PingFederate®

Cloud Identity Connector for Salesforce

Version 1.0

User Guide

PingIdentity®

PingFederate Cloud Identity Connector for Salesforce *Release Notes*
Version 1.0
November, 2010

Ping Identity Corporation
1099 18th Street, Suite 2950
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

Salesforce Cloud Identity Connector

This Cloud Identity Connector enables an enterprise to use its Salesforce environment, together with PingFederate, to enable secure Internet single sign-on (SSO) to online services. The included Salesforce Adapter allows users logged on to any enterprise Salesforce service to perform SSO using Salesforce as the Identity Provider (IdP).

User Guide

User Guide

Introduction

Introduction

This Cloud Identity Connector enables an enterprise to use its Salesforce environment, together with PingFederate, to enable secure Internet single sign-on (SSO) to online services. The included Salesforce Adapter allows users logged on to any enterprise Salesforce service to perform SSO using Salesforce as the Identity Provider (IdP).

Using the Connector, a Software-as-a-Service (SaaS) vendor, for example, can provide customers with direct SSO access to SaaS applications, when the users are already logged on to the organization's Salesforce Customer Portal.

Intended Audience

This document is intended for system administrators with experience in the configuration and maintenance of information-technology infrastructure. Knowledge of network administration and configuration is assumed, as well as some familiarity with PingFederate and Salesforce administrative management.

Additional Resources

Administrators may want to review SSO Integration Kits and Adapters in the PingFederate *Administrator's Manual*.

TIP
If you encounter any difficulties with configuration or deployment, please try searching the Ping Identity Customer Portal (www.pingidentity.com/support/customer-portal.cfm) under **Answers**.

Please consult Salesforce documentation if you encounter any difficulties in areas not directly associated with PingFederate or the Salesforce IdP Adapter.

ZIP Manifest

The distribution ZIP file for the Connector contains the following:

- /docs – contains this documentation:
  - Salesforce_Cloud_Identity_Connector_Qualification_Statement.pdf – testing and platform information
  - Salesforce_Cloud_Identity_Connector_User_Guide.pdf – this document
- /dist – contains libraries needed for the Adapter:
  - pf-salesforce-idp-adapter-1.0.jar – Salesforce Adapter JAR file
  - salesforce-partner-api-20.jar – Salesforce application programming interface (API)

