PingFederate®

Version 7.x

Quick-Start Guide

Ping Identity®

PingFederate *Quick-Start Guide*
Version 7.x
September, 2013

Ping Identity Corporation
1001 17th Street, Suite 100
Denver, CO 80202
U.S.A.

Phone: 877.898.2905 (+1 303.468.2882 outside North America)
Fax: 303.468.2909
Web Site: www.pingidentity.com

Trademarks

Disclaimer

Document Lifetime

Ping Identity may occasionally update online documentation between releases of the related software. Consequently, if this PDF was not downloaded recently, it may not contain the most up-to-date information. Please refer to the online documentation at documentation.pingidentity.com for the most current information.

From the Web site, you may also download and refresh this PDF if it has been updated, as indicated by a change in this date: **September 25, 2013**.

Quick-Start release notes

The PingFederate™ Quick-Start distribution contains demo applications that can be used with PingFederate to handle common single sign-on (SSO) and other scenarios built into the applications. We recommend that new users install the applications as a means of becoming familiar with PingFederate and testing secure Internet SSO, as well as other optional identity-federation use cases.

Change list

Quick-Start Applications 1.1, July 2011

Changed applications and configuration to use the ReferenceID Adapter, distributed with the PingFederate Agentless Integration Kit.

Quick-Start Applications 1.0, August 2010

Initial release separate from the PingFederate distribution. Prior to PingFederate 6.3, the Quick-Start Applications were bundled with PingFederate.

Known issues

Auto-Connect™™ functionality requires that partner SSL server certificates be signed by a trusted Certificate Authority (CA). The SSL server certificate packaged with the Quick-Start is self-signed, so the certificate is also included as a trusted CA in the configuration archive (`data.zip`) contained in the distribution. The configuration archive may be "hot-deployed"; that is, without restarting PingFederate. However, changes to the PingFederate trusted CA store, as they relate to Auto-Connect, do not take effect until the PingFederate server is restarted. Therefore, if you intend to try out Auto-Connect, be sure to follow the installation instructions, restarting the server after deploying the configuration archive.

Important: This certificate used for Quick-Start is for testing and demonstration only. In a production environment, you should remove any self-signed certificates from the trusted CA store.

Contents

Preface **1**
About This Manual 1
Intended Audience 1
Summary 1
Text Conventions 2
Other Documentation 2
Chapter 1 Introduction **5**
Overview 5
Chapter 2 Getting Started **7**
Quick-Start Components 7
Deploying the Quick-Start 8
Chapter 3 Using the Quick-Start Applications **9**
Starting at the IdP 10
Accessing the IdP Application 10
Using the IdP Web Portal 11
Using Advanced SSO Options 12
Starting at the SP 13
Accessing the SP Application 13
Authenticating to the Application 13
Starting Single Sign-On 13
Using Auto-Connect 16
Logging In Locally 16
Using the SP Target Resource Page 17
Chapter 4 Modifying the Configuration **19**
Using the Administrative Console 19
Accessing the Console 20
Navigating Server Settings 20
Viewing the Quick-Start Configuration 20

Changing the Console Configuration 22
Configuring the IdP to Use Pseudonyms 22
Configuring the SP to Use Account Linking 24
Configuring XML Encryption 26
Configuring Other Deployments 27
Using Separate Servers 27
Using Other Web Containers 29
Modifying Configuration Files 29
Extending Use Cases 30

Preface

About This Manual

The PingFederate *Quick-Start Guide* provides procedures for rapidly deploying the PingFederate server, preconfigured to establish a simple Internet single sign-on (SSO) connection between two Web sites. You can use this *Guide* either for product evaluation or to familiarize yourself with PingFederate for future in-depth implementations.

Intended Audience

This *Guide* is intended for security and network administrators and other IT professionals responsible for identity management among both internal and external business entities. If you are not familiar with identity federation, it might be helpful to browse through the first chapters of the *Getting Started* and the <WikiLinkItal>Administrator's Manual in the PingFederate distribution.

Note: The *Guide*, the quick-start applications, and supporting components are provided for demonstration purposes only and are not intended for production use or as models for production deployment.

Summary

The *Guide* consists of the following chapters:

- Chapter 1, "Introduction"— An overview of the purpose and deployment of the quick-start applications.
- Chapter 2, "Getting Started"— How to install and deploy the quick-start components.

- Chapter 3, "Using the Quick-Start Applications"— How to access and use the quick-start application options.
- Chapter 4, "Modifying the Configuration"— How to view the PingFederate configuration used in conjunction with the applications, plus guidance on modifying selected settings.

Text Conventions

This document uses the text conventions identified below.

Table 1: Text Conventions

Convention	Description
`Fixed Width`	Indicates text that must be typed exactly as shown in the instructions. Also used to represent program code, file names, and directory paths.
Blue text	Indicates hypertext links.
Italic	Used for emphasis and document titles.
▶ [text]	Used for procedures where only one step is required.
Sans serif	Identifies descriptive text on a user-interface screen. Example: "Print Document dialog"
Sans serif bold	Identifies menu items, navigational links, or buttons. For example: Click **Save**.

Other Documentation

The documents listed below are available under Product Documentation at pingidentity.com.

Tip: PingFederate provides context-sensitive Help. Click **Help** in the upper-right portion of the administrative console for immediate, relevant guidance and links to related information.

Getting Started – Provides an introduction to secure Internet SSO and PingFederate, including background information about federated identity management and standards, product installation instructions, and a primer on using the PingFederate administrative console.

Administrator's Manual – Provides key concepts as well as detailed instructions for using the PingFederate administrative console—also connection-endpoint and other Web-application developer information, a glossary, and a list of common acronyms.

Integration Overview – A high-level description of options available for integrating identity-management systems and applications with PingFederate.

Server Clustering Guide – Describes how to deploy PingFederate in a cluster to increase throughput and availability.

SDK *Developer's Guide* – Provides technical guidance for using the Java Software Developer Kit for PingFederate.

Web Resources – Ping Identity continually updates its Resource Center (www.pingidentity.com/resource-center) with general and technical information in the form of white papers, demonstrations, webinars, and other resources.

Note: If you encounter any difficulties with configuration or deployment, please look for help at the Ping Identity Support Center (www.pingidentity.com/support).

PingFederate documents may include hypertext links to third-party Web sites that provide installation instructions, file downloads, and reference documentation. These links were tested prior to publication, but they may not remain current throughout the life of these documents. Please contact Ping Identity Support (www.pingidentity.com/support) if you encounter a problem.

