PingFederate®

Internet Information Services (IIS) Integration Kit

Version 3.2

User Guide

Ping Identity®

PingFederate Internet Information Services (IIS) *User Guide*
Version 3.2
June, 2014

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: http://www.pingidentity.com

Trademarks

Disclaimer

The information provided in this document is provided "as is" without warranty of any kind. Ping Identity disclaims all warranties, either expressed or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Ping Identity or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Ping Identity or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

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 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: **June 18, 2014**

Contents

Introduction

The PingFederate Internet Information Services (IIS) Integration Kit adds a Service Provider (SP) application-integration option to PingFederate. The kit includes an IIS Agent that works in conjunction with the PingFederate OpenToken Adapter to allow an SP enterprise to accept SAML assertions and provide single sign-on (SSO) to IIS Web applications. The assertions may be sent using the SAML protocol (version 2.0 or 1.x) or the WS-Federation passive-requestor protocol (see Supported Standards in *Getting Started*).

Intended Audience

This document is intended for system administrators with experience in the configuration and maintenance of Windows and IIS servers. Knowledge of networking and user-management configuration is assumed at certain points in this document. Please consult documentation provided with your server tools if you encounter any difficulties in areas not directly associated with the PingFederate or integration-kit setups.

System Requirements

The following software must be installed in order to implement the IIS Integration Kit:

- PingFederate 6.x (or higher)
- IIS 7.0 or higher using Integrated Mode
- ASP .NET application must use .NET Framework 4.0

ZIP Manifest

The distribution ZIP file for the IIS Integration Kit contains the following:

- `ReadMeFirst.pdf` – contains links to this online documentation
- `/legal` – contains this document:
    - `Legal.pdf` – copyright and license information
- `/dist` – contains the following libraries and supporting files that are needed to install and run the adapter and agent:
    - `opentoken-adapter-2.5.1.jar` – the OpenToken Adapter JAR file
    - `/x64` – installation directory for 64-bit Windows architecture

      – `setup.exe` – Installation program for the PingFederate IIS Agent

      – `Support Files.msi` – Installation supporting files for the PingFederate IIS Agent

      – `/conf` – Contains configuration files

      – `/Module Retargetable Folder` – Contains IIS agent configuration data and a sample application

      – `/Global Assembly Cache Folder` – IIS agent DLLs

- `/x86` – agent installation directory for 32-bit Windows architecture:

  – `setup.exe` – Installation program for the PingFederate IIS Agent

  – `Supporting Files.msi` – Installation supporting files for the PingFederate IIS Agent

  – `/conf` – Contains configuration files

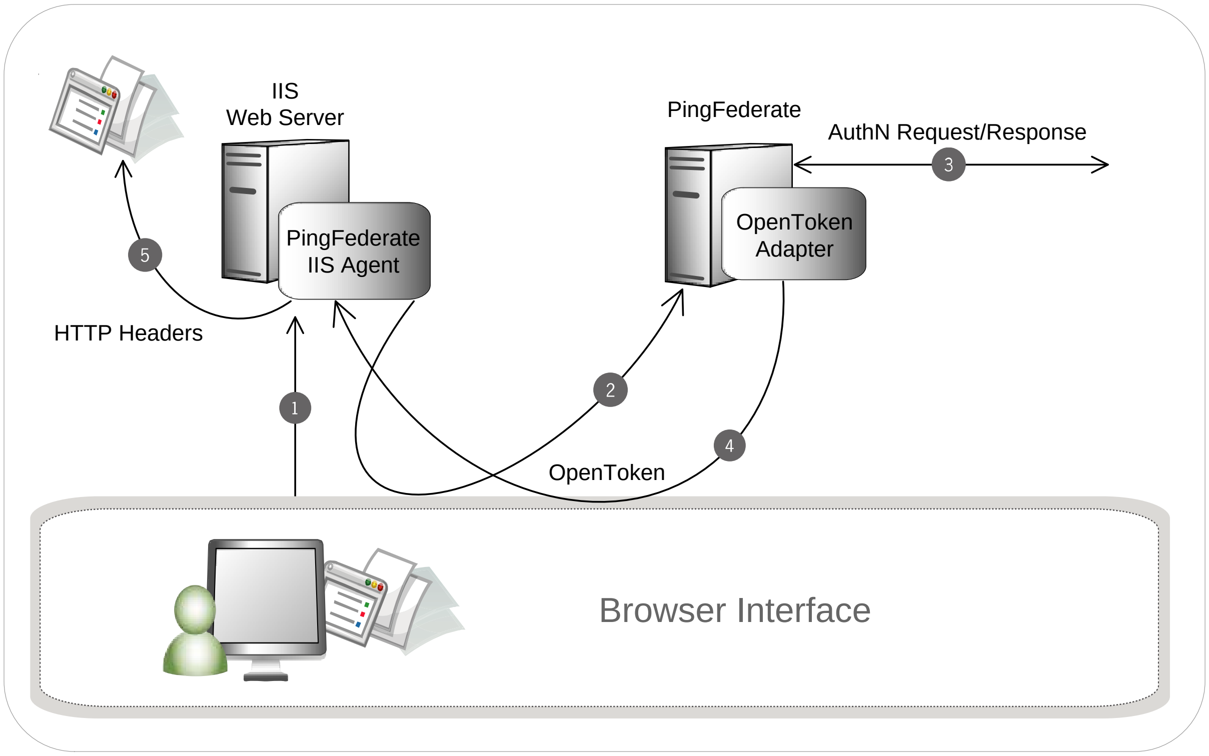
  – `/Module Retargetable Folder` – Contains IIS agent configuration data and a sample application

