PingFederate®

Internet Information Services Integration Kit

Version 2.4

User Guide

Ping Identity®

PingFederate Internet Information Services *User Guide*
Version 2.4
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: www.pingidentity.com

Trademarks

Disclaimer

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 prerequisites must exist in order to implement the IIS Integration Kit:

- PingFederate 5.x (or higher)

  See Installing the OpenToken Adapter and Configuring PingFederate on page 7 for more information.

- IIS 6.x
- ASP .NET application must use .NET Framework 2.0

ZIP Manifest

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

- `ReleaseNotes.pdf` – contains updates on the latest release.
- `/docs` – documentation:
  - `IIS_Integration_Kit_User_Guide.pdf` – this document
  - `IIS_Integration_Kit_Qualification_Statement.pdf` – testing information and known issues
  - `Legal.pdf` – licensing and other information
- `/dist` – libraries and supporting files needed to install and run the adapter and agent:
  - `opentoken-adapter-2.5.1.jar` – the OpenToken Adapter JAR file
  - `/x86` – agent installation directory for 32-bit Windows architecture:

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

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

- `/conf` – configuration file
- `/Module Retargetable Folder` – IIS agent DLL, configuration data, and a sample application

▪ `/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

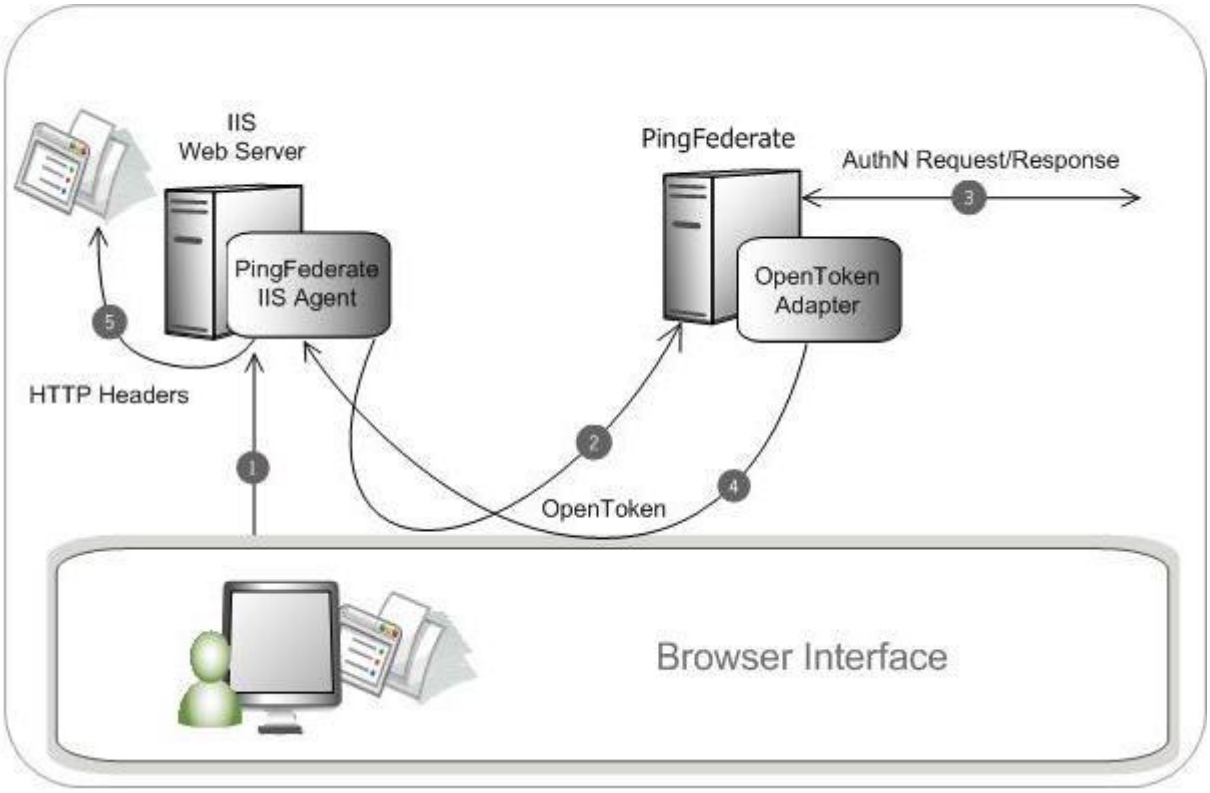
- `/conf` – configuration file
- `/Module Retargetable Folder` – IIS agent DLL, configuration data, and a sample application

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 following figure 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.

