PingFederate®

Salesforce Connector

Version 4.1

Quick Connection Guide

Ping Identity®

PingFederate Salesforce *Quick Connection Guide*
Version 4.1
June, 2011

Ping Identity Corporation
1001 17th St, 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: http://www.pingidentity.com

Trademarks

Disclaimer

This document is provided for informational purposes only, and the information herein is subject to change without notice. Ping Identity Corporation does not provide any warranties and specifically disclaims any liability in connection with this document.

Contents

Preface

About This Manual

This *Guide* provides procedures for configuring a PingFederate server to enable secure Internet single sign-on (SSO) for an organization's user accounts with Salesforce services.

The *Guide* also provides Software-as-a-Service (SaaS) user-provisioning configuration information relevant to Salesforce.

Tip: For general information and instructions on using SaaS Provisioning, see "Configuring SaaS Provisioning" in the "Identity Provider SSO Configuration" chapter of the PingFederate *Administrator's Manual*. (The same material is presented in a different format on the context-sensitive **Help** pages.)

Note: SaaS Provisioning is applicable only for customers using PingFederate 6.x (or higher) under separate license agreements.

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. For installation and configuration, some familiarity with PingFederate operations and the administrative console, as well as Salesforce administration, is highly recommended.

If you are not familiar with cross-domain Internet SSO or identity federation, it might be helpful to browse through the first few sections of *Getting Started* and the *Administrator's Manual* in your PingFederate installation before continuing.

Summary

The *Guide* consists of the following chapters:

- Chapter 1, “Introduction”— An overview of Connector features, system requirements, and use cases.
- Chapter 2, “Installation and Setup”— Installation and preliminary configuration instructions.
- Chapter 3, “Connecting to Salesforce”— How to set up PingFederate to connect to Salesforce CRM & Chatter.
- Appendix A, “Process Diagrams”— Illustrations and detailed processing information for all of the Connector use cases.

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 and Resources

This *Guide* refers frequently to information contained in manuals that are part of the core PingFederate distribution. The documents, listed below, are located in the installation’s `pingfederate/docs` directory.

Tip: PingFederate also 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, including SaaS Provisioning configuration—also connection-endpoint and other Web-application developer information, a glossary, and a list of common acronyms.

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

The PingFederate Salesforce Connector extends PingFederate capabilities to allow enterprises to provide secure single sign-on (SSO), with optional user provisioning, to Salesforce Customer Relations Management (CRM), including Chatter, as well as the Salesforce Partner and Customer Portals.

Note: The Connector package includes quick-connection templates that automatically configure many of the settings in the PingFederate administrative console required for SSO to Salesforce services (see "Connecting to Salesforce" on page 23). The package also contains libraries that support Software-as-a-Service (SaaS) Provisioning (licensed separately) for Salesforce (see "SaaS Provisioning" in the "Key Concepts" chapter of the PingFederate *Administrator's Manual*).

For several use cases, the Connector uses a Service Provider (SP) Adapter and an Authentication Web Service to interact with Salesforce and its proprietary SSO delegated-authentication mechanism (see "Overview" on page 6). The Authentication Web Service uses `OpenToken`, a secure standard, to keep credentials within the company domain.

For CRM & Chatter connections, the Connector also provides support for the Salesforce SAML 2.0 implementation, including metadata import as well as a quick-connection template.

Note: The SAML configuration does not require the SP Adapter or the Authentication Web Service.

With PingFederate, enterprises acting as Identity Providers (IdPs) can enable Salesforce SSO based on various existing authentication methods, including Integrated Windows Authentication (IWA), LDAP authentication, or other Identity Management (IdM) systems. Ping Identity offers Integration Kits to handle a wide variety of authentication mechanisms (see the list of kits available on the Ping Identity Web site (`www.pingidentity.com/products/integration-kits.cfm`).

Note: PingFederate and the Salesforce Connector (formerly the Salesforce.com Integration Kit) are both certified by the Salesforce.com AppExchange.

Overview

The Salesforce Connector is designed to work with the specific use cases described in this section. (For illustrations of supporting implementations and detailed, step-by-step processing descriptions, see "Process Diagrams" on page 37.)

Note: Several of these scenarios require both IdP and SP connections to enable access to the Salesforce proprietary delegated-authentication SSO gateway. (For more information, see "Using a Loopback Connection" on page 22.)

This overview breaks down the usage scenarios into two parts:

- Primary Use Cases
- Secondary Use Cases

Based on these scenarios, a decision table is provided to help administrators determine how to implement requirements and use this *Guide* (see "Choosing a Configuration Path" on page 8).

Primary Use Cases

The main purpose of the Salesforce Connector is to provide SSO (with optional SaaS Provisioning) to Salesforce CRM & Chatter and, separately, to the Salesforce Customer and/or Partner Portals. In addition, the Connector supports SP-initiated SSO using deep links (to internal CRM & Chatter pages) as well as IdP logout from Salesforce.

- IdP-Initiated SSO to CRM & Chatter

  The user logs on to an IdP application or company portal integrated with PingFederate. By clicking a specific URL that goes through PingFederate, the user can sign on seamlessly (without re-authentication) to Salesforce CRM & Chatter.

  The Connector supports two alternative implementations:

  – IdP-Initiated SSO via SAML 2.0

    This choice requires the least configuration but may be used *only* if your SSO deployment does not include any secondary use cases (see "Secondary Use Cases" on page 7).

  - IdP-Initiated SSO via Delegated Authentication

    Use this implementation if you also want to configure any secondary use case.

- IdP-Initiated SSO to the Salesforce Customer or Partner Portal

  From the end user's perspective, these cases are identical to the one above for CRM & Chatter, but extend to the Customer and Partner Portals. The user logs on to an IdP application or company portal and clicks a specific URL for immediate access to either of the Portals.

  These use cases are supported by one implementation—IdP-Initiated SSO via Delegated Authentication. (Currently, Salesforce does not support SAML for SSO to the Salesforce Portals.)

Tip: The connection templates configure most SSO settings to any or all Salesforce services automatically, including both the SP and IdP connections when required for delegated authentication (see "Connecting to Salesforce" on page 23).

- SP-Initiated SSO via Deep Linking

  The user directs the browser to a Web page inside Salesforce, which determines that the user has performed SSO previously and redirects the browser to the IdP for authentication (if no current session exists). After logging on, the user is redirected back to Salesforce—to the "deep link," rather than the default home page.

- SP-Initiated IdP Logout (SLO)

  The user is logged on to a Salesforce service and wants to log out of both Salesforce and the IdP application. Upon clicking the logout link, the user is also logged out of the IdP application.

Secondary Use Cases

These scenarios may be added to the primary use cases and require some additional configuration:

- SP-Initiated SSO via Direct Logon

  On one of the Salesforce service sign-on pages, a user enters a corporate email address and password and is authenticated via the PingFederate Authentication Service.

- Outlook Access via the Rich-Client Proxy Service

  Important: The proxy service is not required for using the Salesforce Outlook plug-in with PingFederate for SSO; the service is provided only as an extra level of password security (beyond SSL/TLS encryption) where needed.

  The user has installed the Salesforce Connect for Outlook plug-in. This plug-in normally makes a Web Service call to Salesforce with the Salesforce username and password to synchronize data between Salesforce and Outlook. Instead, when the proxy service is installed, corporate credentials are sent to the proxy, which validates the credentials against the corporate directory and replaces them with a secure token before passing the request on to Salesforce. With the Rich Client Proxy, corporate credentials do not leave the firewall.

Choosing a Configuration Path

After installing the Connector (see "Connector Installation" on page 11), use the table below as a reference to determine how to configure your Salesforce SSO deployment with PingFederate using this *Guide*.

Tip: If you are upgrading from a previous version of the Salesforce Connector, see "Upgrading Existing Salesforce Connectors" on page 13.

If you want:	With:	Then follow these steps:
SSO to & Salesforce CRM & Chatter	*No* secondary use cases (see "Secondary Use Cases" on page 7)	• Configure Salesforce for SSO and download SAML 2.0 metadata (see "Configuring Salesforce Accounts" on page 20). • Configure PingFederate using the SAML 2.0 Salesforce CRM & Chatter connection template (see "Connecting to Salesforce" on page 23).
	Any secondary use case (see "Secondary Use Cases" on page 7)	• Configure or verify Server Settings (see "Configuring Server Settings" on page 14). • Configure an instance of the Salesforce SP Adapter (see "Salesforce Adapter Setup" on page 16). • Configure Salesforce CRM & Chatter for SSO using delegated authentication (see "Configuring Salesforce Accounts" on page 20). • Configure PingFederate using the delegated-authentication connection template for Salesforce CRM & Chatter (see "Connecting to Salesforce" on page 23).
SSO to the Salesforce Customer or Partner Portal	Any different use case	• If not already done, configure or verify Server Settings (see "Configuring Server Settings" on page 14). • If not already done, configure an instance of the Salesforce SP Adapter (see "Salesforce Adapter Setup" on page 16). The same instance of the adapter may be used across SSO connections. • Configure the desired Salesforce Portal for SSO using delegated authentication (see "Configuring Salesforce Accounts" on page 20). • Configure PingFederate using the delegated-authentication connection template for the Salesforce Portal (see "Connecting to Salesforce" on page 23).

System Requirements

- PingFederate 6.x (or higher) installed with the OpenToken Adapter version 2.4 (or higher)
- An LDAP data store if either direct logon to Salesforce or the Outlook rich-client proxy is enabled (see "Overview" on page 6)

Connector ZIP Contents

The distribution ZIP file for the Salesforce Connector contains the following files:

- `GettingStarted.pdf` – Contains links to this online documentation.
- `/dist` – Contains libraries needed for the Adapter, the Authentication Web Service, and other features:
  - `opentoken-adapter-2.4.1.jar` – Current OpenToken Adapters
  - `pf-salesforce-sp-adapter-4.1.jar` – The PingFederate Salesforce Adapter
  - `pf-salesforce-commons-quickconnection-4.1.jar` – Components shared by all of the quick-connection plug-ins
  - `pf-salesforce-cp-quickconnection-4.1.jar` – The quick-connection plug-in to configure SSO for the Customer Portal
  - `pf-salesforce-crm-quickconnection-4.1.jar` – The quick-connection plug-in to configure SSO to Salesforce CRM & Chatter, using delegated authentication
  - `pf-salesforce-crm-saml2-quickconnection-4.1.jar` – The quick-connection plug-in to configure SSO for CRM & Chatter, using SAML 2.0.
  - `pf-salesforce-pp-quickconnection-4.1.jar` – The quick-connection plug-in to configure SSO to the Partner Portal
  - `pf-salesforce-service-4.1.war` – The PingFederate Salesforce Authentication Web Service
  - `pf-salesforce-rich-client-proxy-4.1.war` – The PingFederate Salesforce rich-client proxy service
  - `salesforce-partner-api-20.jar` – The Salesforce Application Programming Interface

Chapter 2

Installation and Setup

These sections provide instructions for setting up PingFederate and Salesforce to use the Salesforce Connector, including:

- "Connector Installation"
- "Configuring Server Settings"
- "Salesforce Adapter Setup"
- "Configuring Salesforce Accounts"
- "Using a Loopback Connection"
- "Configuring Windows for the Outlook Proxy Service"

Connector Installation

To install the Salesforce Connector:

1. Stop the PingFederate server if it is running.
2. Unzip the Salesforce Connector distribution ZIP file into a holding directory.
3. *If you are upgrading* from an existing Salesforce Connector, *delete* the previous installation files:

   The installation includes all `pf-salesforce*.jar` and `pf-salesforce*.war` files located in the directory:

   ```
   <pf_install>/pingfederate/server/default/deploy
   ```

   Note: Additional steps are needed for upgrading after completing this installation—see "Upgrading Existing Salesforce Connectors" on page 13.

4. From the distribution `dist` directory, copy the files:

- `pf-salesforce-*.jar` (6 files)
- `salesforce-partner-api-20.jar`

into the directory:

```
<pf_install>/pingfederate/server/default/deploy
```

5. If it exists, *delete* the file:

   ```
   salesforce-partner.jar
   ```

   from the directory:

   ```
   <pf_install>/pingfederate/server/default/lib
   ```

   This older version of the Salesforce API is present for PingFederate 6.3 and previous versions, and *may* be present for later versions if you are upgrading this Connector from a prior release.