  – `/Global Assembly Cache Folder` – Contains IIS agent DLLs

Processing Overview

The IIS Agent acts as a filter in front of an application (or any external protected resource). The basic responsibilities of the Agent are to filter requests to determine whether a request is for a protected resource:

- If the request is for an unprotected resource, the Agent passes the request to the application.
- If the request is for a protected resource, the Agent checks to see if there is a PingFederate session available and if it meets the policy for the session.
- If a session exists and the session meets the policy for the request, then the Agent passes the request back to the application.
- If a session does not exist, or if the existing session does not meet the session policy for that request, the Agent redirects the user's browser through the PingFederate server to an Identity Provider (IdP) for authentication. After authentication, PingFederate redirects the user back to the protected resource with a valid session.



The figure above illustrates an SP-initiated SSO scenario, showing the request flow and how the PingFederate OpenToken Adapter wraps attributes from an assertion into a secure token (`OpenToken`) and passes the token to IIS.

Processing Steps

1. A user attempts to access a resource on the IIS server protected by the PingFederate IIS Agent.
2. The user is redirected to the PingFederate server for authentication.
3. (If an `OpenToken` session already exists, the user is granted immediate access.)
4. The PingFederate server redirects the user's browser to an IdP for authentication using either the SAML or WS-Federation protocols. The IdP partner authenticates the user and returns a SAML assertion.
5. PingFederate validates the assertion and creates an `OpenToken` for the user including any configured attributes. PingFederate then redirects the browser, including the `OpenToken`, back to the IIS Agent's OpenToken Exchange service, which converts the `OpenToken` into a cookie, and redirects to the original resource.
6. The IIS Agent verifies the `OpenToken` and grants access to the protected resource. The User ID and any attributes from the `OpenToken` are exposed to the resource as HTTP Request Headers.

Installation and Setup

The following sections describe how to install and configure the OpenToken Adapter for an SP as well as deploy the IIS agent.

Installing the OpenToken Adapter and Configuring PingFederate

Note: If you have already deployed version 2.5.1 (or higher) of the OpenToken Adapter, skip steps 1 through 4 in the following procedure.

1. Stop the PingFederate server if it is running.
2. Remove any existing OpenToken Adapter files (`opentoken*.jar`) from the directory:

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

   The adapter JAR file is `open-token-adapter-<version>.jar`.
3. Unzip the integration-kit distribution file and copy `opentoken-adapter-2.5.1.jar` from the `/dist` directory to the PingFederate directory:

   `<PF_install>/pingfederate/server/default/deploy`
4. Start or restart PingFederate.
5. Configure an instance of the OpenToken Adapter for your SP configuration using settings on the Instance Configuration screen as indicated in the table below.