Chapter 1

Introduction

PingFederate is a best-of-breed Internet-identity security platform that implements multiple standards-based protocols to provide cross-domain single sign-on (SSO) and user-attribute exchange, as well as support for identity-enabled Web Services and cross-domain user provisioning.

This *Guide* provides instructions specifically for configuring PingFederate quickly to run with accompanying Web applications, which demonstrate Internet SSO (also called browser-based SSO) and attribute transmittal, as well as single logout (SLO).

Overview

This *Guide* provides instructions for deploying a PingFederate server to act as both an Identity Provider (IdP) and a Service Provider (SP) in support of the scenario implemented by the quick-start applications:

- Users authenticate to the IdP Quick-Start Application using their username and password. Once authenticated, users gain access to the application's portal page, from which they can initiate SSO and SLO requests.
- The SP Quick-Start Application contains a protected Web page. To access that resource, users must authenticate to the SP Quick-Start Application. There are two ways to authenticate: logging on directly to the SP Quick-Start Application or requesting SSO through the IdP.

You can initiate the SSO process from either the IdP or SP application. The same is true for SLO, which logs the user out of both applications via secure messages across the domains.

The IdP and SP servers each use an "agentless" adapter (called the ReferenceId Adapter) to interact with the authentication system built into the quick-start applications. For information about adapters and their role in PingFederate, refer to "SSO Integration Kits and Adapters" in the Key Concepts chapter of the

PingFederate *Administrator's Manual*. For specific information about the ReferenceID Adapter, refer to the *User Guide* for the PingFederate Agentless Integration Kit (you can download the kit at `www.pingidentity.com/support-and-downloads`).

There are numerous use cases and configuration options for supporting SSO with business partners or applications outside of an enterprise security domain (see "Extending Use Cases" on page 30). The preconfigured quick-start scenario adheres to version 2.0 of the Security Assertion Markup Language (SAML). For a complete discussion of industry standards, see the "Supported Standards" chapter in *Getting Started*.

Chapter 2

Getting Started

This section describes how to deploy the quick-start components. After you install PingFederate, you can configure the server and deploy the applications in a few minutes.

Quick-Start Components

The PingFederate quick-start distribution file contains:

- Two extracted `WAR` directories containing the IdP and SP Web applications written in Java
- A `data.zip` file containing the PingFederate server-configuration archive allowing SSO and SLO between the quick-start applications
- A `JAR` file containing IdP and SP adapters used to integrate PingFederate with the applications
- A second `JAR` used to support the adapters

Important: Deploying the `data.zip` file overwrites any settings you may have configured using the PingFederate administrative console. A backup archive is created automatically in the same directory used to deploy `data.zip` (see the next section), or you can create an archive manually. For more information, see "Using the Configuration Archive Utility" in the System Administration chapter of the PingFederate *Administrator's Manual*.

Deploying the Quick-Start

To deploy the quick-start:

1. If you have not already done so, install the PingFederate server according to the "Installation" instructions in *Getting Started*.
2. From the quick-start distribution directory, copy the files:
   - `quickstart-app-idp.war`
   - `quickstart-app-sp.war`
   - `json-simple-1.1.jar`
   - `pf-referenceid-adapter-1.0.jar`

   into this directory in your PingFederate installation:

   `<pf_install_dir>/pingfederate/server/default/deploy`
3. From the quick-start distribution directory, copy the `data.zip` file into:

   `<pf_install_dir>/pingfederate/server/default/data/drop-in-deployer`
4. Stop and restart the PingFederate server, if it is running.

   If you are new to PingFederate, see the section "Starting and Stopping PingFederate" in the System Administration chapter of the PingFederate *Administrator's Manual*.

Chapter 3

Using the Quick-Start Applications

The quick-start applications demonstrate SSO and SLO processing to and from your IdP- and SP-configured PingFederate server. You can initiate the SSO process from either the IdP or SP applications.

Tip: SSO and SLO transactions happen quickly, and the processing is usually transparent from the user's perspective—two of the benefits of identity federation. If you want to see behind the scenes, keep the PingFederate startup window visible as you use the applications. You can also find logs in the `<pf_install_dir>/pingfederate/log` directory.

IdP-initiated SSO is a scenario in which users of a local IdP gain access to protected, cross-domain Web resources without re-authentication. In this scenario users might access a company portal, for example, that provides links to SP-partner resources such as a Web-based office-supply site or an Internet-service application.

When you log on locally to the IdP Quick-Start Application, no communication occurs between the application and PingFederate—the user authenticates using the local user store. The local Web application contacts PingFederate to initiate SSO only after the user attempts to access a Web resource protected by another security context. This security context may be managed by another department within the organization or be part of a business-partner organization.

In the case of SP-initiated SSO, a user accesses a local Web resource for which authentication is handled by a remote (out-of-domain) IdP site. The user is ultimately redirected to PingFederate at the IdP site, where he or she logs on. Once the authentication is complete, processing occurs as if the user had requested SSO from the IdP site. A real-life example of this scenario might be a user accessing the Web site of a national logistics company from a home computer and being redirected to his or her company's Web site for authentication.

SLO occurs only after a user has completed an SSO transaction. As with SSO, SLO can be initiated from either the IdP or SP application once an SSO user session has been established. SLO closes the user's sessions at each remote partner from which the user accessed a protected Web resource.

Starting at the IdP

The IdP Quick-Start Application demonstrates basic SSO and SLO from an IdP perspective. Included in the application are some advanced SSO features supported by the PingFederate server. You can also start with the SP application (see "Starting at the SP" on page 13).

Accessing the IdP Application

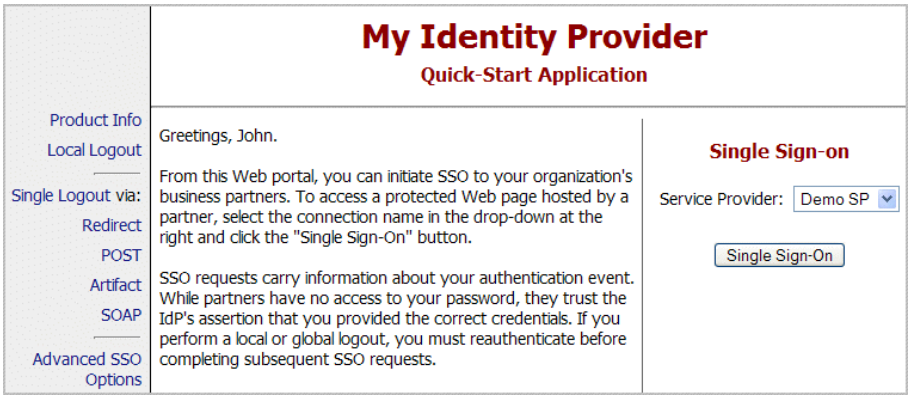
1. Ensure that you have deployed the quick-start components and started the PingFederate server (see "Deploying the Quick-Start" on page 8).
2. Open a Web browser to this location:

   `https://localhost:9031/quickstart-app-idp/go`
3. If your browser prompts you to accept the certificate or continue to the application, please do so.
4. On the Quick-Start IdP Application - Login page, choose any User Id from the drop-down list under User Login, enter `test` in the Password field, and click **Sign On**.

