: max-age=0

REMOTE_USER: schang

PF_AUTH_DISPLAY_NAME: Sue Chang

PF_AUTH_EMAIL: schang@pingidentity.com

PF_AUTH_SUBJECT: schang

Go back to MyApp Index

2. Resource Protected Page Test
   a. Open a browser and go to one of the **protected** pages in *MyApp* (e.g., http://localhost:8080/MyApp/admin/index.jsp or http://localhost:8080/MyApp/members/index.jsp).
   b. Log in with correct credentials when prompted.

   Results: The user should be able to log in successfully, and be redirected to the page he/she was going to. The expected headers should be passed from the PingFederate agentless adapter and displayed on *displaypfdata.jsp*.

Recommended Tests

1. Open a browser and go to the login link of the app to authenticate into. Log in with correct credentials.
   Results: If authorized, the user should be able to log in successfully. The expected headers should be passed from the PingFederate agentless adapter to the application on Tomcat.

2. Repeat the primary test case as defined above, but with bad credentials.
   Results: The user should fail authentication. No headers should be passed.

3. Open a browser and go to a resource protected link in the app. Log in with correct credentials.
   Results: If authorized, the user should be able to log in successfully, and redirected to the link that he/she was going to. The expected headers should be passed from the PingFederate agentless adapter to the application on Tomcat.

4. Repeat the third test case, but with bad credentials.
   Results: The user should fail authentication. No headers should be passed.

Logging

1. To enable/disable logging on the server side:

   Set the *pfEnableLogging* variable to true or false in the valve configuration (see step 5 under ***Installation***).

   Example:
   ```
   <Valve className="com.pingidentity.clientservices.product.tomcat.TomcatAdapter"
             …
             pfEnableLogging=”true” />
   ```

2. To enable/disable logging on the client side:

   Go to <YourTomcatInstall>/webapps/<YourApp>/pf/

   Modify login.jsp
   a. Open up login.jsp and go to line 5
   b. Set the *displayLogging* flag to true or false
   c. Save login.jsp

   Modify redirector.jsp
   a. Open up redirector.jsp and go to line 5
   b. Set the *displayLogging* flag to true or false
   c. Save redirector.jsp

   Modify error.jsp
   a. Open up error.jsp and go to line 5
   b. Set the *displayLogging* flag to true or false
   c. Save error.jsp

Logs will be written to <YourTomcatInstall>/logs/catalina.out.