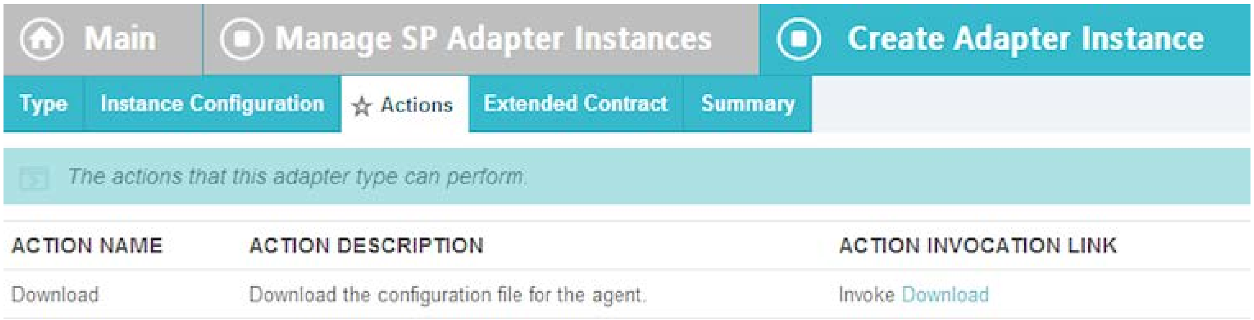
   For detailed instructions, see OpenToken Adapter Configuration in the PingFederate *Administrator's Manual.*)

Option	Description
Password	Enter any password you choose.
Confirm Password	Password confirmation.

Note: In the Advanced Fields section, when populating the Authentication Service field, use either an `HTTP` or `HTTPS` value Best practices include setting the Authentication Service field to a protected resource hosted by your IIS server.

6. On the Actions screen, click the **Download** link and then click **Export** to save the properties file to any directory on the machine running IIS.

   You will move this file later when you set up the PingFederate IIS Agent.



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

7. On the Extended Contract screen, enter any attributes you want to pass to the application as HTTP request headers.
8. Configure or modify the connection(s) to your IdP partner(s), using the instance of the OpenToken Adapter you configured in the last steps.

   For more information, see Identity Provider SSO Configuration in the PingFederate *Administrator's Manual*.

Installing and Configuring the PingFederate IIS Agent for IIS 7

Note: If this is a first-time installation of the IIS Integration Kit, proceed directly to step 3 in the following procedure.

If you are upgrading this integration, we strongly recommend reinstalling the OpenToken IIS Agent in IIS.

1. If you are upgrading this integration:
   a. Temporarily stop your IIS if it is running.
   b. Open the IIS manager console and open the **Modules** view for the server hosting the previous version of the OpenToken module.
   c. Select the old version of the OpenToken module and select **Remove**.
   d. Using the Windows Control Panel, remove the existing OpenToken IIS agent (`OpenToken HTTP Module`) from the IIS server.
2. Restart IIS for changes to take effect.
3. Unzip the IIS Integration Kit distribution file into a directory on the IIS machine.
4. From the integration-kit `/dist/(x86 or x64)/` directory , run `setup.exe` and follow the setup screens.

   Note: The setup installs the supporting components and installs the OpenToken HTTP Module into the Windows global Assembly Cache, which requires an internet connection to complete the installation. Using the `Support Files.msi` in place of `setup.exe` will install the OpenToken HTTP Module without requiring an internet connection, but requires the prerequisite software.

5. Register the .NET Framework 4.0 by entering the following command:

   ```
   <Windows>\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis -iru
   ```