Tip: The default password for all users in the IdP and SP quick-start applications is `test`. You can add users and add or change user attributes (see "Modifying Configuration Files" on page 29).

Using the IdP Web Portal

After you sign on to the IdP quick-start Web Portal page, you can initiate SSO to the SP application.



Several of the options on this page are self-explanatory, and the page itself provides additional information. Some elaboration is provided below, as well as information about advanced options:

- Click **Single Sign-On** to begin SSO to the SP Quick-Start Application.

  Note: The Service Provider drop-down list is provided to accommodate additional (optional) SP connections you may create in the administrative console (see "Using the Administrative Console" on page 19).

  The SP application uses a simple password-protection mechanism. The SSO process fulfills the application's security requirements by presenting the PingFederate SP server with a SAML assertion. A session for the user is created at the SP Web site, and the browser is directed to the SP Target Resource page (see "Using the SP Target Resource Page" on page 17).

- The **Single Logout** choices exercise different SLO transport mechanisms, or *bindings*, configured for the SP connection in the PingFederate administrative console.

  See "Viewing the Quick-Start Configuration" on page 20 for information about where to look for these configuration settings. For detailed information about transport profiles and bindings, see the "Supported Standards" chapter in *Getting Started*.

  Note: Unless you complete an SSO to the SP site, these links are configured to perform local logout only, since SLO is not possible without at least one active SSO session. After you SSO to the SP, you can return to this page and use the links to perform an actual SLO; check the varying transport messages in the server-startup window or in log files.

Using Advanced SSO Options

Clicking **Advanced SSO Options** allows you to modify the default SSO process and try out different features. The table below describes these options.

Tip: For more information about these and other options, see "Application Endpoints" in the PingFederate *Administrator's Manual*.

Table 2: Options for IdP-Initiated SSO

Option	Description
Binding	You can choose which binding (message transport mechanism) you want to use for SSO (POST and Artifact are configured).
ACSIdx	SP partners may support more than one SAML 2.0 endpoint for processing assertions ("Assertion Consumer Service"). An ACS is configured with an index number, which may be specified in the SAML assertion. The connection to the SP Quick-Start Application is configured with two services, one using the POST binding and one using the Artifact binding, with index numbers of 0 and 1, respectively. (Index numbers take precedence over the Binding parameter if both are specified. The configured default is 0.)
Name ID Format	The choices are: • transient – The user's identifier is a secure, randomly generated value for one-time use (see "Account Linking" in the Key Concepts chapter of the PingFederate *Administrator's Manual*). • persistent – The identifier is a pseudonym, which may be used by the SP to create an account link. (This choice will result in an error unless you reconfigure the SP-connection in PingFederate—see "Configuring the IdP to Use Pseudonyms" on page 22). • encrypted – The identifier is encrypted. (This choice will result in an error unless you reconfigure the SP-connection in PingFederate—see "Configuring XML Encryption" on page 26).
Target URL	Specifies the desired protected Web resource at the SP partner. While the quick-start scenario contains only a single such target, this option may be useful in another context. For example, you may want to use the IdP Quick-Start Application to test connectivity with a different SP partner.

Starting at the SP

An SP Web page provided by the SP Quick-Start Application provides access to SP-initiated SSO.

Accessing the SP Application

To access the SP application:

1. Ensure that you have deployed the quick-start components and started the PingFederate server (see "Deploying the Quick-Start" on page 8).
2. Open a Web browser to this location:

   `https://localhost:9031/quickstart-app-sp/go`

Authenticating to the Application

To access a protected resource at the SP site, you have three choices. You can authenticate with the IdP using either conventional SSO or Auto-Connect™, or you can log on locally at the SP.

Like its IdP counterpart, the SP Welcome page also provides some advanced SSO options.

Starting Single Sign-On

1. On the SP Welcome page, click **Single Sign-On**.

   Note: The IdP Partner drop-down list is provided in case you want to create new IdP connections in the administrative console (see "Using the Administrative Console" on page 19).

   If you have an existing user session at the IdP from a previous authentication, the **Single Sign-On** button takes you directly to the SP Target Resource page. If not, the IdP server uses its adapter to authenticate you using the user store local to the IdP.
2. On the IdP Login page, select a User Id and enter the password `test`.

Once your user session is established at the IdP, the IdP server communicates that information to the SP server using a SAML assertion. Then, the SP server

completes the SSO allowing you to access the protected resource (see "Using the SP Target Resource Page" on page 17).

Note: The default password for all users at the IdP and SP quick-start sites is `test`.

Advanced SSO Options

Clicking **Advanced SSO Options** allows you to modify the default SSO process and try out different features and capabilities of PingFederate (see "Viewing the Quick-Start Configuration" on page 20). The table below describes these options.

Tip: For more information about these and other options, see "Application Endpoints" in the PingFederate *Administrator's Manual*.

Table 3: Options for SP-Initiated SSO

Option	Description
Binding	Choose which configured binding (message transport mechanism) you want to use for the authentication request.
Requested Binding	Choose which configured binding you want your IdP partner to use for the SAML assertion response.
Requested ACS Index	Choose the configured index number of the local Assertion Consumer Service endpoint to which you want the IdP to send the assertion (see "Setting Assertion Consumer Service URLs (SAML)" in the Identity Provider SSO Configuration chapter of the PingFederate *Administrator's Manual*).