Note: If you are configuring SSO to Salesforce CRM & Chatter *exclusively* under the SAML 2.0 protocol, skip the next step (see "Overview" on page 6).

6. *If* you are using Salesforce delegated authentication, copy the following WAR directory from `dist`:

   ```
   pf-salesforce-service-4.1.war
   ```

   into the directory:

   ```
   <pf_install>/pingfederate/server/default/deploy
   ```

   Note: This WAR file, for the PingFederate Authentication Web Service, is required for all use cases except direct SAML 2.0 SSO to Salesforce CRM & Chatter (see "Overview" on page 6).

7. *If* you require a proxy for use with the Outlook plug-in, copy the following WAR directory from `dist`:

   ```
   pf-salesforce-rich-client-proxy-4.1.war
   ```

   into the directory:

   ```
   <pf_install>/pingfederate/server/default/deploy
   ```

   For more information, see "Outlook Access via the Rich-Client Proxy Service" on page 44.

Note: The WAR directories are designed for portability and can be deployed, alternatively, within any Web container, such as Tomcat (if converted to WAR files) or Jetty, depending on your network-configuration needs.

8. Ensure that the version number of the previously installed PingFederate OpenToken Adapter JAR file is 2.4 or higher.

   The file is `opentoken-adapter-x.x.jar`, located in the same directory:

   ```
   <pf_install>/pingfederate/server/default/deploy
   ```

   If the JAR file name does *not* indicate version 2.4 or higher, *replace* it with the `opentoken-adapter-2.4.1.jar` file contained in the connector-distribution `dist` directory.

   Important: Be sure to remove the previously installed version of the OpenToken Adapter.

Note: If you are *not* using SaaS Provisioning, skip the next two steps.

9. If you are using SaaS Provisioning, ensure that your PingFederate license supports that feature.

   The license-key file, `pingfederate.lic`, is located in the `<pf_install>/pingfederate/server/default/conf` directory.

10. If you are using SaaS Provisioning, edit the `run.properties` file located in `<pf_install>/pingfederate/bin`, changing the property `pf.provisioner.mode` to the value shown here:

    ```
    pf.provisioner.mode=STANDALONE
    ```

    The property is located near the end of the file.

    For information about using the `FAILOVER` setting for runtime deployment, see the PingFederate Server Clustering Guide.

11. Start the PingFederate server.

12. *If* you are upgrading an existing Connector installation, continue to the next section.

Upgrading Existing Salesforce Connectors

If you are upgrading a previous version of the Salesforce SaaS Connector, use the following procedure to re-establish your PingFederate delegated-authentication connection to Salesforce CRM & Chatter (including SaaS provisioning when applicable). Afterward, you can add additional features as needed (see “Choosing a Configuration Path” on page 8).

Note: If you prefer to use the newer SAML 2.0 implementation for Salesforce CRM & Chatter, you must delete the previous SP and IdP connections and start over, including reconfiguration of provisioning if applicable. In that case, disregard this section and refer to “Choosing a Configuration Path” for more information.

To upgrade existing Salesforce CRM connections:

1. Modify the Salesforce SP adapter-instance configuration and redeploy configuration properties:
   a. Locate the SP Adapter Instance (click **Adapters** in the SP Configuration portion of the Main Menu).
   b. Click the Adapter Instance Name and go to the Instance Configuration screen.
   c. For the field Salesforce.com SSO Start Page, if a URL is present, change the version number of the PingFederate Authentication Service (at the end of the string) to **`4.1`**.
   d. Click **Show Advanced Fields.**
   e. For the field Salesforce.com Server URL, change this value:

      `https://www.salesforce.com/services/Soap/c/9.0`

      to this value:

      `https://www.salesforce.com/services/Soap/c/20.0`
   f. Click **Next** and use the Actions screen to export configuration files, and then deploy them as needed into newly installed WAR directories.

      For detailed instructions, follow the SP Adapter initial setup procedure Actions screen beginning at step 13.
   g. On the Actions screen, click **Done** and then **Save** on the Manage SP Adapter Instances screen.
2. Update the Salesforce administrative configuration for single sign-on (see "Using Delegated Authentication" on page 21).
3. If you are using the Rich Client Proxy Service, update the Windows Registry entry (see "Configuring Windows for the Outlook Proxy Service" on page 22).
4. Restart PingFederate.
5. For all Salesforce connections that include SaaS Provisioning:
   a. Click **Refresh Fields** on the Attribute Mapping screens for all provisioning-channel configurations.

      For more information, see sections under "Managing SaaS Channels" in the "Identity Provider SSO Configuration" chapter of the PingFederate *Administrator's Manual* (or click **Help** in configuration screens).
   b. Save the connection.

Configuring Server Settings

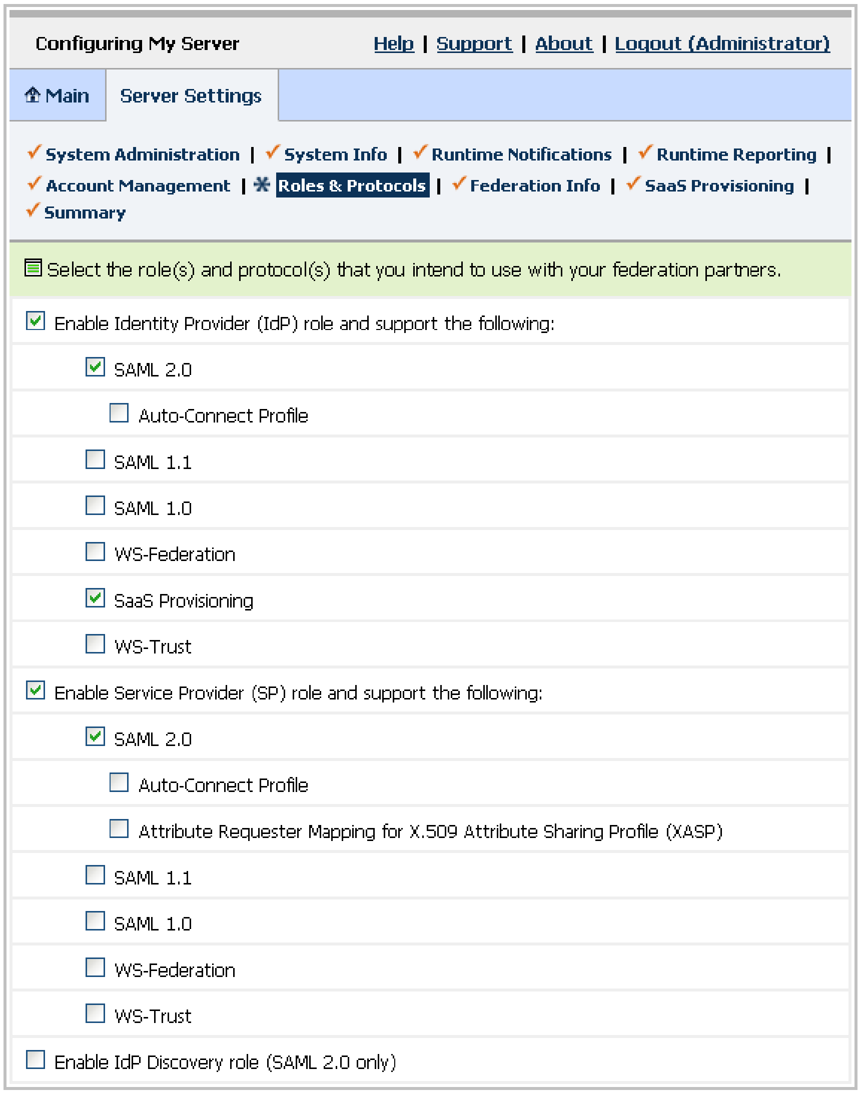
If you have not yet used PingFederate, follow the instructions under "Running PingFederate for the First Time" in the "Installation" chapter of *Getting Started*. To enable quick connections to Salesforce, several selections (described in the following procedure) are required when you reach Roles and Protocols in the Configuring My Server screen sequence.

If you have already run and configured the PingFederate server, you may need to verify or change settings on the Roles and Protocols screen, as well as enable SaaS Provisioning, as described in the following procedure.

To enable SSO quick connections to Salesforce:

1. On the Roles and Protocols screen, ensure that the IdP role is enabled and SAML 2.0 is selected for that role.

   (Click **Server Settings** on the Main Menu to locate this screen after initial installation.)

   Configuring My Server
   Help | Support | About | Logout (Administrator)
   Main
   Server Settings
   ✓ System Administration | ✓ System Info | ✓ Runtime Notifications | ✓ Runtime Reporting |
   ✓ Account Management | ✱ Roles & Protocols | ✓ Federation Info | ✓ SaaS Provisioning |
   ✓ Summary

   Select the role(s) and protocol(s) that you intend to use with your federation partners.

   ☑ Enable Identity Provider (IdP) role and support the following:
   - ☑ SAML 2.0
     - ☐ Auto-Connect Profile
   - ☐ SAML 1.1
   - ☐ SAML 1.0
   - ☐ WS-Federation
   - ☑ SaaS Provisioning
   - ☐ WS-Trust

   ☑ Enable Service Provider (SP) role and support the following:
   - ☑ SAML 2.0
     - ☐ Auto-Connect Profile
     - ☐ Attribute Requester Mapping for X.509 Attribute Sharing Profile (XASP)
   - ☐ SAML 1.1
   - ☐ SAML 1.0
   - ☐ WS-Federation
   - ☐ WS-Trust

   ☐ Enable IdP Discovery role (SAML 2.0 only)

2. If your PingFederate license includes SaaS Provisioning, select that option for the IdP role.

   Tip: This setting enables provisioning globally for all connections to supported SaaS providers. However, you have a choice of including provisioning or not during the configuration of specific connections.

3. *If* your SSO deployment for Salesforce services includes any connections using delegated authentication, enable the SP role, also using SAML 2.0.

   Note: This selection is *not* required for connections to Salesforce CRM & Chatter using the Salesforce native SAML 2.0 gateway. For delegated authentication, PingFederate coincidentally uses SAML 2.0 for both roles in a loopback connection, allowing the Salesforce SP Adapter to be used to communicate with the Salesforce delegated-authentication SSO mechanism (see "Salesforce Adapter Setup" on page 16).

4. Click **Next** to continue the Configuring My Server task (or **Save** for an existing configuration).

   Note: Enabling SaaS Provisioning adds a new screen to the task flow, requiring selection of a database used to monitor provisioning status. For more information, see "Configuring SaaS Provisioning Settings" in the "System Settings" chapter of the PingFederate *Administrator's Manual* (or click **Help** from the configuration screen).

Salesforce Adapter Setup

For SSO connections using Salesforce delegated authentication, the Salesforce SP Adapter should be configured prior to setting up an SSO connection to Salesforce.

Note: If you intend to configure *only* SSO to Salesforce CRM & Chatter via SAML 2.0, then you do *not* need to configure the SP Adapter.

Note: One instance of the adapter may be used across Salesforce connections.