   (If an `OpenToken` session already exists, the user is granted immediate access.)
3. 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.
4. 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.
5. 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 both an IdP and 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 to step 5 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`.

   Important: If you are running PingFederate 5.1.0, also remove the file `opentoken-adapter.jar` from the directory:
   `<PF_install>/pingfederate/server/default/lib`

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.

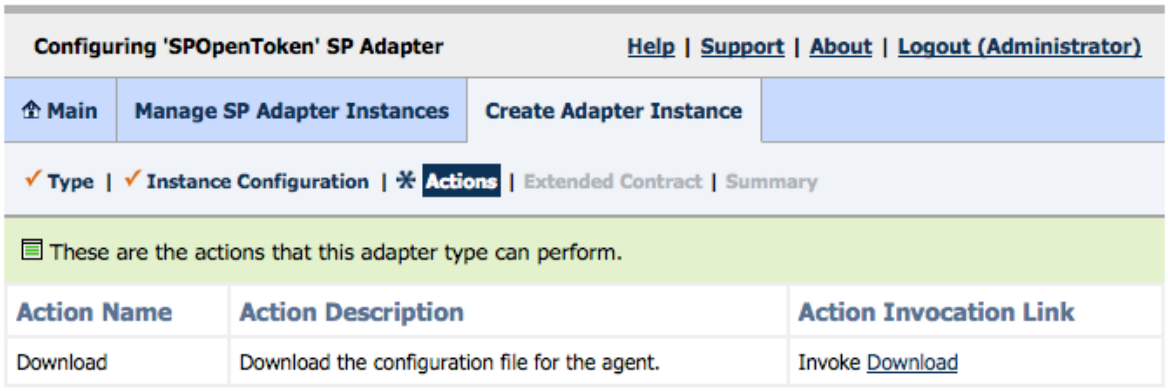
   Note: References to screens in the following steps conform to the appearance of the PingFederate 6.x administrative console. However, the configuration is the same for 5.x versions; only the screen names have changed.

5. Create an instance of the OpenToken Adapter for your SP configuration using settings on the Instance Configuration screen as indicated in the table below. (Fields not specified are optional. For more information, see OpenToken Adapter Configuration in the PingFederate *Administrator's Manual*.)

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

6. On the Actions screen in the adapter setup steps, click the **Download** link and 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 (see Installing and Configuring the PingFederate IIS Agent on page 8).



7. On the Extended Contract screen, enter any attributes you wish to pass to the application as HTTP request headers.

   For more information, see IIS Agent Session Information on page 11.

8. Configure a connection to your IdP partner, 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

> **Note:** If this is a first-time installation of the IIS Integration Kit, proceed directly to step 2 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. Using the Windows Control Panel, remove the existing OpenToken IIS agent from the IIS server.
   b. Restart IIS for changes to take effect.
2. Unzip the IIS Integration Kit distribution file into a directory on the IIS machine.
3. From the integration-kit `/dist` (`Win32` or `Win 64`)/ directory, run `setup.exe` and follow the setup screens.

   > **Note:** The setup installs the .NET Framework and supporting components.

   If you are unable to run the installer, you can manually accomplish these tasks (see Alternative Manual Installation on page 10).

   > **Important**: If you are running Windows Vista or Server 2008, run the executable as `Administrator`.

4. Register the .NET Framework 2.0 by entering the following command:

`<Windows>\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis -i -enable`

where *<Windows>* is the location of the operating system files.