Table 3: Options for SP-Initiated SSO

Option	Description
Requested Name ID Format	The choices are: • none - No requested NameID format is sent with the authentication request. • transient – The user's identifier is a secure randomly generated value for one-time use (see "Account Linking" in the Key Concepts chapter of the PingFederate *Administrator's Manual*). • persistent – The identifier is a pseudonym, which may be used as an account link by the SP. (This choice results in an error unless you reconfigure the SP-connection—see "Configuring the IdP to Use Pseudonyms" on page 22.) • encrypted – The identifier is encrypted. (This choice results in an error unless you reconfigure the SP-connection—see "Configuring XML Encryption" on page 26.) • unspecified - The requested NameID format (*unspecified*) is sent with the authentication request.
Is Passive	When selected, the IdP is requested not to visibly take control of the user's browser. (Thus, if the user is not already logged on at the IdP, SSO will fail.)
Force Authn	When selected, IdP authentication is required regardless of whether the user is currently logged on to the IdP site.
AllowCreate	If checked, the value of the `AllowCreate` attribute of the `NameIDPolicy` element in the `AuthnRequest` is set to `true` (see the OASIS SAML document: saml-core-2.0-os.pdf).
Requested SPNameQualifier	Specifies that the IdP should return an assertion whose subject name is qualified in the given namespace.
Requested Authentication Context(s)	Requests that the IdP use one of the methods specified for authentication and indicate in the assertion what method was used. The allowed values for this field are URIs designated in the SAML specifications (see the OASIS SAML document: saml-authn-context-2.0-os.pdf).
Authentication Context Comparison Method	Specifies the comparison method used to evaluate the requested context (see the OASIS SAML document: saml-core-2.0-os.pdf under "Element <RequestedAuthnContext>").

Using Auto-Connect

PingFederate's Auto-Connect enables SSO for multiple partners by using a common configuration, applicable to all partners, and metadata exchange. The metadata identifies the partner and connection "just in time" for the runtime engine to complete the SSO transaction. (For more information, see the "Using Auto-Connect" in the Key Concepts chapter of the PingFederate *Administrator's Manual*.)

1. On the SP Welcome page, click **Auto-Connect** in the menu bar.
2. Enter an email address, using `localhost` as the domain name.

   For example:

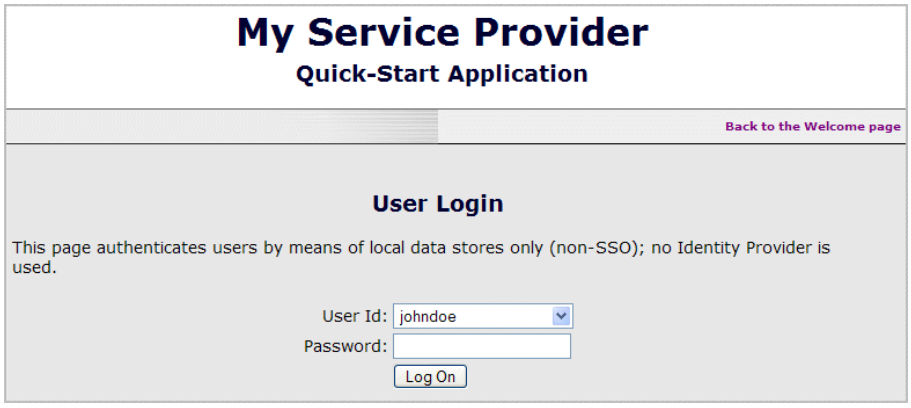
   `john@localhost`

   The domain name is used to identify the IdP partner and retrieve connection metadata. For this demonstration, both the IdP and SP are using the same PingFederate server located at `https://localhost:9031`.
3. Click **Single Sign-on**.

   At this point, the behavior of the applications is the same as that for regular SSO: you are logged on to the SP (see "Using the SP Target Resource Page" on page 17). However, you can see in the server-console window or the server log in the `pingfederate/log` directory that metadata, exchanged at the initial contact, was used to make the connection, rather than manually configured endpoints.

Logging In Locally

The **Local Login** link in the top navigation bar of the SP Quick-Start Application's Welcome page provides access to the protected local Web resource by authenticating users against a local data store (see "Modifying Configuration Files" on page 29).



This page demonstrates the contrast between local and remote sign-on at the SP site. Local accounts are also used for account linking (see "Configuring the SP to Use Account Linking" on page 24).

Using the SP Target Resource Page

This page represents the protected "target" resource of the SSO transaction:

In a real scenario, the User Attributes on the left might be used to determine Web-application authorization levels or how target Web pages should be personalized or branded. For demonstration purposes, several options are available from this page.

The logout options are explained on the screen. This section provides further information.

- The link associated with terminating an account link causes an error unless you modify the SP configuration to enable this feature (see "Configuring the SP to Use Account Linking" on page 24).
- The **Single Logout** links direct your browser to the SP Welcome page, regardless of whether you initiated SSO from the SP or the IdP.
- If you arrived at this page from the IdP's Web Portal page, you might notice that the User Attributes From the IdP are not exactly the same as those you saw on the IdP page. This is the result of attribute-mapping features employed for the adapters in the partner-connection configurations. You can see this mapping on the Attribute Contract Fulfillment page for the IdP's

connection to the SP on the first figure below and on Adapter Contract Fulfillment for the SP's connection to the IdP on the second figure below.

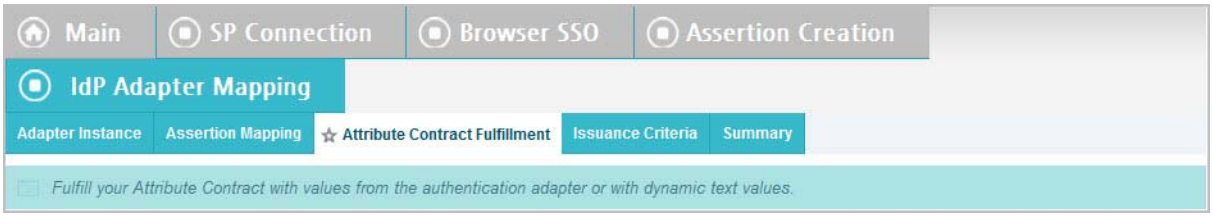


Figure 1: Navigation to Idp-to-SP Attribute Contract Fulfillment

Figure 2: Navigation to SP-to-IdP Adapter Contract Fulfillment

When you find these screens in the administrative console, click the **Help** links to learn about attribute-mapping options. (For more information, see the "Console Navigation" chapter in *Getting Started*.)

Chapter 4

Modifying the Configuration

This section provides pointers for reviewing the configuration of the quick-start IdP and SP partner connections in the PingFederate administrative console. You can also change the console configuration and deployment settings to extend the behavior of the quick-start applications and enable some advanced options.

Note: The administrative-console information in this section is intended as a starting point to introduce new users to PingFederate. Please refer to the Administrator's Manual or console **Help** pages for details about changing or adding to the quick-start settings and for configuring your own identity-federation gateway.

