Citrix XenApp Integration Kit

Contents

Citrix XenApp Integration Kit

The PingFederate Citrix XenApp Integration Kit adds a Service Provider (SP) application-integration option to PingFederate.

> ⓘ **Attention:**
>
> Updates and support have ended for this integration. The availability of this user guide and the related product download is intended only for those who have existing solutions using this integration.

Components

- OpenToken Adapter
  - Installed in PingFederate, this adapter uses the secure OpenToken standard to pass user attributes and session information from PingFederate to the Citrix IIS Agent on the IIS server.
- Citrix IIS Agent
  - Installed on the server running IIS, this program watches for protected resource requests and determines whether to grant access or redirect the user to PingFederate for authentication with an IdP.
- Citrix Web Interface Internet Information Services (IIS) Agent
  - Works in conjunction with the PingFederate OpenToken Adapter to allow an SP enterprise to accept identity assertions and provide Internet single sign-on (SSO) to Citrix XenApp. The assertions may be sent from the Identity Provider (IdP) using the SAML protocol (version 2.0 or 1.x) or the WS-Federation passive-requestor protocol. For more information, see *Supported Standards* in the PingFederate documentation.

Intended audience

This document is intended for PingFederate administrators.

Before you start, you should be familiar with the following parts of the PingFederate documentation:

- *Identity provider SSO configuration*
- *Managing IdP adapters*

System Requirements

The prerequisites in the following sections must be met in order to implement the Citrix Integration Kit.

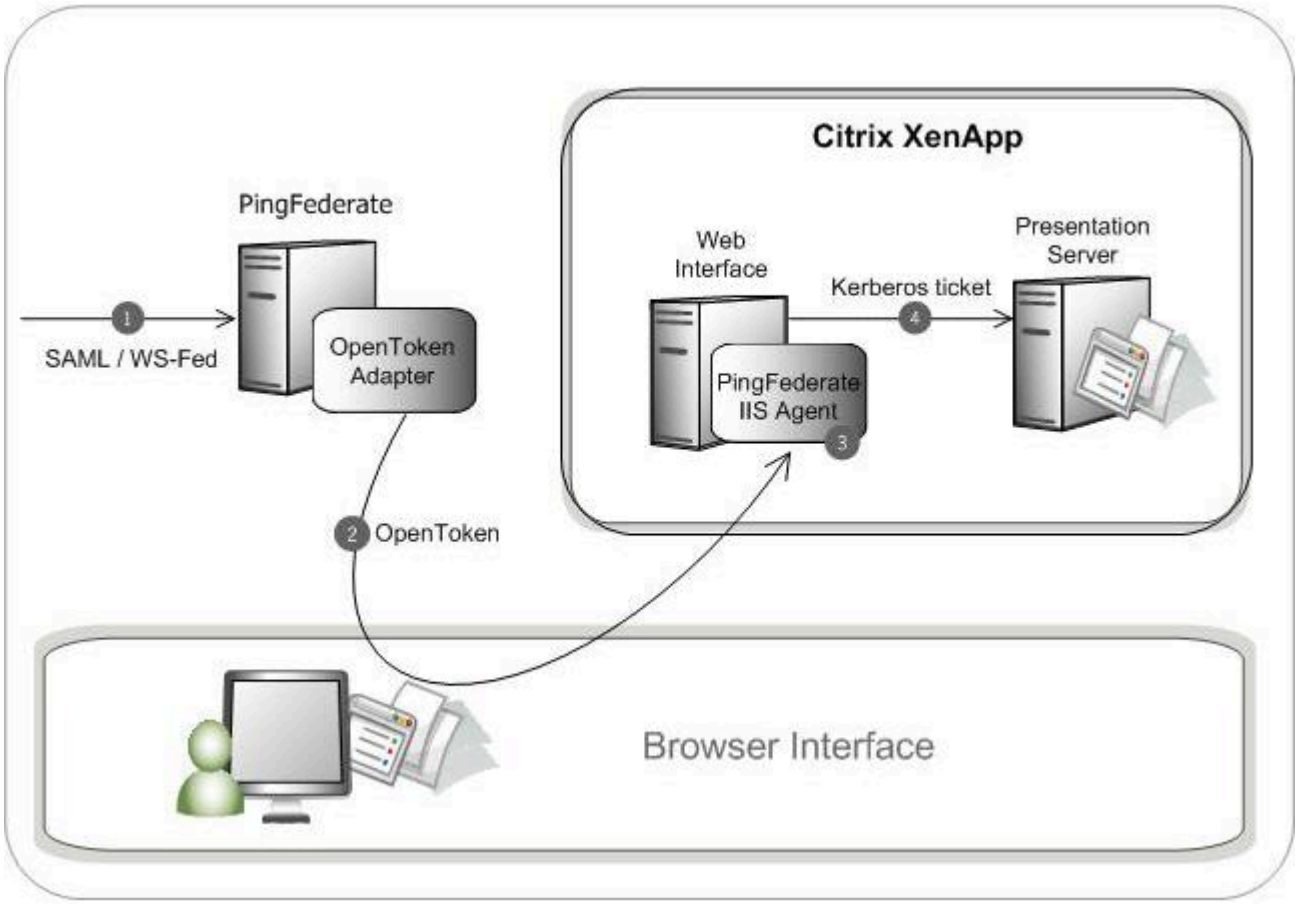
- Operating System and Software Requirements
  - Microsoft Windows Server 2008 or Microsoft Windows Server 2008 R2
  - .NET Framework 2.0
  - Citrix XenApp 6.5
  - Internet Information Services (IIS) 7.0 for Windows with the ISAPI filter and extension support enabled
  - PingFederate 6.x (or higher) server, installed with the OpenToken Adapter version 2.5.1 (or higher)