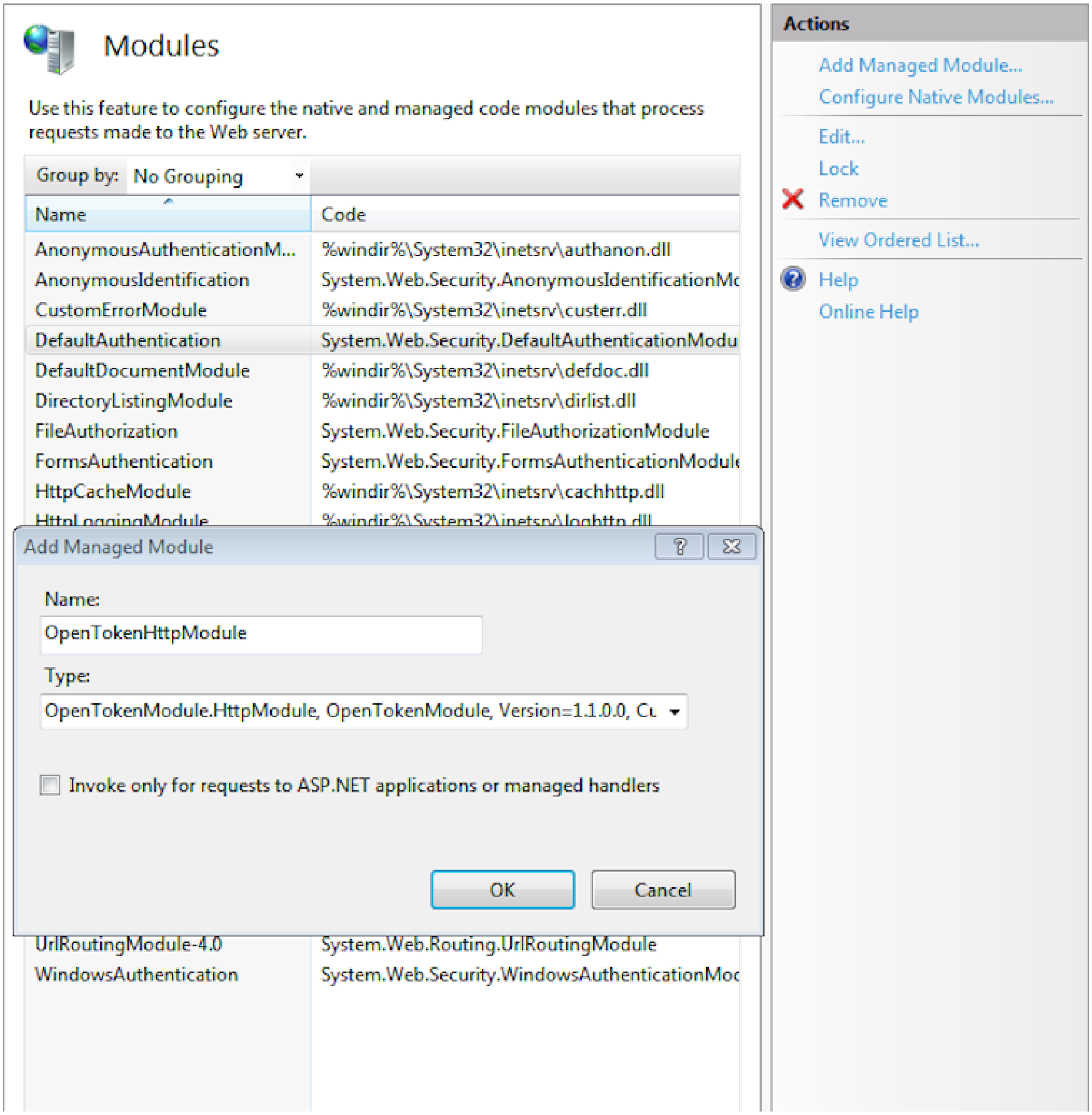
   where `<Windows>` is the location of the operating system files.
6. Move the `agent-config.txt` exported during the Adapter setup into the `\conf` directory created by the installer. By default, this directory is located in:

   ```
   C:\Program Files\Ping Identity Corporation\OpenToken IIS Agent (n-bit)\
   ```

   where *n* is either `32` or `64`, depending on your architecture.

7. Follow the steps below to add the OpenToken HTTP Module into IIS:
   a. Open the IIS Manager console.
   b. Select the server hosting IIS.
   c. Open Features View and select **Modules**.
   d. On the Configuration screen under Modules, click Add Managed Module to locate and add the OpenToken HTTP Module into IIS.
   e. Add a managed module and name it OpenTokenHttpModule.
   f. Select **OpenTokenModule.HttpModule** from the Type list and click **OK**.

Note: Refer to IIS product specific documentation for detailed information on how to add managed modules.



Use this feature to configure the native and managed code modules that process requests made to the Web server.