This chapter covers these topics:

- "Using the Administrative Console"
- "Modifying Configuration Files"
- "Extending Use Cases"

Using the Administrative Console

You can view and modify the preconfigured settings for the quick-start applications in the PingFederate administrative console. The following sections provide first-time users with information on how to run the console and a primer on a few of its major elements.

- "Accessing the Console"
- "Navigating Server Settings"
- "Viewing the Quick-Start Configuration"
- "Changing the Console Configuration"
- "Configuring Other Deployments"

Tip: For important information about using the administrative console, see the "Console Navigation" chapter in *Getting Started*.

Accessing the Console

To access the PingFederate administrative console:

1. Ensure that your PingFederate server is running.
2. Use your browser to reach the following URL:

   `https://localhost:9999/pingfederate/app`
3. If you are running the server console for the first time, enter the default Username and Password:

   Username: `Administrator`

   Password: `2Federate`

   If you have already run through the initial setup, enter the Username and Password of an administrator with both Admin and Crypto Admin privileges (see "Account Management" in the System Administration chapter of the PingFederate *Administrator's Manual*).

   Click **Login**.
4. If you are running the server console for the first time, you must change the Administrator password.

   Update the password and click **Save**.
5. Continue through the initial installation screens by clicking **Next** until you reach the Summary screen. Then click **Save**.

Navigating Server Settings

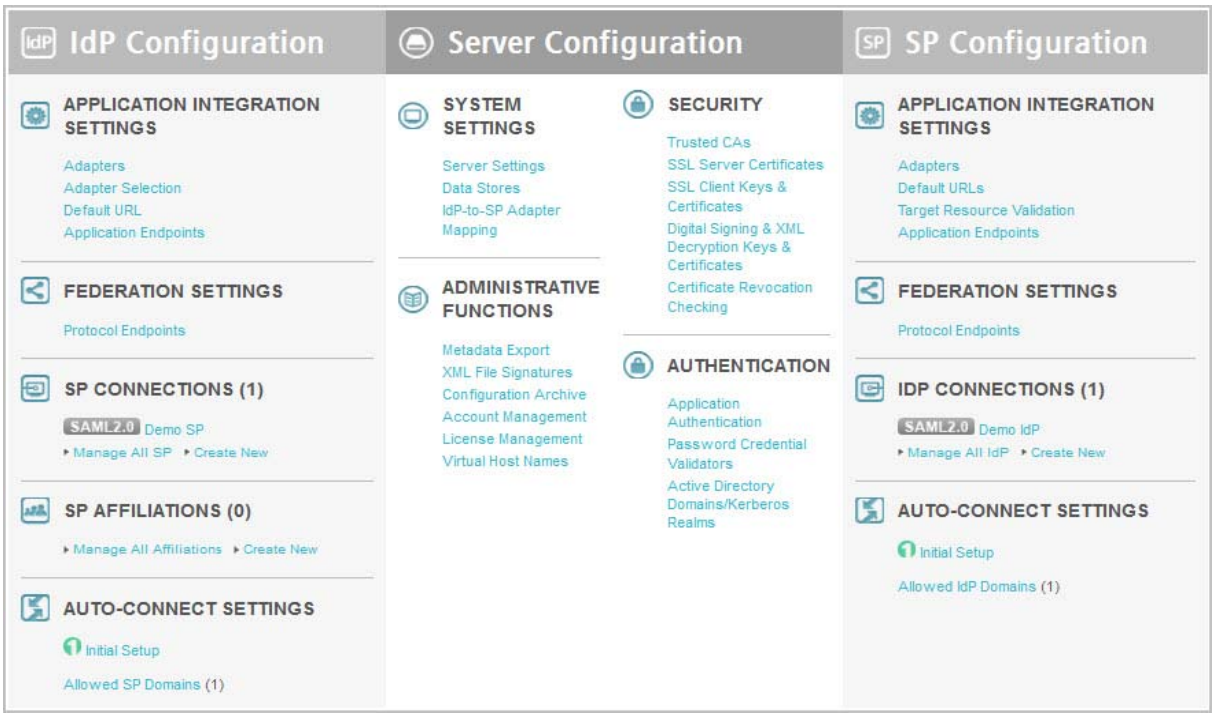
If you are accessing the console for the first time, click through the initial My Server screens until you reach the Summary screen, and then click **Save** to reach the Main Menu.

Note: This procedure allows you to reach the quick-start configuration easily. You can return to modify configuration settings by using the **Server Settings** link on the Main Menu at any time.

Viewing the Quick-Start Configuration

The PingFederate Main Menu provides access to existing configuration settings, as well as to step-by-step screen flows that guide you through new configurations. This section provides a broad-brush overview of settings for the quick-start applications; refer to the online **Help** pages or the Administrator's Manual for detailed information.

To return to the Main Menu from any screen in the configuration settings, click **Main** at the upper-left of the screen. (For more information about using the administrative console, see the "Console Navigation" chapter in *Getting Started*.)



▶ To view the major elements of the quick-start configuration:

- Click each of the Adapters links under Application Integration Settings for the IdP and SP Configuration sections.
- These settings are used to communicate with the respective local authentication mechanism. On the Manage Adapter Instances screens for each configuration, click the Adapter Instance Name links to review the settings.
- On the Main Menu under My Server, click the **Server Settings** link under System Settings.
- From the Summary screen, review the settings under **Roles and Protocols** and **Federation Info**. These settings specify which federation role(s) and protocol(s) the PingFederate server supports and identify the server endpoint uniquely among federation partners.

- Click the **Demo SP** and the **Demo IdP** links in the My IdP Configuration and My SP Configuration sections, respectively.

  From the Activation & Summary screen, you can browse these settings to familiarize yourself with connection-configuration requirements and options.

Tip: To return to the Summary screen from other screens in the connection configuration, click the **Activation & Summary** task links. If these links do not appear on particular screens, click **Done** or **Next** until you reach a screen that does display the link. (For more information, see "Console Buttons" in the "Console Navigation" chapter of *Getting Started*.)

Changing the Console Configuration

You can modify the administrative-console configuration in numerous ways and then use the quick-start applications to test connections and see end-to-end processing (see "Extending Use Cases" on page 30). Several examples are discussed next.