- Network and Citrix Configuration Requirements
  - The Citrix Web Interface server must be a member of the Presentation Server domain (or a trusted domain).
  - User identities must be mapped to accounts in the Presentation Server domain.
  - The Citrix Web Interface and Presentation Servers must be configured for constrained delegation.
  - The XML Service on the Presentation Server must share its port with IIS.

Overview of the SSO flow

The following figure illustrates the request flow and how the PingFederate SP OpenToken Adapter wraps attributes from an assertion into an `OpenToken` and passes the token to the PingFederate IIS Agent protecting the Citrix Web Interface. The PingFederate IIS Agent validates the `OpenToken` and then, using *protocol transition*, produces a Kerberos ticket on the IIS server allowing the user access to Citrix Web Interface. Because the Web Interface belongs to the same domain as the Presentation Server, through the use of *constrained delegation*, users can see and launch applications that are published on the Presentation Server.

ⓘ **Note:** The PingFederate IIS Agent is responsible for producing the Kerberos ticket for access to the Citrix Web Interface. The authentication between the Web Interface and the Presentation Server is governed by Kerberos-constrained delegation between the Citrix servers and is outside the scope of the PingFederate IIS Agent.



Processing Steps:

1. The PingFederate SP server receives an assertion from the IdP.
2. 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.
3. The IIS Agent verifies and parses the `OpenToken`, retrieves the `subject` and `realm` attributes from the `OpenToken` and generates a Kerberos ticket from these attributes, which the Web Interface and Presentation Server accept as credentials.
4. The Citrix Web Interface and Presentation Server authenticate the user using the Kerberos ticket and then allow access to applications on the Presentation Server via constrained delegation.

Setup

Install or upgrade the OpenToken adapter

About this task

ⓘ **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.

Steps

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 `opentoken-adapter-<version>.jar`.

   If the adapter JAR filename indicates version 2.1 or less, also delete the supporting library `opentoken-java-1.x.jar` from the same directory.

   ⓘ **Note:** 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`

   ⓘ **Note:** From the integration kit `/dist` directory, copy the `opentoken-agent-2.5.1.jar` into `app_server_root/lib/ext`.
4. Start or restart the PingFederate server.
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 *Configuring an OpenToken SP Adapter instance* in the PingFederate documentation.

Option	Description
Password	Enter any password you choose.

Option	Description
Confirm Password	Password confirmation.

ⓘ **Note:** In the Advanced Fields section, be sure to leave Authentication Service blank: the SP Adapter redirects a user to the protected resource directly.

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 Citrix Agent (see *Install and configure the PingFederate IIS web agent* on page 8).

7. Configure or modify the connection(s) to your IdP partner(s) to use the instance of the OpenToken Adapter you configured in the last steps.