To configure the Salesforce SP Adapter:

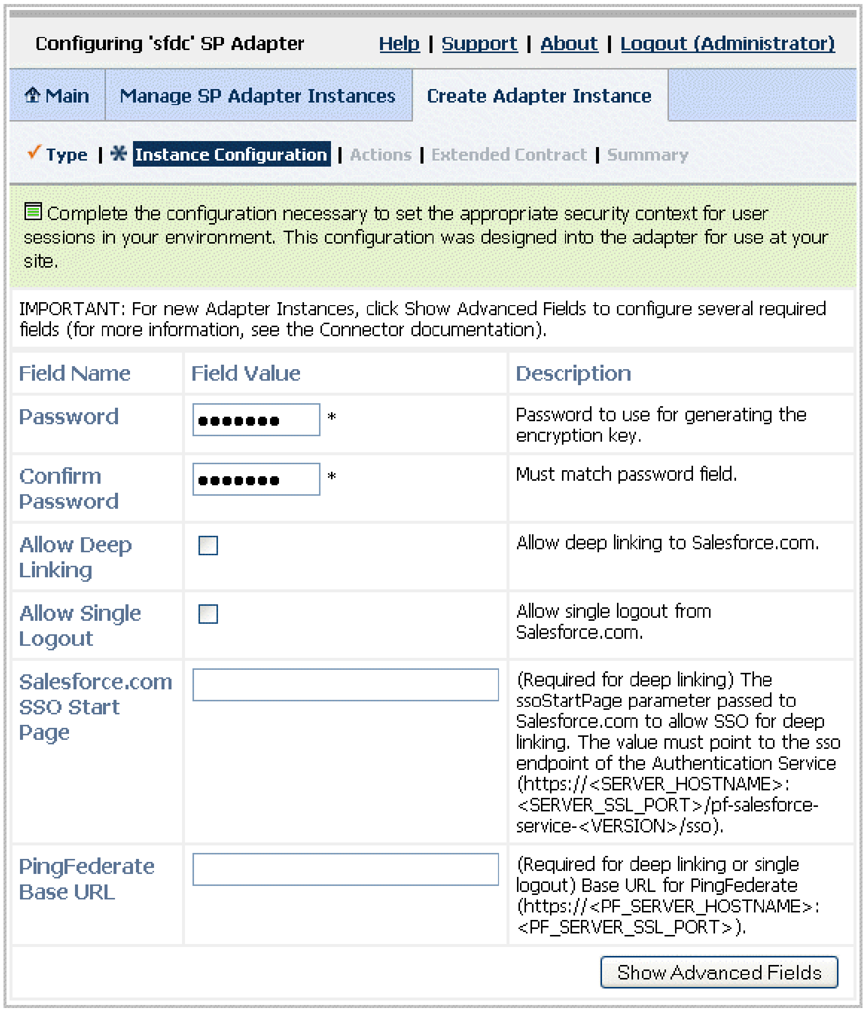
1. If not already done, set up PingFederate to act as an SP (as well as an IdP), using the SAML 2.0 protocol.

   (The use of SAML 2.0 as the protocol for the SP configuration is incidental and unrelated to using SAML 2.0 for direct SSO access to Salesforce CRM & Chatter.)

2. Log on to the PingFederate administrative console and click **Adapters** under My SP Configuration on the Main Menu.

3. On the Manage Adapter Instances screen, click **Create New Adapter Instance**.

4. On the Type screen, enter an Instance Name and ID, choose Salesforce.com Adapter 4.1 from the drop-down list, and click **Next**.


Configuring 'sfdc' SP Adapter
Help | Support | About | Logout (Administrator)
Main
Manage SP Adapter Instances
Create Adapter Instance
✓ Type | ✱ Instance Configuration | Actions | Extended Contract | Summary
Show Advanced Fields

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.

IMPORTANT: For new Adapter Instances, click Show Advanced Fields to configure several required fields (for more information, see the Connector documentation).

Field Name	Field Value	Description
Password	••••••• *	Password to use for generating the encryption key.
Confirm Password	••••••• *	Must match password field.
Allow Deep Linking	□	Allow deep linking to Salesforce.com.
Allow Single Logout	□	Allow single logout from Salesforce.com.
Salesforce.com SSO Start Page		(Required for deep linking) The ssoStartPage parameter passed to Salesforce.com to allow SSO for deep linking. The value must point to the sso endpoint of the Authentication Service (https://<SERVER_HOSTNAME>:<SERVER_SSL_PORT>/pf-salesforce-service-<VERSION>/sso).
PingFederate Base URL		(Required for deep linking or single logout) Base URL for PingFederate (https://<PF_SERVER_HOSTNAME>:<PF_SERVER_SSL_PORT>).

5. On the Instance Configuration screen, enter any password in the Password and Confirm Password fields.

6. (Optional) Select Allow Deep Linking if you want to enable this feature.

   You also need to complete the Salesforce.com SSO Start Page and PingFederate Base URL fields.

7. (Optional) Select **Allow Single Logout** if you want to enable this feature.

   You also need to complete the PingFederate Base URL field.

8. (Optional) Click **Show Advanced Fields** near the bottom of the screen.

9. (Optional) To enable direct login, select Allow Direct Login (in **Advanced Fields**) and provide information in the remaining LDAP-related fields on the screen.

   Refer to the screen descriptions for more information. Ensure that the LDAP-connection information you enter is complete and correct.

10. (Optional) To enable the Outlook rich-client proxy, provide information in the LDAP-related fields.

    Note that deployment of the proxy is not required to use the Salesforce Outlook plug-in with PingFederate. (For more information, see "Configuring Windows for the Outlook Proxy Service" on page 22 and "Outlook Access via the Rich-Client Proxy Service" on page 44.)

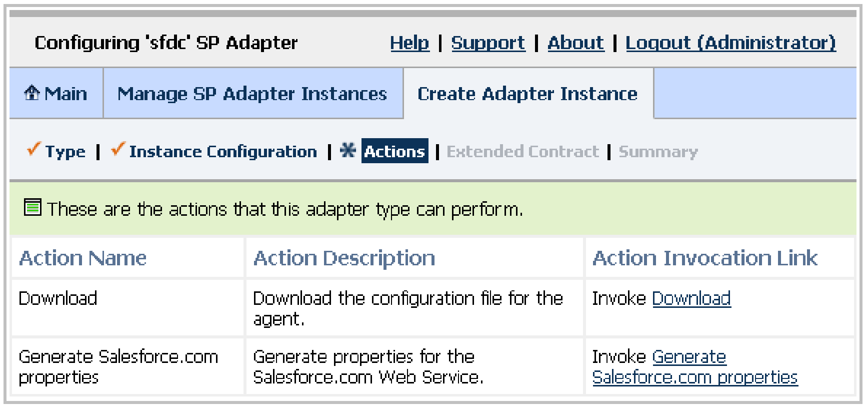
11. (Optional) To enable the Authentication Service to use client SSL/TLS for back-channel communication, select **Require Mutual TLS Authentication**.

    Enter the client-certificate Subject DN below the Mutual TLS selection if the Salesforce default DN is not correct.

    If not already accomplished for other purposes, additional steps are required to enable back-channel client authentication for the PingFederate server itself and the JBoss platform (see "Enabling Mutual SSL/TLS in PingFederate" on page 19).

Note: Other advanced selections and fields on the Instance Configuration screen are either optional or preset. Enter or modify other settings according to your implementation requirements.

12. Click **Next.**


Configuring 'sfdc' SP Adapter
Help | Support | About | Logout (Administrator)
Main
Manage SP Adapter Instances
Create Adapter Instance
✓ Type | ✓ Instance Configuration | Actions | Extended Contract | Summary

These are the actions that this adapter type can perform.

Action Name	Action Description	Action Invocation Link
Download	Download the configuration file for the agent.	Invoke Download
Generate Salesforce.com properties	Generate properties for the Salesforce.com Web Service.	Invoke Generate Salesforce.com properties

13. On the Actions screen, click **Download**.

14. On the next screen, click **Export** and save the file `agent-config.txt` into the directory:

    ```
    <pf_install>/pingfederate/server/default/deploy/pf-
    salesforce-service-4.1.war/WEB-INF/classes
    ```

    If you are using the rich-client proxy, copy the `agent-config.txt` into the directory:

    ```
    <pf_install>/pingfederate/server/default/deploy/pf-
    salesforce-rich-client-proxy-4.1.war/WEB-INF/classes
    ```

15. On the download screen, click **Reset** to return to the main Actions screen.

16. On the Actions screen, click **Generate Salesforce.com properties**.

17. On the next screen, click **Export** and save the file `pf-salesforce.properties` into the directory:

    `<pf_install>/pingfederate/server/default/deploy/pf-salesforce-service-4.1.war/WEB-INF/classes`

    If you are using the rich-client proxy, copy `pf-salesforce.properties` into the directory:

    `<pf_install>/pingfederate/server/default/deploy/pf-salesforce-rich-client-proxy-4.1.war/WEB-INF/classes`

18. Click **Next.**

19. On the Extended Contract screen, click **Next**.

    Extended attributes are not needed in most cases. (For more information, see "Adapter Contracts" in the "Key Concepts" chapter of the PingFederate *Administrator's Manual.*)

20. On the Summary screen, verify that the information is correct and click **Done**.

21. On the Manage Adapter Instances screen, click **Save** to complete the adapter configuration.

Enabling Mutual SSL/TLS in PingFederate

If you have set up the Salesforce SP Adapter to require back-channel mutual SSL/TLS authentication (see Step 11 on page 18 under Salesforce Adapter Setup), ensure that PingFederate is configured to support the option.

To configure PingFederate for mutual SSL/TLS authentication:

1. In the file `<pf_install>/pingfederate/bin/run.properties`, ensure that the value of pf.secondary.https.port is set to a valid port number.

    ✓ **Important:** Use this port for the Delegated Gateway URL in your Salesforce setup (see "Configuring Salesforce Accounts" on page 20).

2. In the file `<pf_install>/pingfederate/server/default/deploy/jetty.sar/META-INF/jboss-service.xml`, ensure that the value of the attribute named WantClientAuth is set to `true`.

    The attribute is located in the section Add a second HTTPS/SSL Connector.

3. Start or restart PingFederate.

Configuring Salesforce Accounts

This section provides instructions for setting up SSO for either SAML 2.0 or delegated authentication (or both) on the Salesforce administrative site (depending on your organizational needs—see "Overview" on page 6).

Note: These instructions are based on the Winter 11 update of Salesforce (scheduled for release in October, 2010). The administrative setup is subject to change. Please refer to the Salesforce online documentation for current or additional information, as needed.

We recommend testing the configuration using a Salesforce developer account before using it with your enterprise account.

Note: Salesforce accounts assigned the System Administrator profile cannot be set up to use SSO. This limitation is enforced by Salesforce.

Using SAML 2.0

For CRM & Chatter connections, you can use the SAML 2.0 standard for SSO.

Note: SAML XML transmissions containing assertions must be digitally signed. If you have not already done so, export the public certificate for the signing key to be used for the Salesforce connection(s). Note the file location. Certificate export is available via the **Digital Signing...** link in the Security section of the PingFederate Main Menu.

1. Log on as an administrator for your organization's Salesforce configuration.
2. Under Setup > Administration Setup > Security Controls, select:

   Single Sign-On Settings
3. On the Single Sign-On Settings screen, click **Edit**.
4. Select the checkbox to enable SAML, and choose version 2.0.
5. In the Issuer field, enter your site's Federation ID for SAML 2.0.

   The ID is located in PingFederate under **System Settings** on the Federation Info screen.
6. For the Identity Provider Certificate, click Browse to locate and upload the certificate for verifying your site's digital signatures.

7. (Optional) In the Identity Provider Login URL field, if you want to enable SP-initiated SSO for deep linking to Salesforce, enter the PingFederate endpoint URL for SSO.

   Tip: You can return to enter this URL later, after configuring the PingFederate SP connection. Just continue with the next steps, including downloading metadata. Then, when the SP connection is configured, you can copy the URL from the connection Summary screen and paste it here.

8. (Optional) In the Identity Provider Logout URL field, if you want to enable IdP-application logout concurrent with Salesforce logout, enter the URL for your IdP application's logout service.

   Salesforce sends a redirect to the URL after ending the Salesforce session.

9. Save the configuration.

10. Click **Download Metadata** and save the XML file.

    The file must be accessible to the machine running PingFederate. For versions 6.0-6.2, the quick-connection template looks for Salesforce metadata by default in the directory:

    ```
    <pf_install>/pingfederate/server/default/data
    ```

Other settings on the screen are either optional, outside the context of the PingFederate Connector, or preset to the correct defaults. For more information, refer to the Salesforce online Help.

Using Delegated Authentication

Follow the steps below to set up the Salesforce for delegated authentication.

Note: Delegated authentication is *not* enabled in Salesforce by default.

1. If you have not already done so, contact your Salesforce representative to enable delegated authentication for your organization.

2. Log on as an administrator for your organization's configuration for the applicable Salesforce service.

3. Under Setup > Administration Setup > Security Controls > Single Sign-On Settings, enter the Delegated Gateway URL.

   If PingFederate is not proxied by an HTTP server, the URL is:

   ```
   https://<PingFederate_URL>:<PingFederate_Https_Port>/
   pf-salesforce-service-4.1/services/
   AuthenticationService
   ```

   Note: Ensure that the server SSL certificate used by PingFederate is signed by a known Certificate Authority trusted by Salesforce. You must use an SSL connection to Salesforce.