5. 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:

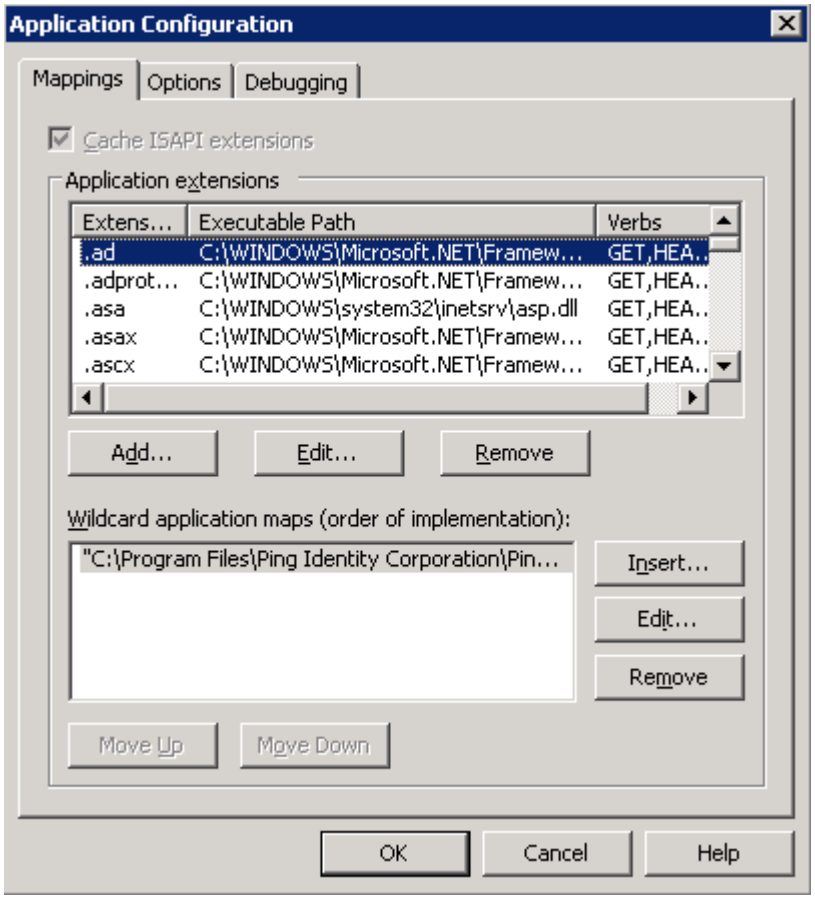
   `C:\Program Files\Ping Identity Corporation\OpenToken IIS Agent (n-bit)\`

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

6. For IIS 6.0, follow the steps below to register the PingFederate ISAPI extension:
   a. Access the IIS Manager.
   b. Locate the virtual directory representing the IIS site and right-click to go to Properties.
   c. On the Properties screen under the Virtual Directory tab, click **Configuration**.
   d. On the Application Configuration screen under Mappings, click **Insert** to locate and add the PingFederate IIS Agent to the Wildcard application maps. If you chose the default path for the PingFederate IIS Agent during installation, the path and file for the extension is:

      `"C:\Program Files\Ping Identity Corporation\OpenToken IIS Agent (n-bit)\bin\OpenTokenIISAgent.dll"`

Note: If you used the default path or chose another path with spaces in a folder name, then you must add quotation marks around the path.



e. Click **OK** and then click **OK** again on the Properties screen.

7. For IIS 7.0, follow the steps below to register the PingFederate ISAPI extension:
   a. Open the IIS Manager console.
   b. Select the Site you wish to protect with the Agent.
   c. Open the Features view, and select **ISAPI Filters**.
   d. Add a new filter named `OpenTokenIISAgent` with an executable of:

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

   e. On either a Site level, or an Application/Virtual Directory level, create a Wildcard script map to the IISAgent. To do this, select **Handler Mappings** on the Features view, click **Add Wildcard Script Map...**, and add a new script named `OpenTokenIISAgent` with an executable of:

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

8. Configure the properties file for IIS:

   The file is `pfisapi.conf` located in `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, at minimum, when no defaults are provided (change defaults as needed).