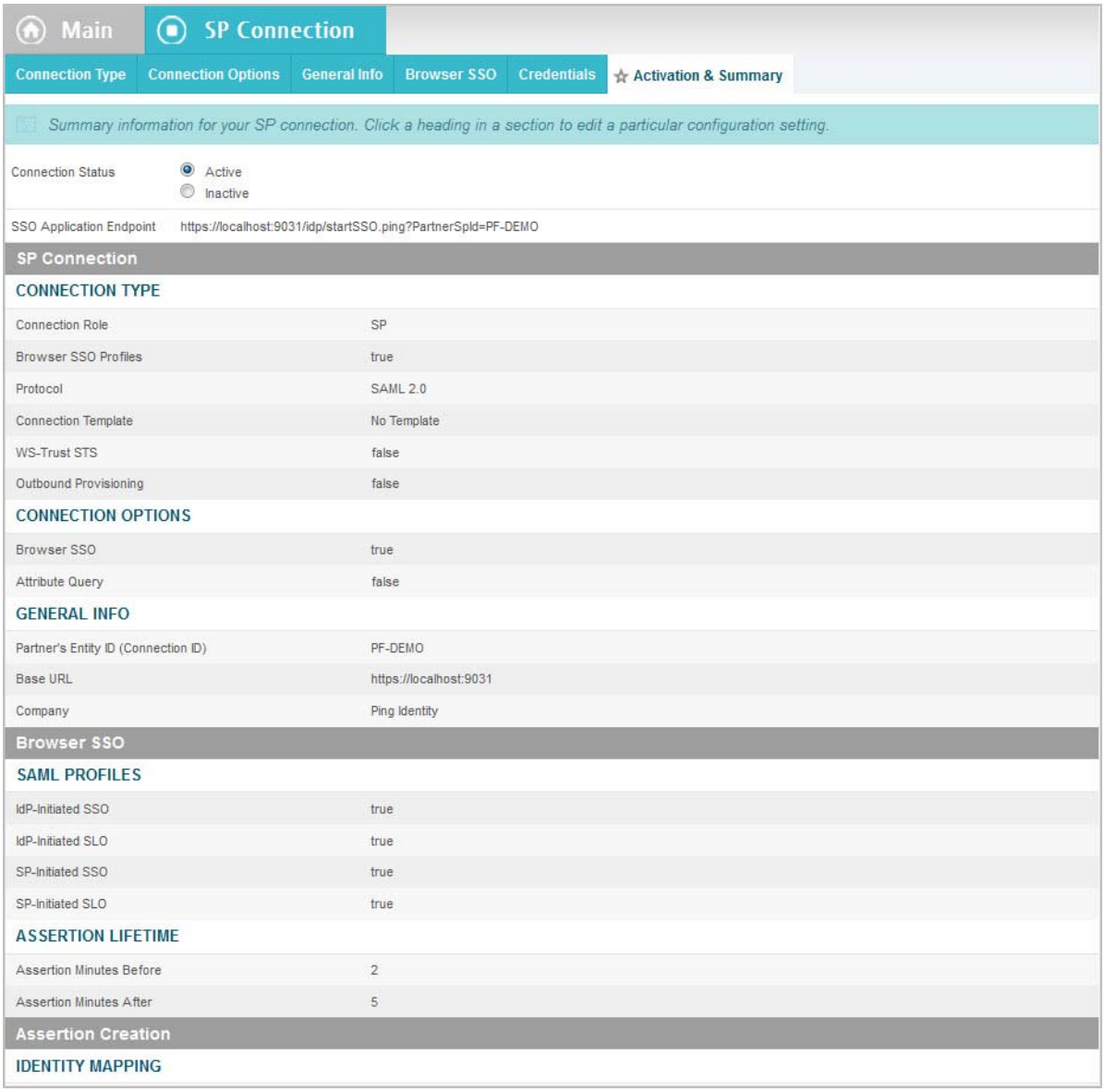
- "Configuring the IdP to Use Pseudonyms"
- "Configuring the SP to Use Account Linking"
- "Configuring XML Encryption"

Configuring the IdP to Use Pseudonyms

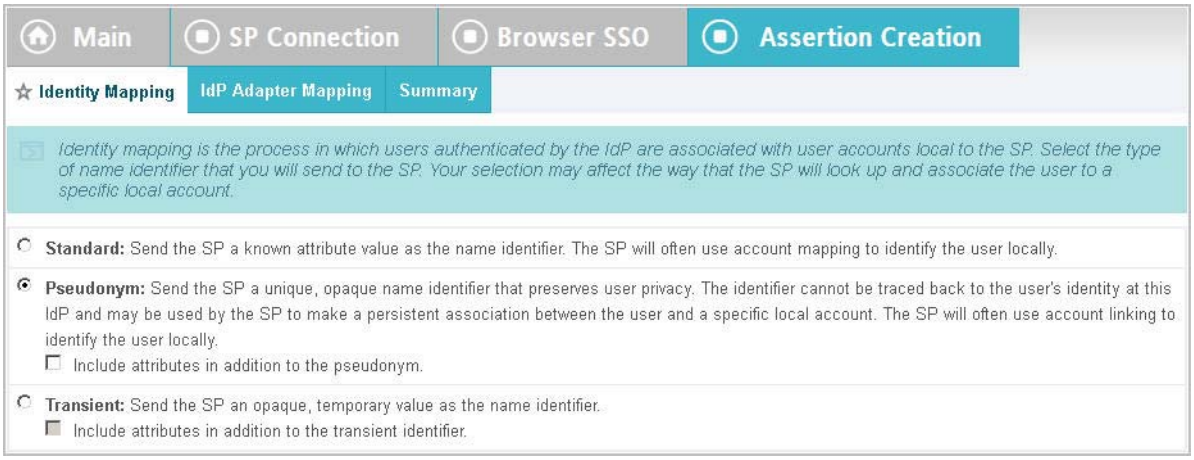
PingFederate supports the use of *pseudonyms* to identify users in SSO transactions for which privacy is a concern (see "Account Linking" in the Key Concepts chapter of the PingFederate *Administrator's Manual*). The quick-start applications may be used to demonstrate this functionality.

To configure the IdP to use pseudonyms:

1. On the Main Menu, access the **Demo SP** partner connection (see "Viewing the Quick-Start Configuration" on page 20).



2. On the Activation & Summary screen, under Assertion Creation, click **Identity Mapping**.



3. On the Identity Mapping screen, select **Pseudonym**.
4. (Optional) Select the checkbox to include attributes in addition to the pseudonym.

   If you make this selection, the attribute table on the quick-start SP Target Resource page will look the same except for the UserId value. If you leave this checkbox unselected, UserId is the *only* attribute that will appear in the table.

   Note: If you leave the checkbox unselected, you will have to reconfigure the **Attribute Contract** and **IdP Adapter Mapping** (or redeploy the PingFederate configuration archive) if you want to restore original functionality.