4. Under Setup > Administration Setup > Manage Users > Profiles, edit each of the appropriate User Profiles to enable SSO.

   Select the checkbox to enable Single Sign-On.

5. *If* you are using the rich-client proxy, add the server IP that the proxy is running on to the trusted IP list in Salesforce under Setup > Administration Setup > Security Controls > Network Access.

   For more information, see "Configuring Windows for the Outlook Proxy Service" on page 22.

Using a Loopback Connection

The SP adapter instance needed for delegated authentication serves two functions:

- Provides a way of programmatically generating and exporting property files for the service WARs
- Serves as a proxy for last-mile integration to Salesforce in a loopback configuration (using PingFederate as both IdP and SP)

The delegated-authentication connection templates automatically configure most IdP and SP settings. Some additional, manual configuration is required if you are using deep linking or SP-initiated SSO/SLO, as indicated in the configuration steps (see "Connecting to Salesforce" on page 23).

Configuring Windows for the Outlook Proxy Service

Follow this procedure if you have deployed the rich-client proxy service to use in conjunction with the Connect for Outlook plug-in for Salesforce.

To configure Windows for the optional Outlook plug-in rich-client proxy service:

1. For each client running Outlook with the Salesforce plug-in, open the Windows Registry Editor, `regedit`, and locate the property ServerURL for Salesforce under HKEY_CURRENT_USER.

   Note: For versions 3.2.111 up to 3.3.110 of the plug-in on a 32-bit version of Windows, this property is located in the key:

   HKEY_CURRENT_USER\Software\Salesforce.com\SM

   Future releases may move this key, and it may be different for 64-bit versions of Windows.

2. Change the value of ServerUrl to:

   ```
   https://<PingFederate_URL>:<PingFederate_Https_Port>/
   pf-salesforce-rich-client-proxy-4.1/proxy
   ```

   For enterprise deployment, this registry change may be added to an automated logon script for the domain.

Chapter 3

Connecting to Salesforce

This chapter describes how to use the installed quick-connection templates to enable SSO for Salesforce services. In addition, a final section provides information on construction of SSO links to Salesforce (see "SSO Linking to Salesforce" on page 35).

The PingFederate administrative console uses quick-connection templates to configure most of the settings needed to connect to Salesforce for SSO. Choose the Salesforce template you want on the initial Connection Template screen during configuration of an SP Connection.

Connections to multiple Salesforce services require separate connections.

Note: For connections using Salesforce delegated authentication, the templates lay the foundation for both an SP Connection and an IdP Connection, in a loopback configuration. The IdP Connection uses the PingFederate Salesforce SP Adapter and Authentication Web Service to interact with Salesforce's proprietary SSO mechanism (see "Salesforce Adapter Setup" on page 16).

For connections using the Salesforce SAML 2.0 endpoint, the template prompts you to import metadata downloaded from the Salesforce administrative site (see "Configuring Salesforce Accounts" on page 20). The SAML 2.0 configuration does not require a loopback IdP Connection.

This section provides instructions for filling in site-specific connection settings. Once the settings are complete, if you are using SaaS Provisioning, you can configure provisioning settings according to your deployment needs.

Tip: This section is intended *only* to provide configuration instructions associated with using any of the quick-connection templates for SSO, along with SaaS-provisioning information related specifically to Salesforce. After completing the SSO configuration, if you are including provisioning for the connection, please refer to "Configuring SaaS Provisioning" in the "Identity Provider SSO Configuration" chapter of the PingFederate *Administrator's Manual* (or see the associated **Help** pages during the configuration).

Use the procedures in the following sections, in sequence, to configure SSO to any Salesforce services.

Tip: These procedures provide instructions for configuring minimum required connection settings; the instructions skip setup screens in which all necessary information is automatically configured (or in which standard defaults are used). The administrative console guides you to required configuration steps automatically by displaying prompts at entry points for the task flows (see "About Tasks and Steps" in the "Console Navigation" chapter of *Getting Started*).

Tip: The steps and screen captures in these procedures conform to the administrative console for PingFederate 6.1 and above. The configuration for version 6.0 is somewhat different at two points: selecting connection templates and configuring signing and verification certificates.

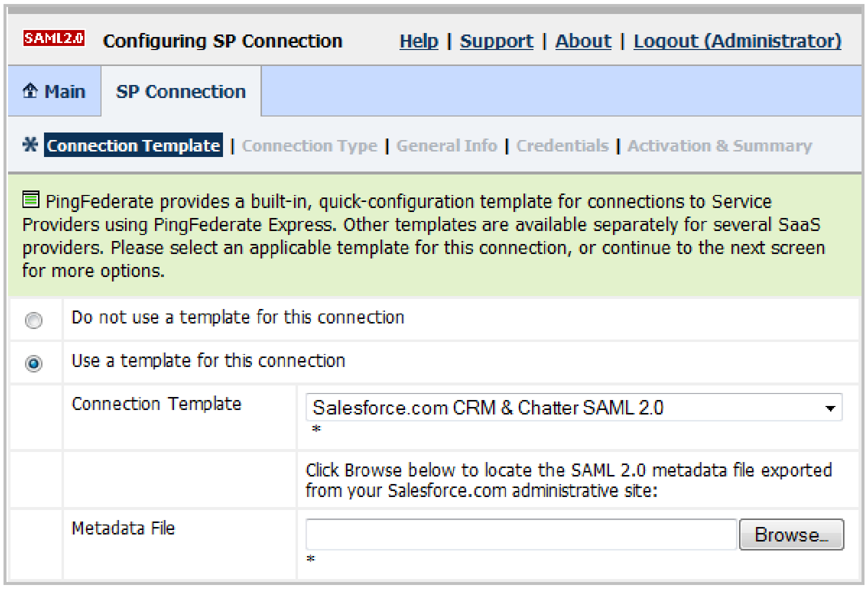
Configuring the SP Connection

To configure the SP connection to Salesforce:

1. If you have not already done so, follow the instructions under "Configuring Server Settings" on page 14.
2. If you have not already done so, configure the IdP Adapter you are using with PingFederate.

   For information and instructions, see "Configuring IdP Adapters" in the "Identity Provider SSO Configuration" chapter of the PingFederate *Administrator's Manual.*

3. On the Main Menu, click **Create New** under SP Connections in the My IdP Configuration section.


SAML2.0
Configuring SP Connection
Help | Support | About | Logout (Administrator)
Main
SP Connection
Connection Template | Connection Type | General Info | Credentials | Activation & Summary

PingFederate provides a built-in, quick-configuration template for connections to Service Providers using PingFederate Express. Other templates are available separately for several SaaS providers. Please select an applicable template for this connection, or continue to the next screen for more options.

○ Do not use a template for this connection

● Use a template for this connection

Connection Template: Salesforce.com CRM & Chatter SAML 2.0 *

Click Browse below to locate the SAML 2.0 metadata file exported from your Salesforce.com administrative site:

Metadata File: [ ] Browse... *

4. On the Connection Template screen, select the Salesforce.com template you want in the Connection Template drop-down list.

   If the template you want is not shown, verify the Connector installation and restart PingFederate.

   Note: For PingFederate 6.0, the Connection Template drop-down is part of the Connection Type screen.

5. If you are using the SAML 2.0 SSO template for Salesforce CRM & Chatter, click **Browse** to locate and upload the Salesforce Metadata File.

   Note: For PingFederate 6.0-6.2, there is no **Browse** button: ensure that the default path to the file, as shown in the text box, is correct.

   If you have not yet exported the metadata from Salesforce, do so now and then return to this screen to continue (see "Configuring Salesforce Accounts" on page 20).

6. Click **Next**.

7. Click **Next** again on the Connection Type screen.

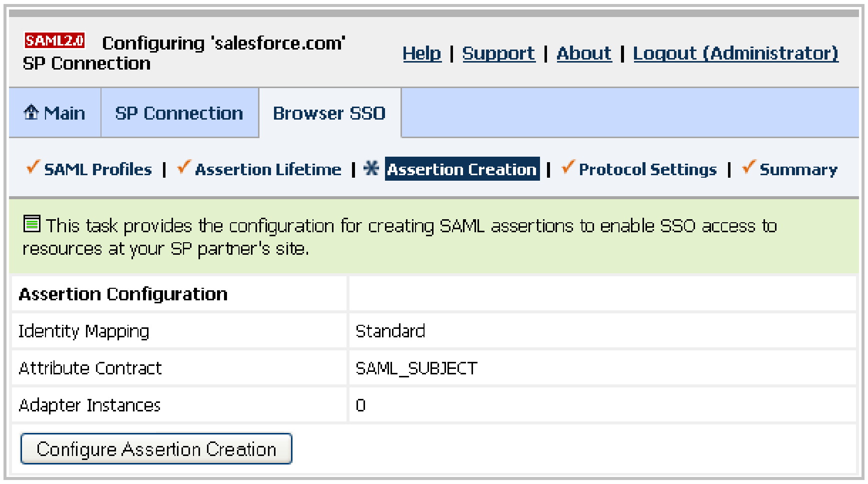
8. (Optional) On the Connection Options screen, if you are *not* using provisioning for this connection, clear the SaaS Provisioning checkbox.

   This feature is enabled by default for SaaS-provider connection types (assuming it is also enabled in System Settings—see "Configuring Server Settings" on page 14).

9. Click **Next**.

10. Click **Browser SSO** under the SP Connection tab, or click **Next**.

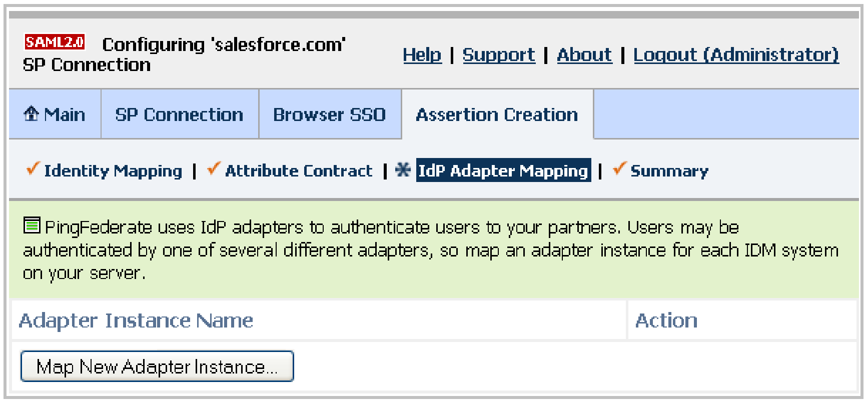
11. Click **Configure Browser SSO** on the Browser SSO screen.


SAML2.0
Configuring 'salesforce.com' SP Connection
Help | Support | About | Logout (Administrator)
Main
SP Connection
Browser SSO
✓ SAML Profiles | ✓ Assertion Lifetime | ✱ Assertion Creation | ✓ Protocol Settings | ✓ Summary
Configure Assertion Creation

This task provides the configuration for creating SAML assertions to enable SSO access to resources at your SP partner's site.

Assertion Configuration	
Identity Mapping	Standard
Attribute Contract	SAML_SUBJECT
Adapter Instances	0

12. On the Assertion Creation screen, click **Configure Assertion Creation**.


SAML2.0
Configuring 'salesforce.com' SP Connection
Help | Support | About | Logout (Administrator)
Main
SP Connection
Browser SSO
Assertion Creation
✓ Identity Mapping | ✓ Attribute Contract | ✱ IdP Adapter Mapping | ✓ Summary
Map New Adapter Instance...

PingFederate uses IdP adapters to authenticate users to your partners. Users may be authenticated by one of several different adapters, so map an adapter instance for each IDM system on your server.