Group by: No Grouping

Name	Code
AnonymousAuthenticationM...	%windir%\System32\inetsrv\authanon.dll
AnonymousIdentification	System.Web.Security.AnonymousIdentificationMc
CustomErrorModule	%windir%\System32\inetsrv\custerr.dll
DefaultAuthentication	System.Web.Security.DefaultAuthenticationModu
DefaultDocumentModule	%windir%\System32\inetsrv\defdoc.dll
DirectoryListingModule	%windir%\System32\inetsrv\dirlist.dll
FileAuthorization	System.Web.Security.FileAuthorizationModule
FormsAuthentication	System.Web.Security.FormsAuthenticationModule
HttpCacheModule	%windir%\System32\inetsrv\cachhttp.dll
HttpLoggingModule	%windir%\System32\inetsrv\loghttp.dll
UrlRoutingModule-4.0	System.Web.Routing.UrlRoutingModule
WindowsAuthentication	System.Web.Security.WindowsAuthenticationMoc

Add Managed Module

Name:
OpenTokenHttpModule

Type:
OpenTokenModule.HttpModule, OpenTokenModule, Version=1.1.0.0, Cu

☐ Invoke only for requests to ASP.NET applications or managed handlers

8. Configure the properties file for IIS:

   The file `pfisapi.conf` is located at `C:\Program Files\Ping Identity Corporation\OpenToken IIS Agent (`*`n`*`-bit)\conf\`. Refer to comments in the file for information and configure the required properties.

Note: You can test the IIS kit configuration by deploying the sample application (`PFIsapiSample`) that is included in the installation located at `C:\Program Files\Ping Identity Corporation\OpenToken IIS Agent (n-bit)\samples`.

---

9. Restart IIS for changes to `pfisapi.conf` to take effect.

Installing and Configuring the PingFederate IIS Agent for IIS 8

Note: If this is a first-time installation of the IIS Integration Kit, proceed directly to step 3 in the following procedure.

If you are upgrading this integration, we strongly recommend reinstalling the OpenToken IIS Agent in IIS.

1. If you are upgrading this integration:
    a. Temporarily stop your IIS if it is running.
    b. Open the IIS manager console and open the **Modules** view for the server hosting the previous version of the OpenToken module.
    c. Select the old version of the OpenToken module and click **Remove**.
    d. Using the Windows Control Panel, remove the existing OpenToken IIS agent (`OpenToken HTTP Module`) from the IIS server.
2. Restart IIS for changes to take effect.
3. Open the Server Manager and click Add roles and features.
4. On the Installation Type tab, select Role-based or feature-based installation radio button and click Next.
5. On the **Server Selection** tab, select the destination server hosting IIS8 and click **Next**.
6. On the **Server Roles** page, expand the **Web Server (IIS)** list item. Expand the **Web Server** sub-item and the **Application Development** item beneath it. Select **.NET 3.5 Extensibility** and **.NET 4.5 Extensibility** before clicking **Next**. (*Note: enabling this feature may open a window asking to enable other features. Accept the changes the window suggests and continue.*)
7. On the **Features** tab, click **Next**.
8. On the **Confirmation** tab, ensure the installation features are correct and click **Install**. This step may take several minutes.
9. Once the installation is complete, click **Close**.
10. Unzip the IIS Integration Kit distribution file into a directory on the IIS machine.
11. From the integration-kit `/dist/x64/` directory , run `setup.exe` and follow the setup screens.

    Note: The setup installs the supporting components and installs the OpenToken HTTP Module into the Windows global Assembly Cache, which requires an internet connection to complete the installation. Using the `Support Files.msi` in place of `setup.exe` will install the OpenToken HTTP Module without requiring an internet connection, but requires the prerequisite software.

12. Move the `agent-config.txt` exported during the Adapter setup into the `\conf` directory created by the installer. By default, this directory is located in:

    `C:\Program Files\Ping Identity Corporation\OpenToken IIS Agent (`*`n`*`-bit)\`

13. Follow the steps below to add the OpenToken HTTP Module into IIS:

    a. Open the IIS Manager console.

    b. Select the server hosting IIS.

    c. Open Features View and select **Modules**.

    d. On the Configuration screen under Modules, click Add Managed Module to locate and add the OpenToken HTTP Module into IIS.

    e. Add a managed module and name it OpenTokenHttpModule.

    f. Select **OpenTokenModule.HttpModule** from the Type list and click **OK**.

Note: Refer to IIS product specific documentation for detailed information on how to add managed modules.