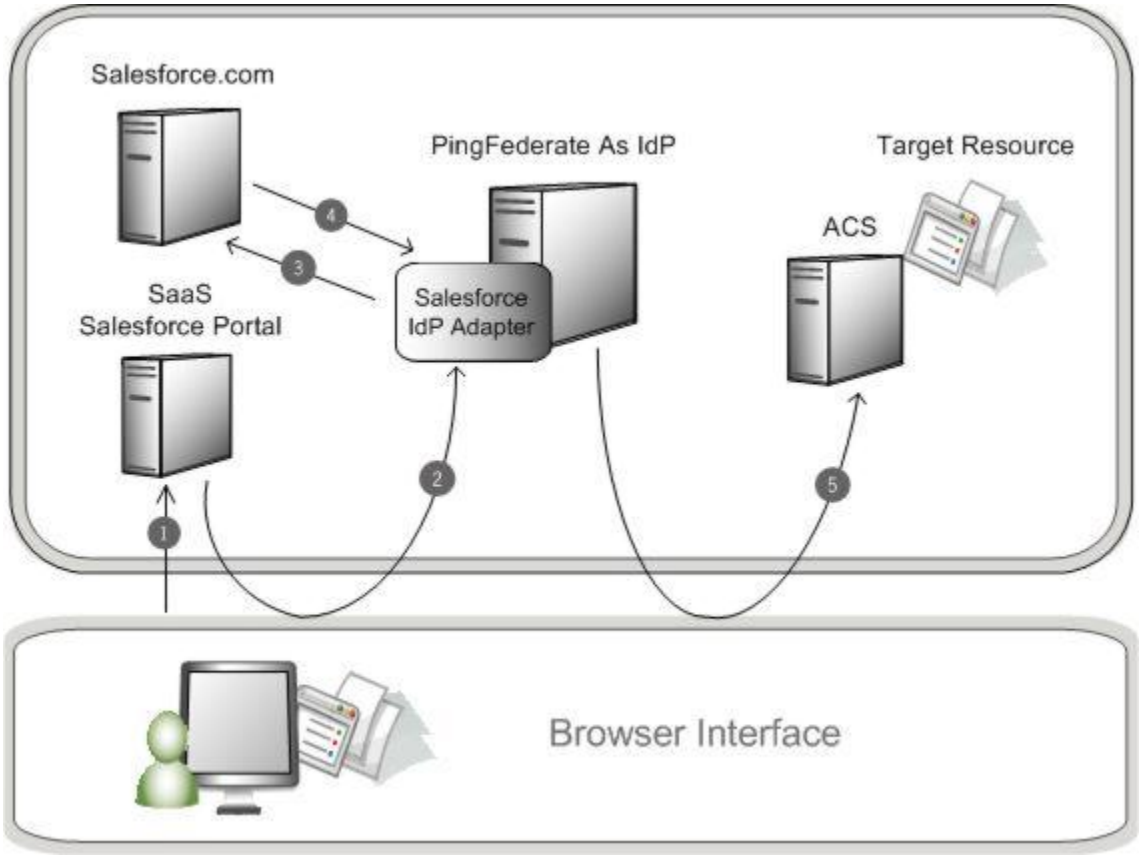
System Requirements

The Salesforce IdP Adapter requires installation of PingFederate 6.2 or higher.

Processing Overview

Processing Overview

The following diagram illustrates the SSO processing flow, using the Salesforce Cloud Identity Connector in a SaaS environment as an example implementation:



Processing Steps

1. On the enterprise Salesforce site, a user clicks a custom link for access to a protected resource.

   IMPORTANT
   The user must be logged on to Salesforce.

2. The link goes to PingFederate and includes the user's Salesforce session ID and service URL as query parameters.
   For more information, see Step 3 – Define the SSO URL in Salesforce.
3. The Salesforce IdP Adapter makes a SOAP (Simple Object Access Protocol) request to Salesforce to obtain attributes for the user.
4. Salesforce validates the session and returns requested user attributes in the SOAP response.
5. PingFederate issues a SAML (Security Assertion Markup Language) assertion to the SP-connection Assertion Consumer Service (ACS).

   NOTE
   Alternatively, for onsite target resources within the same security context as PingFederate, SSO can be accomplished via adapter-to-adapter mapping without using a SAML connection (see Complete the Configuration).

6. (Not shown) The user is logged on to the target resource.

Introduction Installation and Configuration

Installation and Configuration

Installation and Configuration

This section describes how to:

- Install the Salesforce Connector components
- Configure PingFederate
- Define the SSO launch URL in Salesforce

Processing Overview Step 1 -- Install the Salesforce Connector

Step 1 -- Install the Salesforce Connector

Step 1 -- Install the Salesforce Connector

1. From the distribution dist directory, copy the files:
   - pf-salesforce-idp-adapter-1.0.jar
   - salesforce-partner-api-20.jar
   into the directory:
   <pf_install>/pingfederate/server/default/deploy
2. If it exists, delete the file:
   salesforce-partner.jar
   from the directory:
   <pf_install>/pingfederate/server/default/lib
   This library is an older version of the Salesforce API and not compatible with the PingFederate Salesforce Connector.
3. Start or restart PingFederate.

Installation and Configuration Step 2 -- Configure PingFederate

Step 2 -- Configure PingFederate

Step 2 -- Configure PingFederate

Setting up PingFederate involves configuring an instance of the Salesforce IdP Adapter and then using the instance in a connection to an SP partner. Alternatively, for applications at your site in the same security domain, you can use direct IdP-to-SP Adapter Mapping, rather than an SP connection.