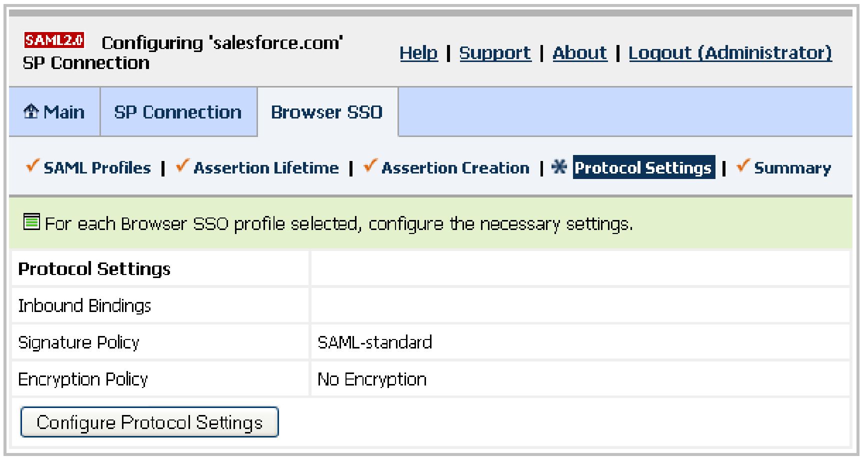
Adapter Instance Name	Action

13. On the IdP Adapter Mapping screen, click **Map New Adapter Instance** and map the IdP Adapter Instance you defined earlier in this procedure.

    This configuration is site-dependent and thus cannot be preconfigured. For detailed information and instructions, see “IdP Adapter Mapping” in the “Identity Provider SSO Configuration” chapter of the PingFederate *Administrator’s Manual* (or refer to the **Help** pages).

    When you return to this screen, click **Done**.

14. When you return to the Assertion Creation screen, click **Next**.



SAML2.0 Configuring 'salesforce.com' SP Connection
Help | Support | About | Logout (Administrator)
Main
SP Connection
Browser SSO
✓ SAML Profiles | ✓ Assertion Lifetime | ✓ Assertion Creation | Protocol Settings | ✓ Summary
Configure Protocol Settings

For each Browser SSO profile selected, configure the necessary settings.

Protocol Settings	
Inbound Bindings	
Signature Policy	SAML-standard
Encryption Policy	No Encryption

15. (Optional) If you require either SP-initiated SSO or SP-initiated SLO (for delegated-authentication connections), or both, click **SAML Profiles** under Browser SSO and follow these steps:

    a. On the SAML Profiles screen, select the checkbox(es) needed: SP-Initiated SSO and/or SP-Initiated SLO.

    Note: Do *not* select the SLO checkbox if you are configuring the connection template for CRM & Chatter via SAML 2.0. SP-initiated IdP logout from Salesforce, when enabled in the Salesforce administrative setup, is handled via redirects outside of SAML specifications. Clicking the checkbox here results in SAML protocol errors in the PingFederate connection configuration.

    b. Return to the **Protocol Settings** screen and click **Configure Protocol Settings**.

    c. On the SLO Service URLs screen (if presented), choose Redirect under Binding, enter `/sp/SLO.saml2` as the Endpoint URL, and then click **Add**.

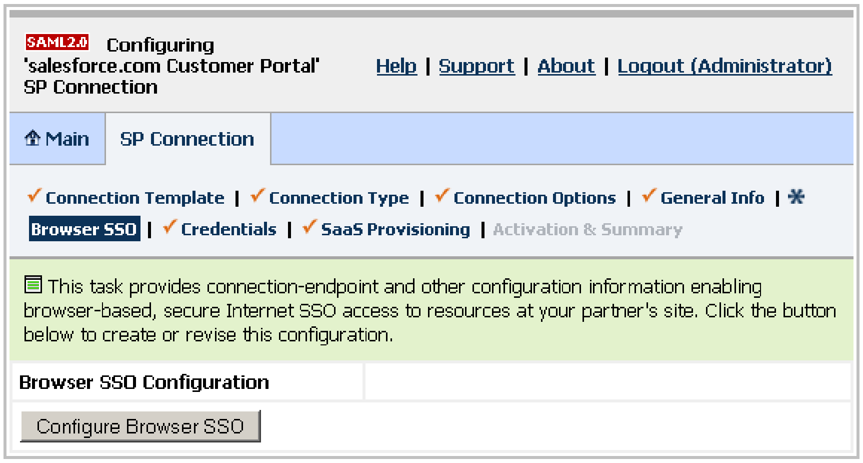
    d. Click **Next**.

    e. On the Allowable SAML Bindings screen, clear the checkboxes Artifact and SOAP if selected (retain or select POST and Redirect).

    f. Click **Done**.

16. On the Protocol Settings screen, click **Done**.

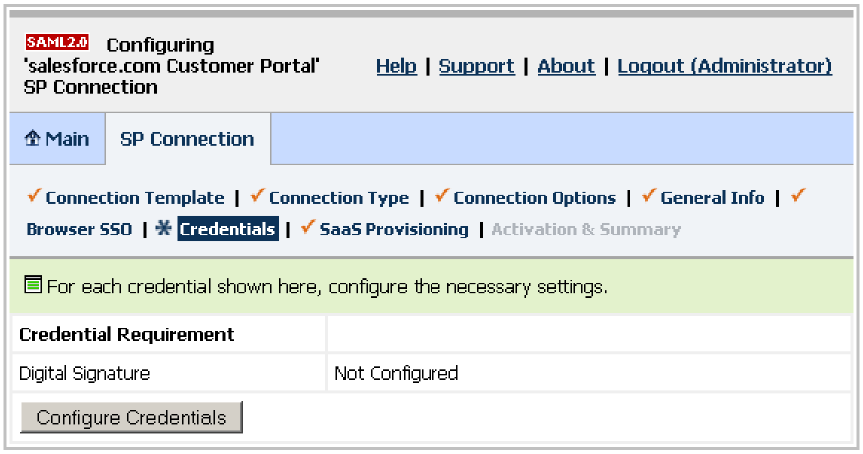
Tip: Except for the optional settings described above, this central task is completely configured for you, but click **Configure Protocol Settings** if you want to review the Salesforce connection settings. For configuration information, see sections under “Configuring Protocol Settings” in the “Identity Provider SSO Configuration” chapter of the PingFederate *Administrator’s Manual* (or use the context-sensitive **Help**).


SAML2.0
Configuring 'salesforce.com Customer Portal' SP Connection
Help | Support | About | Logout (Administrator)
Main
SP Connection
✓ Connection Template | ✓ Connection Type | ✓ Connection Options | ✓ General Info | ✱ Browser SSO | ✓ Credentials | ✓ SaaS Provisioning | Activation & Summary
Configure Browser SSO

This task provides connection-endpoint and other configuration information enabling browser-based, secure Internet SSO access to resources at your partner's site. Click the button below to create or revise this configuration.

Browser SSO Configuration	

17. On the Browser SSO screen, click **Next**.


SAML2.0
Configuring 'salesforce.com Customer Portal' SP Connection
Help | Support | About | Logout (Administrator)
Main
SP Connection
✓ Connection Template | ✓ Connection Type | ✓ Connection Options | ✓ General Info | ✓ Browser SSO | ✱ Credentials | ✓ SaaS Provisioning | Activation & Summary
Configure Credentials

For each credential shown here, configure the necessary settings.

Credential Requirement	
Digital Signature	Not Configured

18. On the Credentials screen, click **Configure Credentials**.

19. On the Digital Signature Settings screen, select a signing certificate for SAML assertions.

    For more information, see “Configuring Digital Signature Settings” in the “Identity Provider SSO Configuration” chapter of the PingFederate *Administrator’s Manual* (or click **Help**).

    If you have not yet created or imported a signing certificate, click **Manage Certificates** and do so now (see “Digital Signing and Decryption Keys & Certificates” in the “Security Management” chapter of the PingFederate *Administrator’s Manual*).

Note: For delegated-authentication connections, if you have not yet *exported* the public portion of the signing certificate, click **Manage Certificates** and do so now. You will need access to the public certificate during configuration of the loopback IdP connection (see the next section).

20. *If* this connection uses a delegated-authentication template *and* you have configured optional SP-initiated SLO, click **Next** and follow these steps:

    a. On the Signature Verification Settings screen, click **Manage Signature Verification Settings**.

    b. On the Trust Model screen, click **Next**.

    For information about this screen and others in this configuration sequence, see "Configuring Signature Verification Settings" in the "Identity Provider SSO Configuration" chapter of the PingFederate *Administrator's Manual* (or click **Help** on any of the screens).

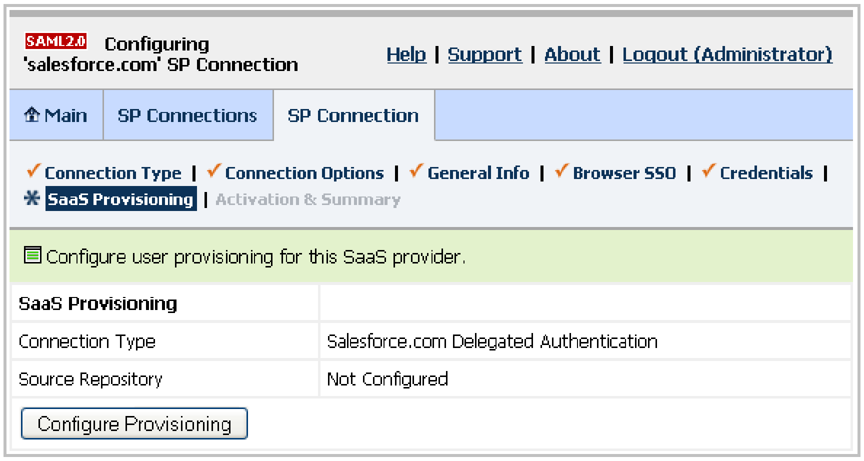
    c. On the Signature Verification Certificate screen, next to Primary, select the public certificate associated with the signing certificate you specified earlier for this SP connection (see Step 3).

> **Note:** To simplify this configuration, this step allows you to reuse the same signing certificate for the IdP connection later, since security is not an issue for this special-case, loopback scenario. Normally, you would choose an external partner's public certificate on this screen.

21. Click **Next** and then **Done** on the Summary screen.

22. Click **Done** and then **Next** on the Credentials screen.

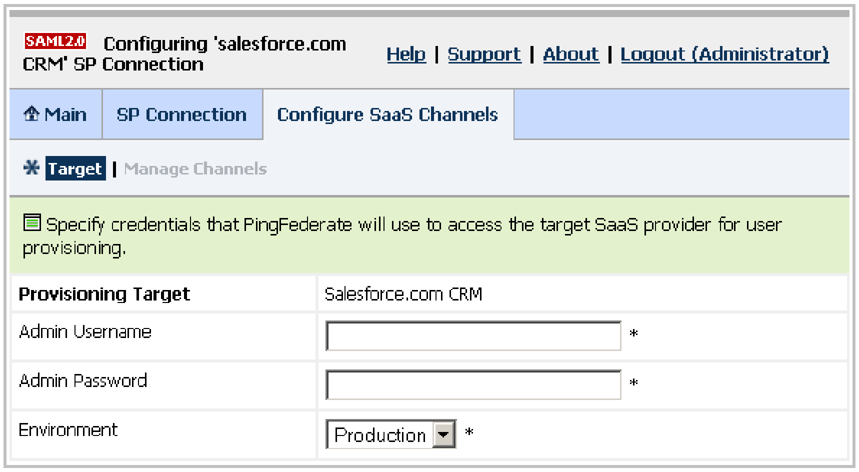
> **Note:** At this point, the SP connection for SSO to Salesforce is complete. If you are also configuring SaaS Provisioning for this connection, go to the next step. If you are not using provisioning for this connection, go to Step 26. (The screen below is not presented.)


SAML2.0
Configuring 'salesforce.com' SP Connection
Help | Support | About | Logout (Administrator)
Main
SP Connections
SP Connection
✓ Connection Type | ✓ Connection Options | ✓ General Info | ✓ Browser SSO | ✓ Credentials |
✱ SaaS Provisioning | Activation & Summary
Configure Provisioning

Configure user provisioning for this SaaS provider.

SaaS Provisioning	
Connection Type	Salesforce.com Delegated Authentication
Source Repository	Not Configured

23. On the SaaS Provisioning screen (if presented), click **Configure Provisioning**.



SAML2.0
Configuring 'salesforce.com CRM' SP Connection
Help | Support | About | Logout (Administrator)
Main
SP Connection
Configure SaaS Channels
Target | Manage Channels

Specify credentials that PingFederate will use to access the target SaaS provider for user provisioning.

Provisioning Target	Salesforce.com CRM
Admin Username	*
Admin Password	*
Environment	Production *

24. Enter the Admin Username and Admin Password for your Salesforce site and select an Environment.

Important: Ensure that the administrative user has API access enabled in Salesforce *and* that the password includes an appended security token when one has been issued from Salesforce. (For more information, see the Salesforce online documentation.)