5. Click **Done**.
6. On the Assertion Creation screen, click **Done**.
7. On the Browser SSO screen, click **Save**.

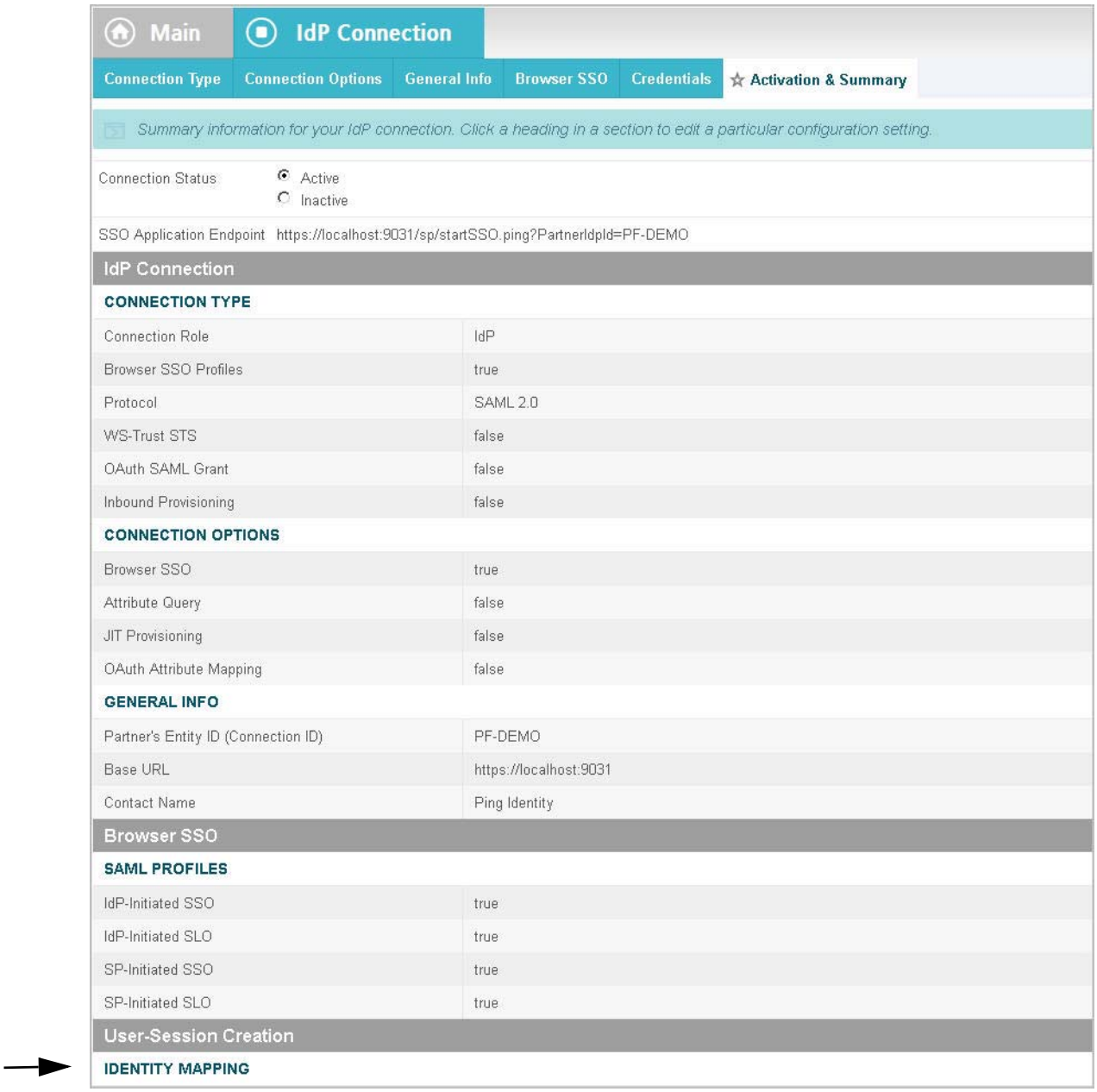
You can now check the result of the configuration immediately by trying SSO for any user from the IdP or SP quick-start applications. Note that the UserId passed in the assertion is obfuscated.

Configuring the SP to Use Account Linking

Account linking establishes a persistent association between two accounts for the same user in different domains (see "Account Linking" in the Key Concepts chapter of the PingFederate *Administrator's Manual*). By configuring account linking for the quick-start applications in PingFederate, you set up a different sequence through the SSO process. In addition, you will enable the **Terminate Account Link** option on the SP Target Application page.

To configure SP account linking:

1. On the Main Menu, access the **Demo IdP** partner connection (see "Viewing the Quick-Start Configuration" on page 20).



2. On the Activation & Summary screen, under User-Session Creation, click **Identity Mapping**.

3. On the Identity Mapping screen, select **Account Linking**.
4. (Optional) Select the checkbox to include attributes in addition to the pseudonym.

   If you leave this checkbox unselected, UserId is the *only* attribute that will appear in the table of attributes shown on the SP Target Resource page.

   Note: If you leave the checkbox unselected, you will have to reconfigure the **Attribute Contract** and **Adapter Mapping & User Lookup** (or redeploy the PingFederate configuration archive) if you want to restore original functionality.

5. Click **Adapter Mapping & User Lookup**.
6. On the Adapter Mapping & User Lookup screen, click **SP Adapter** under Adapter Instance Name.
7. Click **Adapter Contract Fulfillment**.

   On this screen, remap the Adapter Contract attribute userid to use Account Link as the Source and Local User Id as the Value.
8. Click **Done**.
9. On the Adapter Mapping & User Lookup, click **Done**.
10. On the User-Session Creation screen, click **Done**.
11. On the Browser SSO screen, click **Save**.

You can now test the result of the configuration immediately by trying SSO for any user from either the IdP or SP Quick-Start Application. The first time SSO is initiated, you will see a screen asking the user to log on locally to the SP in order to establish an account link.

Configuring XML Encryption

To enhance privacy, you can set up SP and IdP connections to encrypt all or part of SAML assertions and SLO name-identifier data. To do this, start by setting the Encryption Policy in the Protocol Settings task (under Browser SSO) for each partner connection. For more information, consult the context-sensitive **Help** or see "XML Encryption" in the Key Concepts chapter of the PingFederate

Administrator's Manual.

Configuring Other Deployments

You can change the way the quick-start applications are deployed in several ways, as described in this section.