Step 1 -- Install the Salesforce Connector Configure the IdP Adapter

Configure the IdP Adapter

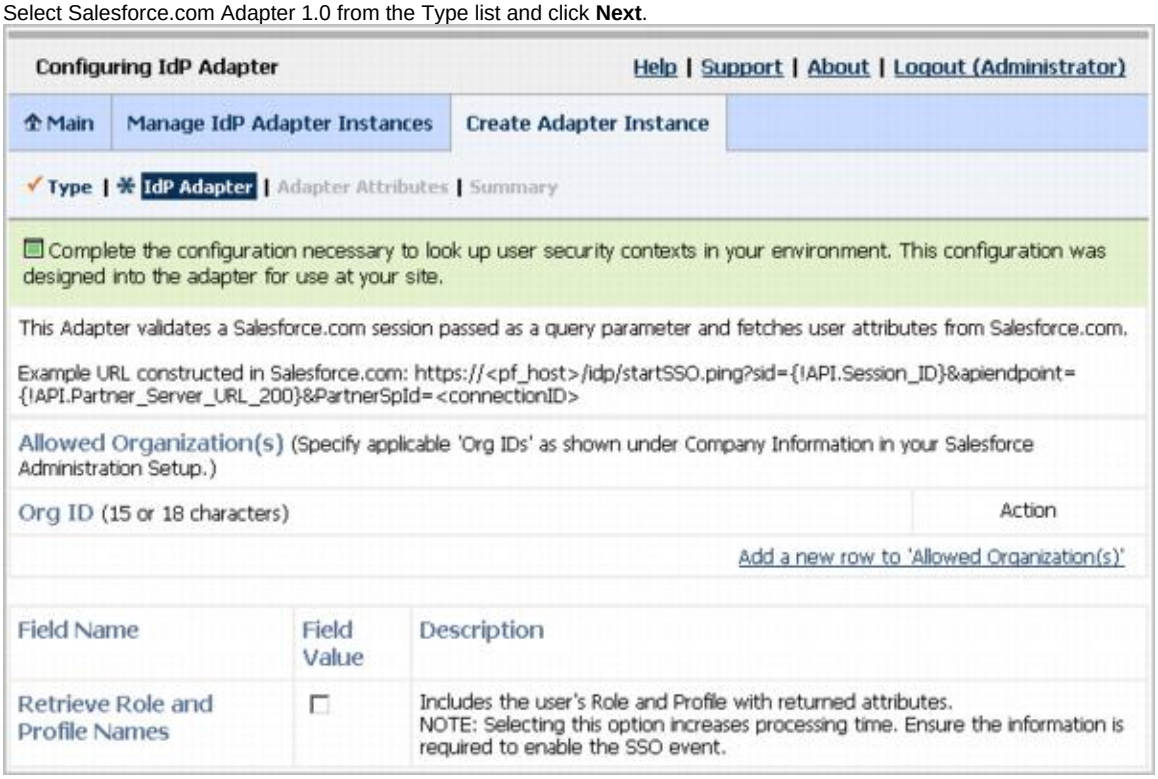
Configure the IdP Adapter

TIP
For this configuration, you need to know your Salesforce.com Organization ID (you can use more than one ID as needed). Organization IDs are listed under Company Information in your Salesforce Administration Setup.

1. Log on to the PingFederate administrative console and click **Adapters** under My IdP Configuration on the Main Menu.
2. On the Manage IdP Adapter Instances screen, click **Create New Instance**.
3. On the Type screen, enter an Instance Name and Instance Id.
   The Name is any you choose for identifying this Adapter Instance. The Id is used internally and must be alphanumeric without any spaces.

TIP
Make a note of the Adapter Id for later use.

4. Select Salesforce.com Adapter 1.0 from the Type list and click **Next**.



5. On the IdP Adapter screen, under Allowed Organization(s):
    a. Click **Add a new row to 'Allowed Organization(s)'**.
    b. Enter your Salesforce Org ID.
    c. Click **Update**.
    d. Repeat these steps for any other Salesforce IDs at your site, as needed.
6. (Optional) *If* SSO to a target application requires the user's organizational role and/or profile, select the associated checkbox. Note that this selection marginally increases processing time for the SSO transaction.
7. Click **Next.**
8. On the Adapter Attributes screen, select the checkbox next to subject under Pseudonym.
Pseudonyms are opaque subject identifiers used for SAML account linking and may not be applicable in the context of cloud-identity deployments. To ensure correct PingFederate performance under all circumstances, however, a selection is required. (For information about account linking, refer to the Key Concepts section in the PingFederate *Administrator's Manual*, or click **Help** on this screen.)
9. On the Summary screen, verify that the information is correct and click **Done**.
10. On the Manage IdP Adapter Instances screen, click **Save**.

Step 2 -- Configure PingFederate

Complete the Configuration

Complete the Configuration

Complete the Configuration

To complete the SSO setup from PingFederate to the target resource:

- For an external SP partner, configure an SP connection (see instructions under For SSO to an SP Partner, next).
- For SSO to an application at your site in the same security domain, a standard SAML connection is not necessary; instead you can use direct IdP-to-SP adapter mapping (see instructions under For SSO to an Onsite Application).

For SSO to an SP Partner

» Use the Salesforce IdP Adapter Instance (configured earlier) in an SP Connection.

You select the Adapter Instance during the IdP Adapter Mapping setup under Assertion Creation.

For more information, see Managing SP Connections in the PingFederate *Administrator's Manual*.