25. Click **Next** to verify connectivity and then continue the provisioning configuration.

For information and instructions, see sections contained under “Configuring SaaS Provisioning” in the “Identity Provider SSO Configuration” chapter of the PingFederate *Administrator’s Manual*. (Or refer to the context-sensitive **Help** pages.)

Tip: If you are not ready to complete the provisioning configuration, you can click **Save Draft** and return to the configuration later (from the Manage Connections screen—click **Manage All SP** on the Main Menu).

Important: As part of the provisioning channel configuration for Salesforce CRM users, you must map the required Salesforce fields called “Role” and “Profile ID” to a user Profile enabled for SSO in the Salesforce administrative interface. All Salesforce users must be provisioned with an SSO-enabled Profile.

When configuring a provisioning channel for Salesforce Chatter Free users, the “Role” field must be left blank.

For instructions on enabling SSO for user profiles in Salesforce, see “Configuring Salesforce Accounts” on page 20.

When you return to the SaaS Provisioning screen, click **Next**.

26. On the Activation & Summary screen, click **Save**.

    For important information about using this screen, refer to the **Help** page or see "Connection Activation and Summary" in the "Identity Provider SSO Configuration" chapter of the PingFederate *Administrator's Manual*.

    Note: When you save the connection based on any of the delegated-authentication templates, a draft of a loopback IdP connection is created automatically for the SP Configuration (see "Using a Loopback Connection" on page 22). You must supply some site-specific information in this draft, including configuration of the PingFederate Salesforce SP Adapter, and then save the connection, as described in the next section.

    Important: If you decide to delete a delegated-authentication SP connection and start over for any reason, then you must also delete the loopback IdP connection from the Manage Connections screen for the SP Configuration (see Step 2 on page 32). (Click **Save** after deleting the connection.) Otherwise, repeating the Salesforce SP-connection setup causes an error.

27. *If* you are using the SAML 2.0 connection template for Salesforce CRM & Chatter, skip the next section: go to "SSO Linking to Salesforce" on page 35.

Configuring the IdP Connection

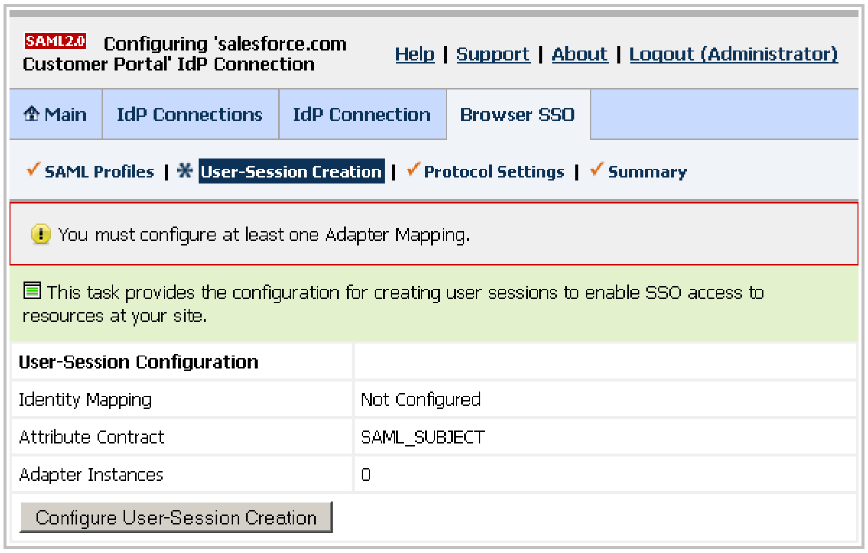
This configuration completes the PingFederate setup of a delegated-authentication SSO connection to Salesforce.

Note: This configuration *does not* apply if you are using the SAML 2.0 connection template for SSO to Salesforce CRM & Chatter.

To configure the IdP connection:

1. Ensure that you have created an instance of the PingFederate Salesforce SP Adapter (see “Salesforce Adapter Setup” on page 16).
2. On the Main Menu, under IdP Connections in the My SP Configuration section, click **Manage All IdP**.
3. On the Manage Connections screen, click the Draft salesforce.com connection under Connection Name.

   This draft was created by the template you chose for the SP connection, as indicated in the Connection Name.
4. On the General Info screen, click **Browser SSO** under the IdP Connection tab, or click **Next**.
5. On the Browser SSO screen, click **Configure Browser SSO**.


SAML2.0
Configuring 'salesforce.com Customer Portal' IdP Connection
Help | Support | About | Logout (Administrator)
Main
IdP Connections
IdP Connection
Browser SSO
✓ SAML Profiles | ✱ User-Session Creation | ✓ Protocol Settings | ✓ Summary

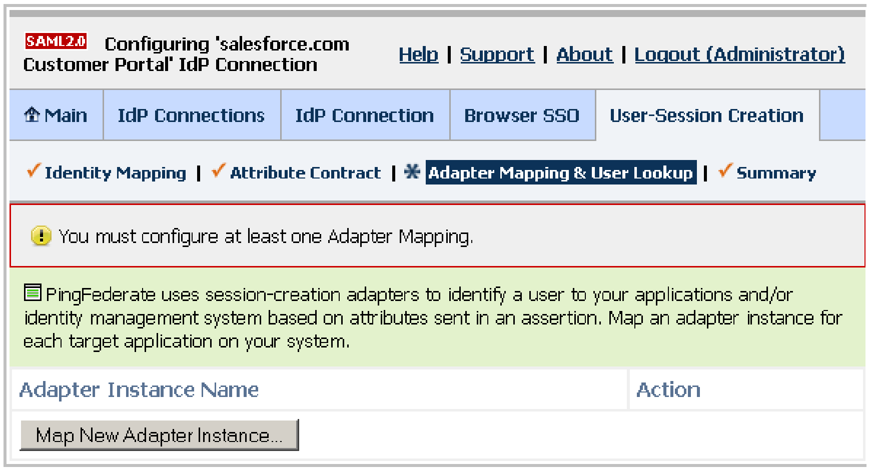
You must configure at least one Adapter Mapping.

This task provides the configuration for creating user sessions to enable SSO access to resources at your site.

User-Session Configuration	
Identity Mapping	Not Configured
Attribute Contract	SAML_SUBJECT
Adapter Instances	0

Configure User-Session Creation

6. On the User-Session Creation screen, click **Configure User-Session Creation**.



SAML2.0 Configuring 'salesforce.com Customer Portal' IdP Connection

Help | Support | About | Logout (Administrator)
Main | IdP Connections | IdP Connection | Browser SSO | User-Session Creation
✓ Identity Mapping | ✓ Attribute Contract | ✱ Adapter Mapping & User Lookup | ✓ Summary

You must configure at least one Adapter Mapping.

PingFederate uses session-creation adapters to identify a user to your applications and/or identity management system based on attributes sent in an assertion. Map an adapter instance for each target application on your system.

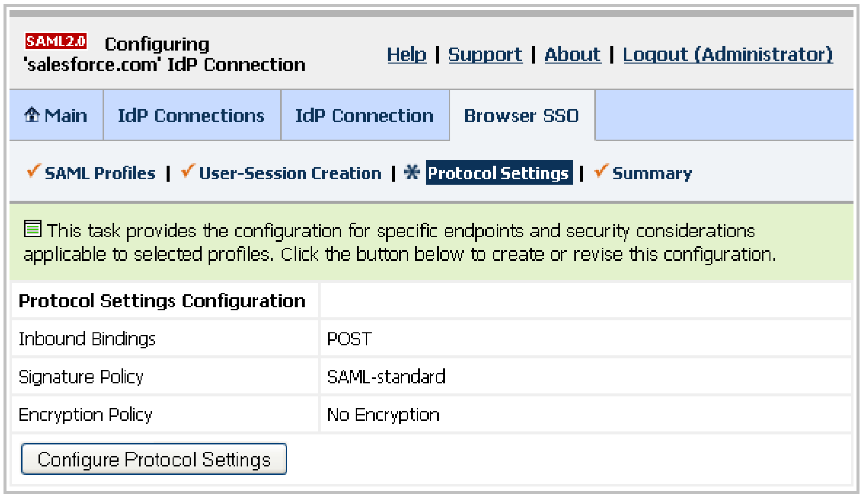
Adapter Instance Name	Action

7. On the Adapter Mapping & User Lookup screen, click **Map New Adapter Instance** and map the Salesforce SP Adapter Instance you defined earlier (see "Salesforce Adapter Setup" on page 16).

   This configuration is site-dependent and thus cannot be preconfigured. For detailed information and instructions, see "Configuring Adapter Mapping and User Lookup" in the "Service Provider SSO Configuration" chapter of the PingFederate *Administrator's Manual* (or refer to the **Help** pages).

   When you return to this screen, click **Done**.

8. When you return to the User-Session Creation screen, click **Next**.



SAML2.0 Configuring 'salesforce.com' IdP Connection

Help | Support | About | Logout (Administrator)
Main | IdP Connections | IdP Connection | Browser SSO
✓ SAML Profiles | ✓ User-Session Creation | ✱ Protocol Settings | ✓ Summary

This task provides the configuration for specific endpoints and security considerations applicable to selected profiles. Click the button below to create or revise this configuration.

Protocol Settings Configuration	
Inbound Bindings	POST
Signature Policy	SAML-standard
Encryption Policy	No Encryption

9. (Optional) If you require either SP-initiated SSO or SP-initiated SLO (for delegated-authentication connections), or both, click **SAML Profiles** under Browser SSO and follow these steps:

   a. On the SAML Profiles screen, select the checkbox(es) needed: SP-Initiated SSO and/or SP-Initiated SLO.

   b. Return to the **Protocol Settings** screen and click **Configure Protocol Settings**.

c. On the SSO Service URL screen (if presented), choose Post under Binding, enter `/idp/SSO.saml2` as the Endpoint URL, and then click **Add**.

d. Click **Next**.

e. On the SLO Service URLs screen (if presented), choose Redirect under Binding, enter `/idp/SLO.saml2` as the Endpoint URL, and then click **Add**.

f. Click **Next**.

g. On the Allowable SAML Bindings screen, clear the checkboxes Artifact and SOAP if selected (retain or select POST and Redirect).

h. Click **Done**.

10. On the Protocol Settings screen, click **Done**.

> **Tip:** Again, except for the optional settings described above, this task is completely configured for you, but click **Configure Protocol Settings** if you want to review the Salesforce connection settings. For configuration information, see sections under "Configuring Protocol Settings" in the "Identity Provider SSO Configuration" chapter of the PingFederate *Administrator's Manual* (or use the context-sensitive **Help**).

11. On the Browser SSO screen, click **Next**.

12. On the Credentials screen, click **Configure Credentials**.

13. If the Digital Signature Settings screen is presented (for optional SLO configuration), select the same signing certificate used for the SP Connection and click **Next**.

14. On the Signature Verification Settings screen, click **Manage Signature Verification Settings**.

15. On the Signature Verification Certificate screen, select the verification certificate for the connection.

    This is the exported public certificate specified during the Salesforce IdP configuration (see Step 19 on page 28). If you have not yet imported the certificate, click **Manage Certificates** and do so now.

    The Secondary certificate selection is not required.

    Click **Done**.

16. When you return to the Credentials screen, click **Next**.

17. On the Activation & Summary screen, click **Save**.

    For important information about using this screen, refer to the **Help** page or see "Connection Activation and Summary" in the "Service Provider SSO Configuration" chapter of the PingFederate *Administrator's Manual*.

SSO Linking to Salesforce

Once you have configured PingFederate to enable SSO, use the following URL for the link to Salesforce on your company portal:

```
https://<pf_host>:<pf_port>/idp/startSSO.ping?
   PartnerSpId=<Partner_Id>&<TargetResource>
```

where:

- `<pf_host>` is the fully qualified domain name of the server running PingFederate.
- `<pf_port>` is the SSL port for PingFederate.
- `<Partner_Id>` is the Connection ID for the SP connection specified in PingFederate.
- `<TargetResource>` is your organization's Salesforce URL where the user should be directed after successful SSO.

For delegated-authentication connections, add the following additional query parameter to ensure continuous proper functioning:

```
&SpSessionAuthnAdapterId=<Salesforce_Adapter_Id>
```

where:

`<Salesforce_Adapter_Id>` is the Adapter Instance Id entered during the PingFederate setup procedure.