   For more information, see *Identity Provider SSO Configuration* in the PingFederate documentation.

ⓘ **Note:** For Idp-initiated SSO, your IdP partner must set the target resource URL to the Citrix Web Interface `auth/federated.aspx` or `auth/login.aspx` protected sites. For information about constructing SSO URLs when PingFederate is used at the IdP site, see *Application Endpoints* in the PingFederate documentation.

Configure Citrix XenApp

Configuring Citrix XenApp to work with the PingFederate Integration Kit involves:

Create a web interface for federated authentication

To create a Web Interface site that uses federated authentication to Presentation Server(s), you can use the **Create site** task in the Web Interface Management Console. After the site is created, it can be managed using the Web Interface Console.

Create a site through the Web Interface Management Console. When specifying the point of authentication, select **At third party using Kerberos** as the authentication mechanism.

Configure the Citrix presentation server

About this task

To configure the Citrix Presentation server, you must set up a trust relationship between the server running the Web Interface and any other servers in the farm running the Citrix XML Service that the Web Interface contacts.

ⓘ **Note:** The XML Service running on the Citrix Presentation Server must share its port with IIS.

From the Citrix App Center for the Presentation Server:

ⓘ **Note:** The Trust XML requests option is disabled by default within Citrix.It must be enabled to set up a trust relationship between the server running the Web Interface.

Steps

1. Click **Policies** and go to the **Computer** tab.
2. Click **Summary**.
3. Click **Edit** in the Trust XML requests option.
4. Click **Enabled – The Citrix XML Service will trust requests sent to it** and then click **OK**.

Configure delegation for Citrix servers

Ensure that all servers within your deployment are trusted for delegation by performing these tasks:

- Trust the server(s) running the Web Interface for delegation
- Trust the server(s) running the XML Service (Presentation Server) for delegation

ⓘ **Note:** You need access to the Domain Controller running your Citrix servers to perform the following tasks.

Trust the server running the Web Interface for delegation

About this task

Steps

1. From the domain controller, in the MMC Active Directory Users and Computers snap-in **View** menu, enable **Advanced Features**.
2. In the Computers folder under the domain name, select the server running the Web Interface.
3. On the **Action** menu, click **Properties** or double-click the Web Interface Server name.
4. Under the Delegation tab, select **Trust this computer for delegation to specified services only** and **Use any authentication protocol**, and then click **Add**.
5. On the Add Services screen, click **Users or Computers**.
6. On the Select Users or Computers screen, type the name of the server running the XML Service (Presentation Server) in the text box, and then click **OK**.
7. Select the **http** service type from the list and then click **OK**.
8. Under the Delegation tab, verify that the http service type for the server running the Presentation Server appears in the list box, and then click **OK**.

Trust the server running the Presentation Server for delegation

About this task

Steps

1. From the domain controller, in the Computers folder under the MMC Active Directory Users and Computers snap-in, select the name of the server running the XML Service that the Web Interface is configured to contact.
2. On the Action menu, click **Properties** or double-click the Presentation Server name.
3. Under the Delegation tab, select **Trust this computer for delegation to specified services only** and **Use Kerberos only**, and then click **Add**.
4. On the Add Services screen, click **Users or Computers**.
5. In the text box on the Select Users or Computers screen, enter the name of the Web Interface Server running the XML Service and then click **OK**.
6. Select the **HOST** service type from the list and then click **OK**.
7. Under the Delegation tab, verify that the HOST service type for the server running the XML Service appears in the list.
8. Under the Delegation tab, click **Add**.
9. On the Add Services screen, click **Users or Computers**.
10. In the text box on the Select Users or Computers screen, enter the name of the Domain Controller and then click **OK**.
11. Select the **ldap** service type from the list and then click **OK**.

> ⓘ **Note:** There may be multiple instances of ldap service types. Ensure you select the ldap service type with the Domain Controller name.

12. Under the Delegation tab, verify that the ldap service type for the Domain Controller appears in the list and click **OK**.
13. Click **Apply** and then **OK**.

> ⓘ **Note:** Depending on how your active directory and presentation server farms are deployed, you may need to repeat the procedure for each server running the XML Service that the Web Interface is configured to contact. Please refer to *Citrix support documentation* for additional information.