14. Configure the properties file for IIS:

    The file `pfisapi.conf` is located at `C:\Program Files\Ping Identity Corporation\OpenToken IIS Agent (`*n*`-bit)\conf\`. Refer to comments in the file for information and configure the required properties.

Note: You can test the IIS kit configuration by deploying the sample application (`PFIsapiSample`) that is included in the installation located at `C:\Program Files\Ping Identity Corporation\OpenToken IIS Agent (n-bit)\samples`.

15. Restart IIS for changes to `pfisapi.conf` to take effect.

IIS Agent Session Information

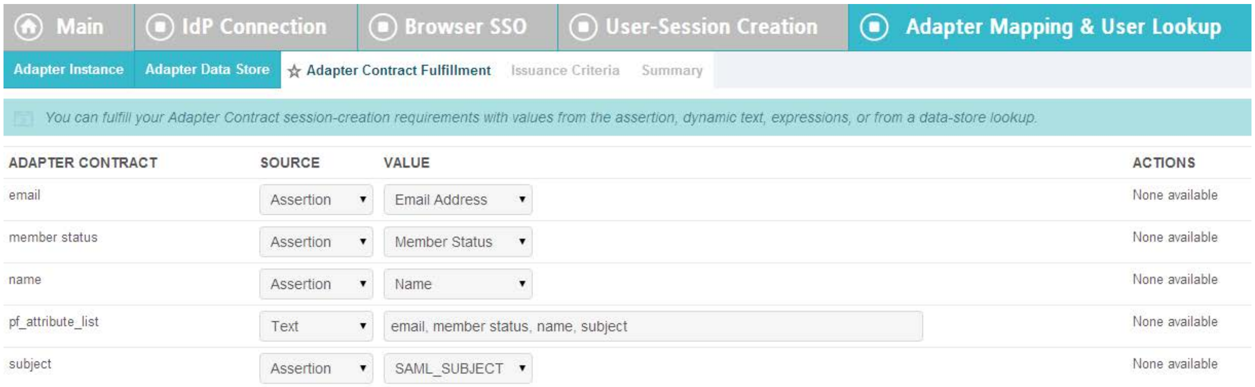
The PingFederate IIS Agent exposes session information and user attributes from the adapter to the protected application via HTTP request headers. This information can then be used by the application for authorization decisions, for example, or for generation of content specific to the user making the request.

The session and attribute information exposed to the application includes the following:

- Attributes from the OpenToken Adapter contract – These include, by default, the subject (`SUBJECT`) and attributes specified on the Extended Contract screen of the adapter setup. Only the attributes fulfilled at runtime are exposed to the application; attributes with a NULL value are not included in the OpenToken.
- `NOT-ON-OR-AFTER` – The time until inactivity timeout is reached.
- `RENEW-UNTIL` – The time until overall session timeout is reached.
- `AUTH_NOT-BEFORE` – The time when the session was created.
- `AUTHNCONTEXT` – Information from the SAML assertion that describes how the user was authenticated at the IdP. (For more information, locate Authentication Context in the PingFederate *Getting Started* manual.)

For security reasons, each HTTP request header is first pre-pended with a specific (configurable) prefix. The IIS Agent will always remove and rewrite these prefixed request headers for each request.

If applications protected by the IIS Agent cannot be modified to accept headers with this prefix, the IIS Agent can be configured not to add a prefix to the HTTP headers. In this case, on the Extended Contract screen in the OpenToken Adapter configuration, include an attribute named `pf_attribute_list`. Then map that attribute in your IdP Connection as a Text field containing a comma-separated list of all the attributes in the adapter contract (see figure below). This attribute list is sent in the `OpenToken` and used by the IIS Agent to overwrite headers in the request.



You can fulfill your Adapter Contract session-creation requirements with values from the assertion, dynamic text, expressions, or from a data-store lookup.

ADAPTER CONTRACT	SOURCE	VALUE	ACTIONS
email	Assertion	Email Address	None available
member status	Assertion	Member Status	None available
name	Assertion	Name	None available
pf_attribute_list	Text	email, member status, name, subject	None available
subject	Assertion	SAML_SUBJECT	None available

For more information, see Configuring Adapter Contract Fulfillment in the PingFederate *Administrator's Manual*.