Note: Do not use the adapter-ID parameter for CRM & Chatter connections based on the SAML 2.0 connection template.

Appendix A

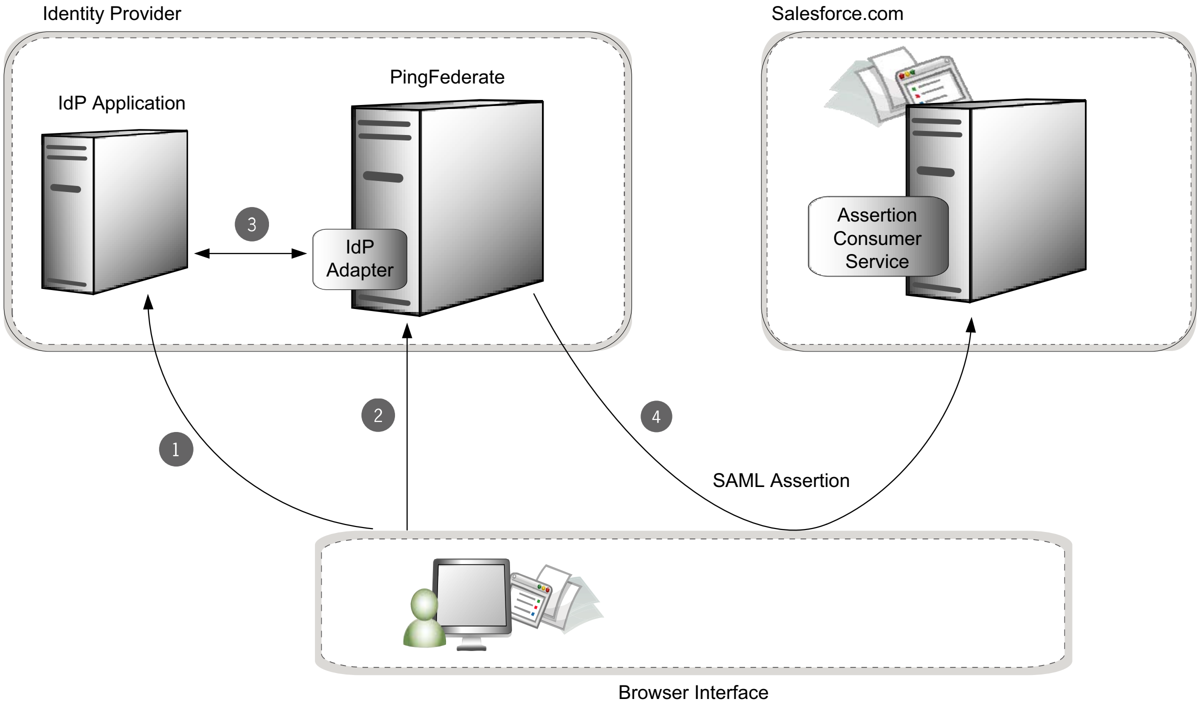
Process Diagrams

The following sections illustrate and describe step-by-step processing involved in the use cases for the Salesforce Connector:

- "IdP-Initiated SSO via SAML 2.0"
- "IdP-Initiated SSO via Delegated Authentication"
- "SP-Initiated SSO via Direct Logon"
- "SP-Initiated SSO via Deep Linking"
- "SP-Initiated IdP Logout (SLO)"
- "Outlook Access via the Rich-Client Proxy Service"

Note that in all cases HTTPS is used to secure the connection.

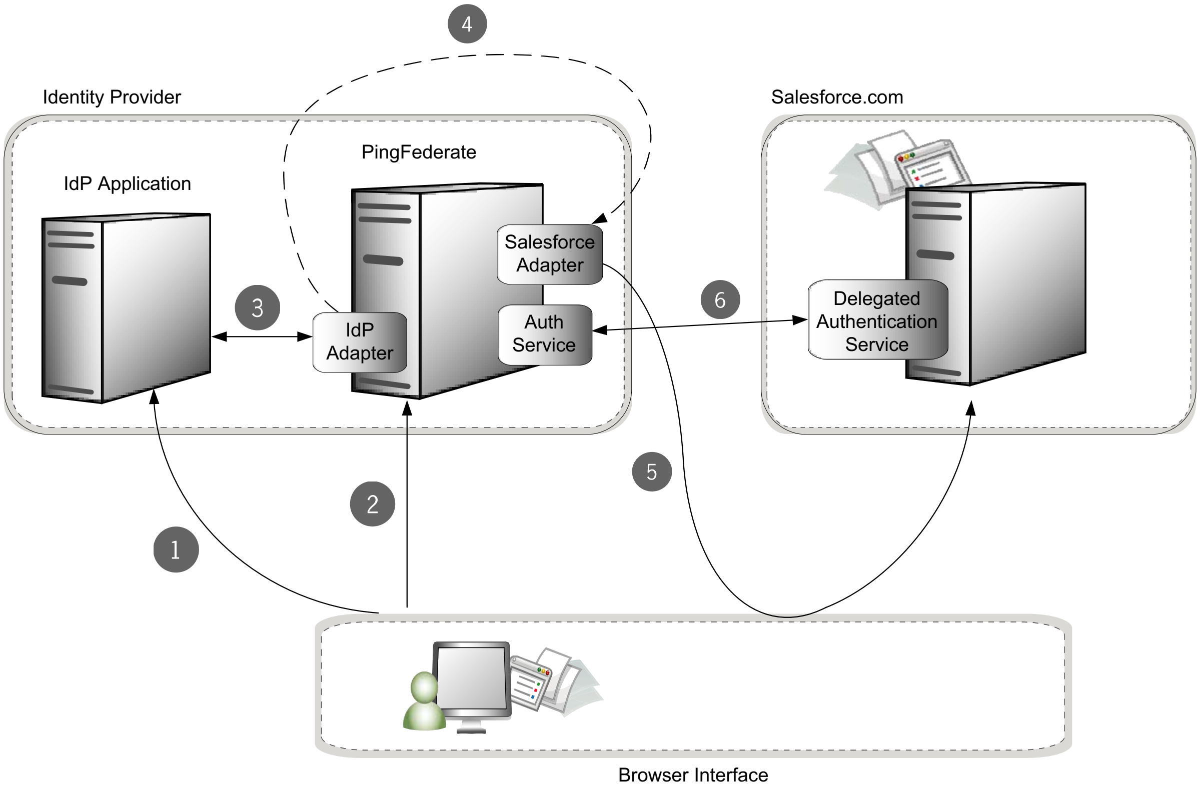
IdP-Initiated SSO via SAML 2.0



Processing Steps:

1. A user authenticates at the IdP.
2. The user initiates an SSO transaction to Salesforce CRM.
3. Login session information is retrieved by an IdP Adapter running in PingFederate. The IdP can be any authentication service, including an LDAP directory, an IdM system, or a custom application. See the Ping Identity Web site (www.pingidentity.com) for a full list of IdP Integration Kits available for PingFederate.
4. The IdP Adapter passes user attributes to PingFederate, which generates a SAML assertion and sends it to the Salesforce SSO processing site for SAML.

IdP-Initiated SSO via Delegated Authentication



Processing Steps:

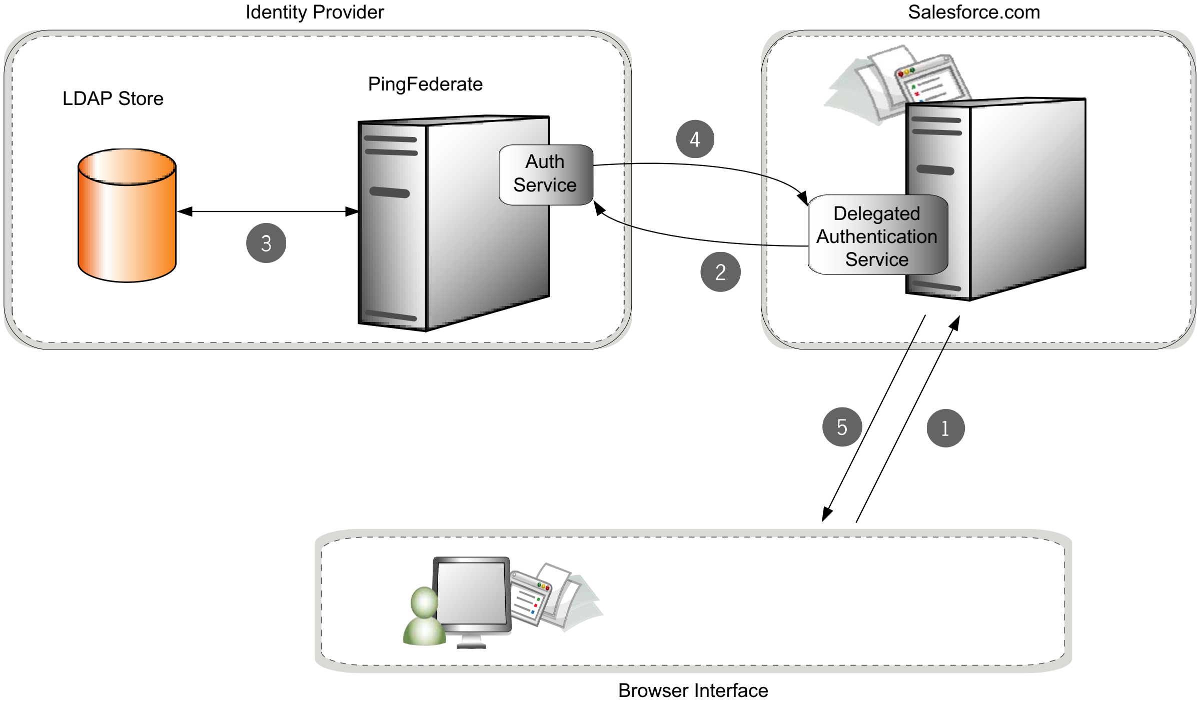
1. A user authenticates at the IdP.
2. The user initiates an SSO transaction to Salesforce.
3. Login session information is retrieved by an IdP Adapter running in PingFederate. The IdP can be any authentication service, including an LDAP directory, an IdM system, or a custom application. See the Downloads page on the Ping Identity Web site (www.pingidentity.com/support-and-downloads/) for a full list of IdP Integration Kits available for PingFederate.
4. The IdP adapter passes the user attributes to PingFederate. The PingFederate IdP server generates a SAML assertion and sends it to the PingFederate SP site.

   Note: In this deployment, with a single PingFederate instance serving in both the IdP and the SP roles, PingFederate performs a loopback, sending messages to and from itself. The SP serves as a proxy for Salesforce.

5. The PingFederate SP server parses the SAML assertion and passes the user attributes to the Salesforce Adapter. The Adapter generates an `OpenToken` as a password and redirects the browser to Salesforce, with the user ID and the `OpenToken` as credentials.

6. Salesforce validates the user ID and, if Web SSO is enabled for that user's profile, sends a SOAP request containing the ID and the `OpenToken` to the PingFederate Authentication Web Service. The Web Service validates the ID and `OpenToken` and sends a SOAP response back to Salesforce with `TRUE` or `FALSE`.
7. (Not Shown) If the response is `TRUE`, the user is logged on to Salesforce. If SLO or Deep Linking parameters were sent in the original request, Salesforce creates `logouturl` and/or `ssostartpage` cookies to hold these values.