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

Alternative Manual Installation

If you are unable to run the installer script, you can configure the IIS Integration Kit Agent manually using the following procedure:

1. Download and install the .NET Framework 2.0 from Microsoft, and register the framework in IIS.
2. Copy the contents of `Module Retargetable Folder` in the integration-kit distribution to any directory.

   In this procedure, the full path of this directory is referred to as `<agent-install-dir>`.

3. Copy `conf/pfisapi.conf` from the distribution into a directory named:

   ```
   <agent-install-dir>\conf
   ```

4. Create a registry key under HKEY_LOCAL_MACHINE\SOFTWARE using the key folder\subfolder:

   Ping Identity Corporation\ISAPI Configuration

   Use the following key attributes:

   Name: `InstallPath`

   Type: `REG_SZ` (the default)

   Value: `<agent-install-dir>`

5. Install the Agent service:

Open a Command window and go to the `<agent-install-dir>\bin` folder. Run the following command:

```
AgentService.exe –install
```

Note: To uninstall the agent service, run the following command:

```
AgentService.exe –remove
```

6. Start the service from the Windows Services manager.
7. (For IIS 6.0) Register the ISAPI filter in IIS:
   a. Open the IIS Manager console.
   b. On the Web Sites level, right click Web Sites and select Properties.
   c. Under the ISAPI Filters tab, click **Add**.
   d. Add a new filter named `OpenTokenIISAgent` with a value:

      `<agent-install-dir>\bin\OpenTokenIISAgent.dll`
8. (For IIS 7.0) Register the ISAPI filter in IIS:
   a. Open the IIS Manager console.
   b. Select the Site you wish to protect with the Agent.
   c. Open the Features view, and select ISAPI Filters.
   d. Add a new filter named `OpenTokenIISAgent` with an executable of:

      `<agent-install-dir>\bin\OpenTokenIISAgent.dll`
   e. On either a Site level, or an Application/Virtual Directory level, create a Wildcard script map to the IIS Agent. To do this, select **Handler Mappings** on the Feature view, and click **Add Wildcard Script Map…** . Add a new script named `OpenTokenIISAgent` with an executable of:

      `<agent-install-dir>\bin\OpenTokenIISAgent.dll`

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.

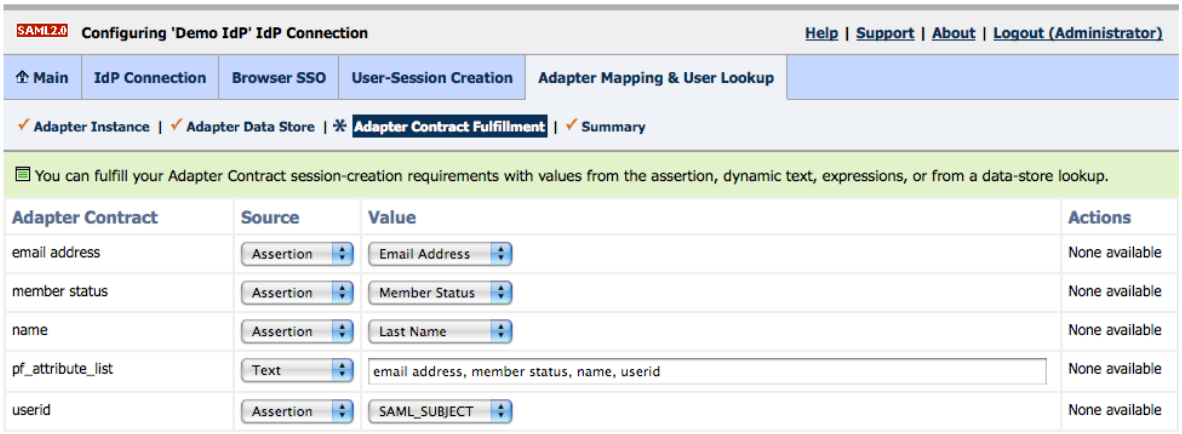
The session and attribute information exposed to the application includes the following:

- 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 (see Installing the OpenToken Adapter and Configuring PingFederate on page 7). Only the attributes fulfilled at runtime will be exposed to the application; attributes with a NULL value will not be 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.



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