NOTE
Be sure to activate the connection on the Activation & Summary screen when you are ready to test the Connector deployment.

For SSO to an Onsite Application

1. On the Main Menu, click **Server Settings**.
2. On the Roles and Protocols screen in the Server Settings configuration, ensure that both the IdP *and* SP roles are enabled.

NOTE
The choice of protocol is not relevant for either role to implement the Salesforce Connector for onsite SSO, but a selection is required to enable a role.

NOTE
If updates are needed on the screen, be sure to click **Save**.

3. Configure an SP Adapter Instance, if one is not already configured or you want to use a new one.
   Click **Adapters** under SP Configuration on the Main Menu.
   Use any adapter type, including the OpenToken Adapter bundled with PingFederate (see Configuring SP Adapters in the PingFederate *Administrator's Manual*).
4. On the Main Menu under System Settings, click **IdP-to-SP Adapter Mapping** and follow the screen flow to complete this configuration.
   Select the Salesforce IdP Adapter Instance configured earlier as the Source instance and any SP Adapter Instance as the Target.
   For more information, see IdP-to-SP Adapter Mapping in the PingFederate *Administrator's Manual* (or click **Help** on any screen).
5. (Optional) On the Main Menu under SP Configuration, click **Default URLs**.
   If the default SSO URL (the top text box) is unspecified *and* the SP configuration will be used *only* to set up this Salesforce Connector, you can enter the target-application URL as the default.

NOTE
The default URL for single logout (the second text box) does not apply for the Salesforce Connector; SLO is not supported.

   Alternatively, you can enter a fallback URL (or leave an existing entry unchanged) and provide the target-application URL as a query parameter in the Salesforce link, as described in the next section (recommended).
   For more information about how default URLs are used, see Configuring Default URLs in the PingFederate *Administrator's Manual* or click **Help**.

Configure the IdP Adapter

Step 3 -- Define the SSO URL in Salesforce

Step 3 -- Define the SSO URL in Salesforce

Step 3 -- Define the SSO URL in Salesforce

In your Salesforce administrative Web interface, add a link to initiate SSO where needed for your Salesforce deployment. Commonly, you would add as Custom Link as described in this section. The content of the link depends on the PingFederate configuration.

TIP
Salesforce navigational details and identification of screens and selections in these steps are subject to change, and only configuration options directly relevant to the PingFederate Connector are described. Some configuration steps are summarized, and different configurations may be possible. Please consult Salesforce documentation for complete, up-to-date information as needed.

To add an SSO link in Salesforce (example):

1. In the administrative App Setup, select **Customize | Home | Custom Links**.
2. On the Edit Home Custom Link page, click **New** and enter identifying and descriptive information.
3. For Content Source, select URL.
4. In the large text box area, enter one of the following URLs:
   For SSO via an SP-partner connection in PingFederate:
   ```
   https://<pf_host>:<pf_port>/idp/startSSO.ping?
   sid={!API.Session_ID}&apiendpoint={!API.Partner_Server_URL_200}&
   TargetResource=<destination_URL>&
   PartnerSpId=<connection_ID>
   ```
   where:
   - <pf_host> is the host name or IP address of the machine running PingFederate.
   - <pf_port> is the PingFederate port number.
   - <destination_URL> is the fully qualified URL of the target application or other protected resource.
   - <connection_ID> is the SAML entity ID for the SP connection configured earlier (located on the General Info screen for the PingFederate SP connection).

     For SSO via IdP-to-SP adapter mapping in PingFederate:
     ```
     https://<pf_host>:<pf_port>/pf/adapter2adapter.ping?
     sid={!API.Session_ID}&apiendpoint={!API.Partner_Server_URL_200}&
     TargetResource=<destination_URL>&
     IdpAdapterId=<adapter_ID>
     ```
     where:
   - <pf_host> is the host name or IP address of the machine running PingFederate.
   - <pf_port> is the PingFederate port number.
   - <destination_URL> is the fully qualified URL of the target application or other protected resource.
   - <adapter_ID> is the Adapter Id for the Salesforce IdP Adapter Instance configured earlier in PingFederate.
5. **Save** the link configuration in Salesforce.
6. In the Salesforce App Setup, select **Customize | Home | Home Page Components**.
7. Add a new link component using the Custom Link created in the previous steps.
8. In the Salesforce App Setup, select **Customize | Home | Home Page Layout**.
9. Edit the required layout(s), or create a new layout, to include the new link component.
10. Ensure that the user Profile is configured to use the Page Layout.

Complete the Configuration