SP-Initiated SSO via Direct Logon



Processing Steps:

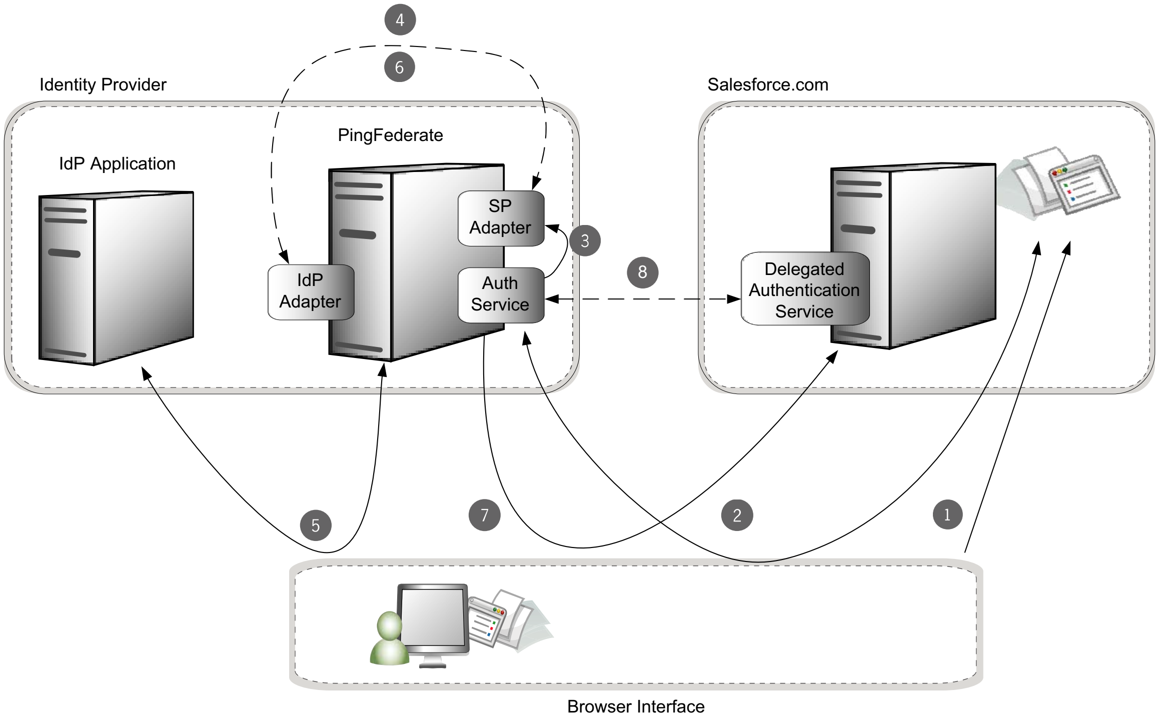
1. User goes to Salesforce and enters his or her corporate email and password, which are sent to Salesforce via a form POST.
2. Salesforce checks the user ID and sees that Web SSO is enabled for the Salesforce "Profile" for which the user is a member. Salesforce then sends a SOAP request containing the ID and the password over a TLS-secured channel to the PingFederate Salesforce Authentication Web Service.
3. The Authentication Web Service validates the email and password against an LDAP data store.
4. The Authentication Web Service sends a SOAP response back to Salesforce with `TRUE` or `FALSE`.

5. If the response is `TRUE`, the user is logged on to Salesforce.

Note: The Authentication Service in the diagram is deployed within PingFederate, but it may also be deployed in any Web container, such as Tomcat or Jetty.

SP-Initiated SSO via Deep Linking

Note: This illustration shows the deep-linking process flow for delegated authentication. The Connector also supports deep linking to Salesforce after initial IdP-initiated SSO via SAML 2.0. Processing diagrams and steps for standard SAML 2.0 are available in the "Supported Standards" chapter in *Getting Started*.



Processing Steps:

1. A user receives and clicks on a link to a page within Salesforce.
2. Salesforce sees that the user has performed IdP-initiated SSO before by reading the `ssostartpage` cookie and redirects the user to the URL in

the cookie, which is PingFederate's Authentication Web Service SSO endpoint.

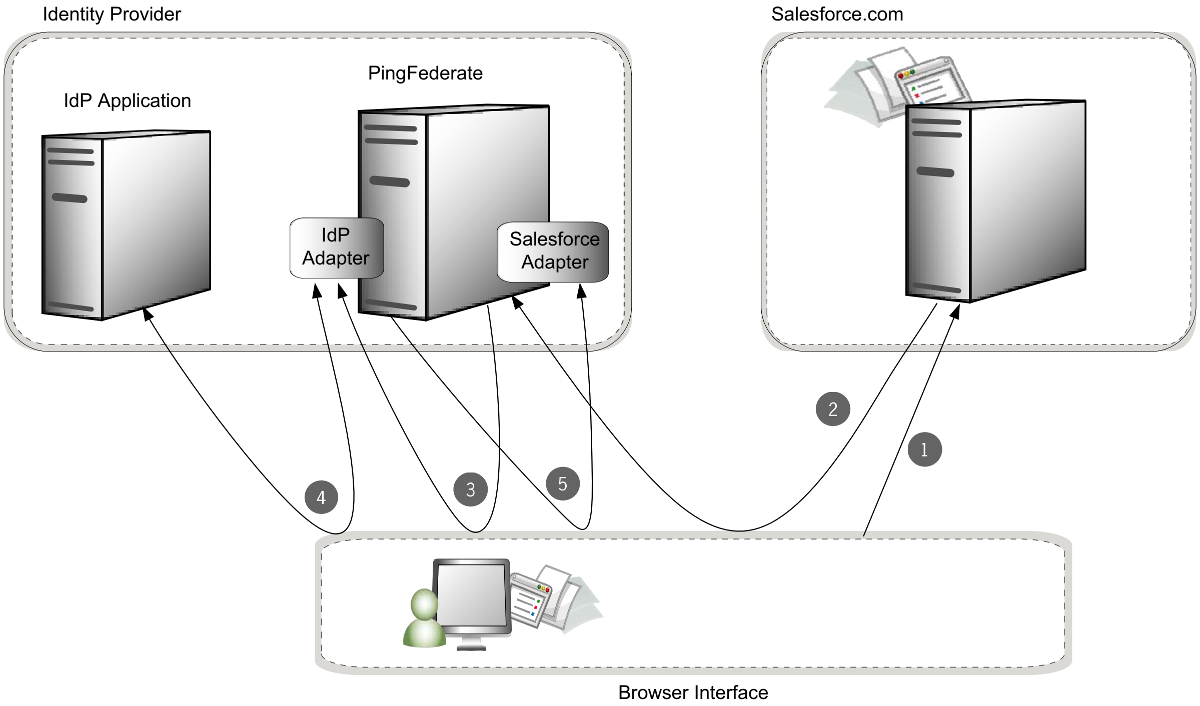
Note: For deep linking to work, IdP-initiated SSO via the Authentication Service must have been performed previously for that user. Salesforce redirects the user only when it finds the `ssostartpage` cookie, which is set only during IdP-initiated SSO via the Authentication Service.

3. The Authentication Web Service's SSO endpoint redirects the user to the SP Application endpoint with proper parameters.
4. PingFederate sends a SAML Authentication Request to itself through the user's browser.
5. The user is authenticated if necessary via a configured IdP adapter.
6. PingFederate sends a SAML Response to itself through the user's browser to the Salesforce Adapter.
7. The adapter generates an `OpenToken` and redirects the user to Salesforce with this secure token and a `startURL` parameter containing the deep link originally requested.
8. Salesforce validates the user ID and, if Web SSO is enabled, sends a SOAP request containing the ID and the `OpenToken` to the PingFederate Authentication Web Service. The Web Service validates the ID and `OpenToken` and sends a SOAP response back to Salesforce with `TRUE` or `FALSE`.
9. (Not Shown) If the result is `TRUE`, Salesforce creates a user session and redirects the user to the deep link originally requested.

Note: Deep linking works only for pages that are *inside* Salesforce; links to Salesforce logon pages are not redirected.

SP-Initiated IdP Logout (SLO)

Note: This illustration shows the single-logout process flow for delegated authentication. For a CRM & Chatter connection via SAML 2.0, the Connector also supports SP-initiated IdP logout via a redirect from Salesforce to an IdP-application logout URL, when specified (see "Using SAML 2.0" on page 20).



Processing Steps:

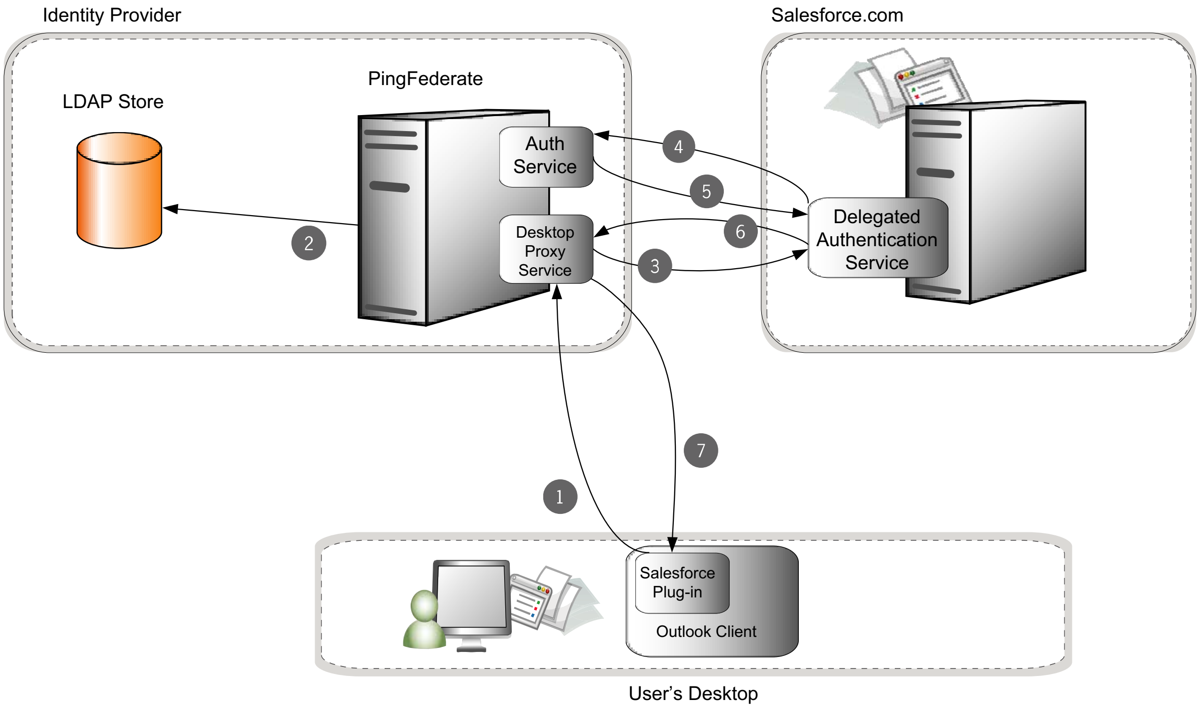
1. User is logged on to Salesforce and an external IdP application, and clicks the Logout link in Salesforce.
2. Salesforce terminates the user session and looks for an SLO cookie. If the cookie is found, it redirects the user to the PingFederate `/sp/startSLO.ping` endpoint.

   Note: For SLO to work, an IdP-initiated SSO via the Authentication Service must have been performed previously for that user. Salesforce redirects the user only when it finds the `logouturl` cookie, which is set only during IdP-initiated SSO via the Authentication Service.

3. PingFederate starts an SLO by sending a logout request to the IdP.
4. The PingFederate IdP server logs the user out via all configured adapters, as applicable, and returns a SAML response indicating success or failure. (For more information, see the “Application Endpoints” chapter in the PingFederate *Administrator’s Manual.*)
5. The user is redirected to the default SP SLO Success URL configured in PingFederate administrative console if the SLO was successful, or to an error template if not.

Outlook Access via the Rich-Client Proxy Service

Note: Deploying the proxy service is *not* required for using the Salesforce Outlook plug-in with PingFederate for SSO (see "Secondary Use Cases" on page 7).



Processing Steps:

1. The user accesses Salesforce via the Outlook plug-in configured with the user's corporate credentials. The Outlook plug-in sends a Web-service request to the PingFederate rich-client proxy service.
2. The proxy service validates the corporate credentials against an LDAP store.
3. If the credentials are valid, the proxy service generates an `OpenToken` as a password and sends a SOAP request to Salesforce, with the user ID and the `OpenToken` as credentials.
4. Salesforce validates the ID and, if Web SSO is enabled, sends a SOAP request containing the ID and the `OpenToken` to the PingFederate Authentication Web Service.
5. The Authentication Web Service validates the ID and `OpenToken`, and sends a SOAP response back to Salesforce with `TRUE` or `FALSE`.
6. If the response from the Authentication Web Service is `TRUE`, Salesforce sends a SOAP response back to the rich-client proxy service validating the user.
7. The proxy service forwards the SOAP response to the Salesforce Outlook plug-in.