- Using Separate Servers
- Using Other Web Containers

Using Separate Servers

For demonstration purposes, the included `data.zip` archive configures a single PingFederate instance to serve both the IdP and SP roles. In such a deployment, PingFederate performs a loopback, sending messages to and from itself. While this scenario keeps the setup simple, it does not represent a realistic scenario.

As an exercise to further your understanding of end-to-end processing between business partners, you may wish to deploy the quick-start applications on two separate servers. This scenario would require several URL changes and SSL-certificate updates for the separate IdP and SP PingFederate installations, as well as updates in the quick-start application configurations. The steps are described in the sections below.

Note: The changes necessary to support Auto-Connect between two separate servers involve additional steps not discussed here. Refer to the PingFederate Administrator's Manual for information, if you want to try changes to this configuration.

Initial Setup:

1. Deploy the `quickstart` components into a second instance of PingFederate running on a remote host (see "Deploying the Quick-Start" on page 8).

   Note: You may choose to set up two new hosts.

2. Choose which federation role you want the PingFederate server to perform (IdP or SP) by disabling the opposite role in each PingFederate administrative console:

   For an existing deployment, in the Main Menu click **Server Settings** and then **Roles & Protocols**. Clear the checkbox for the applicable role and click **Save**.

   For a new deployment, you will reach this screen when you set up PingFederate (see "Navigating Server Settings" on page 20). You can make your choice at that time and click **Next**.

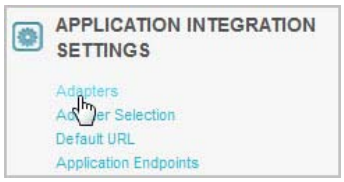
3. Under Server Settings on the **Federation Info** screen for each server, update the Base URL to reflect the host name or IP address of the *local* PingFederate installation, and then click **Save**.

Update Endpoints:

1. On the General Info screens for both the **Demo SP** and the **Demo IdP** connections on the respective servers, change the Base URL fields to point to the *partner* PingFederate host name or IP address.
2. Update the URLs configured for the IdP and SP quick-start adapter instances to point to the host name or IdP address of the respective *local* quick-start applications.

   These updates allow each PingFederate server to communicate with the local quick-start application.

   The **Adapters** configuration links are available under Application Integration Settings in both the IdP and SP Configuration sections:

   On the Manage Adapter Instances screens, click the Adapter Instance Name on both the IdP and SP sides. Then update the URL "Endpoint" fields on the IdP Adapter and SP Adapter screens, respectively.

   Be sure to click **Save** after you have made your changes.
3. Update the IdP and SP **Default URL(s)** settings via the Main Menu to point to the host name or IP address of the respective, *local* quick-start applications.

   These links are just below the adapter links under Application Integration Settings (there are two URLs for the SP).

   Be sure to click **Save** after you have made your changes.

Update Certificates:

Note: Refer to Chapter 5 of the PingFederate *Administrator's Guide* for detailed information about managing certificates.

1. On each server, use PingFederate to create a new SSL server certificate with a CN that corresponds to the host name or IP address of the server.
2. On each server, export the public portion of the new SSL server certificate and then import it back into PingFederate's list of Trusted CAs.

3. For each application deployment, replace the following SSL client certificates with the newly exported SSL certificates. The quick-start

applications use these certificates to communicate with the local PingFederate server.

Replace these certificates:

- (IdP server) Use the IdP-generated public SSL-certificate file in place of:
  `quickstart-app-idp.war\WEB-INF\classes\pf.https.server.crt`
- (SP server) Use the SP-generated public SSL-certificate file in place of:
  `quickstart-app-sp.war\WEB-INF\classes\pf.https.server.crt`

Important: Use the installed file names in each case.

4. Exchange the exported SSL server certificates between PingFederate servers: on each server, import the partner server's SSL certificate into PingFederate's list of Trusted CAs.

Update Application Configurations:

The quick-start applications need to know where the PingFederate server is deployed, so the links and buttons within the applications will use the correct URLs to PingFederate endpoints.

For each relevant deployment, change the value of `pf.hostname` in the file `WEB-INF/classes config.props` file to the host name or IP address where the local PingFederate is running (see "Modifying Configuration Files" on page 29):

- For the IdP PingFederate installation, change the properties file in the `quickstart-app-idp.war` deployment.
- For the SP PingFederate installation, change the properties file in the `quickstart-app-sp.war` deployment.

Using Other Web Containers

For simplicity, PingFederate's application server is used to host the quick-start applications. This allows for simpler setup for demonstration purposes but does not represent a realistic deployment. A more realistic scenario is to deploy the applications in an independent servlet container, or two different Web containers.

To do this, you will need to make the same configuration changes described in the previous section. You may also need to update the Trusted CAs in PingFederate with the container's SSL server certificate, depending on the container's SSL configuration.

Modifying Configuration Files

You can change several properties that the quick-start applications use to interact with the PingFederate server, including the server's host name and port. In addition, you can add users and modify users attributes for either application.

The configuration files used for these purposes are located in the quick-start `WAR` directories in their respective `WEB-INF/classes` directories (see "Quick-Start Components" on page 7):

- `config.props` – These files contain properties needed for each quick-start application to communicate with the PingFederate server. Refer to the file for descriptions of each property.
- `users.xml` – Use this file in either of the quick-start deployments to add users or modify user information.

Extending Use Cases

The quick-start applications demonstrate a basic set of SAML 2.0 use cases with a preconfigured PingFederate server instance. The applications and the server configuration are also partially set up to facilitate adding some additional features (see "Modifying the Configuration" on page 19).

PingFederate supports additional protocols and numerous configuration options. You can adapt the quick-start applications to use additional PingFederate configurations that more closely match your intended use. (Configurations are not provided for alternate implementations—please consult the Administrator's Manual for information.)

Other scenarios and features that can be configured with the quick-start applications include:

- **Other protocols** – These include SAML 1.0, SAML 1.1, and WS-Federation.
- **Additional back-channel security requirements** – The basic quick-start scenario uses digital signatures to secure SOAP communication. Alternatives include HTTP Basic, SSL client certificates, or any combination of the three.
- **Encryption and signatures** – You can choose to encrypt all or part of the SAML assertions, or require digital signatures on some or all HTTP requests and responses.
- **Data stores** – You can add connections in PingFederate to JDBC-enabled databases, LDAP directories, or custom data sources. In the IdP role, the server can use the data store to look up user attributes to include in an assertion. As an SP, the server can look up attributes to send to the SP application. (You will need to add user IDs to the relevant server's data store—see "Modifying Configuration Files" on page 29.)