Install and configure the PingFederate IIS web agent

About this task

> ⓘ **Note:** If this is a first-time installation of the Citrix Integration Kit, proceed directly to step *2* in the following procedure.

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

Steps

1. If you are upgrading this integration:
   a. Temporarily stop your IIS if it is running.
   b. Using the Windows Control Panel, remove the existing OpenToken IIS agent (OpenToken IIS Agent (`32-bit`)) from the IIS server.
   c. Restart IIS for changes to take effect.
2. Unzip the Citrix Integration Kit distribution file into a directory on the Citrix Web Interface server.
3. From the `/dist` folder in the directory where you unzipped the distribution file, run `setup.exe` and follow the setup screens.

   ⓘ **Note:** The OpenToken IIS Agent 32-bit setup (`setup.exe`) file must be run for every Web Interface server that you want to integrate with PingFederate. The setup installs .NET Framework 2.0 and supporting components.
4. 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 (32-bit)\
   ```
5. Follow the steps below to register the PingFederate ISAPI extension with IIS:
   a. Access the Internet Information Services (IIS) Manager.
   b. Locate the virtual directory representing the Citrix Web Interface.

      This is the directory created in IIS when you created the Access Platform.
   c. On the Application Configuration screen under Handler Mappings, click **Add Wildcard Script Map…** to locate and add the PingFederate IIS Agent to the Handler Mappings.

      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 (32-bit)\bin\OpenTokenIISAgent.dll
      ```

      ⓘ **Note:** Refer to IIS product specific documentation for detailed information on how to add Wildcard application maps.
   d. Click **OK** and then click **Yes** to confirm the allowance of the ISAPI extension.
6. Configure the properties file for IIS:

   The file is `pfisapi.conf` located in `C:\Program Files(x86)\Ping Identity Corporation\OpenToken IIS Agent (32-bit)\conf`. Refer to comments in the file for information and configuration of the required properties.
7. Restart IIS for `pfisapi.conf` changes to take effect.

Release notes

Changelog

Change List by Version

ⓘ **Note:** 2.1 and 2.2 version numbers skipped for internal configuration management.

Citrix Integration Kit 2.4 – December 2012 (Current Release)

- Updated to address security issues found since previous release
- Added support for OpenToken 2.5.1 Adapter and OpenToken 2.5.1 Agent

Citrix Integration Kit 2.3 – August 2012

- Added support for the following
  - Citrix XenApp 6.5
  - Citrix Web Interface v5.4.0.59
  - Windows Server 2008 R2
  - Internet Information Services (IIS) 7.0 for Windows

Citrix Integration Kit 2.0 – September 2009

- Added support for Citrix XenApp 5
- Ported the IIS Agent to use the OpenToken Adapter and the OpenToken .NET library
- Support added for the POST transport method from the OpenToken Adapter

Citrix Integration Kit 1.0.1 – October 2007

- Updated Citrix Integration Kit User Guide documentation

Citrix Integration Kit 1.0 – March 2007

- Initial release

Qualification statement

This section documents testing performed on the PingFederate Citrix Integration Kit with PingFederate 6.x, as of December 2012.

Version Tested

- pf-citrix-integration-kit-2.4

Operating Systems Tested

- Windows 2008 Server Enterprise Edition R2 64-bit
- Windows Server 2003 R2 32-bit

PingFederate Versions Tested

- PingFederate 6.10

Browsers Tested

- Internet Explorer 9
- FireFox 14

Citrix Configuration Tested

- Citrix XenApp 6.5 Enterprise Edition
- Citrix Web Interface 5.4.0.59

Common issues/problems/limitations

The following table provides a list of potential configuration issues that could arise with the Citrix Integration Kit installation, together with possible causes and solutions.

Issue/Error	Possible Cause	Potential Solution
The Citrix Integration Kit only supports OpenToken smaller than 1000 characters.	Large number of extended attributes in OpenToken can cause the size of OpenToken to increase in size beyond 1000 characters.	These extended attributes are not used in Citrix inte such there is no issue with the Citrix Integration Kit.
End-users remain logged on even though their browser sessions were ended or single logout was invoked.	Redundant session cookies from different domains.	Ensure that the domain specified in the `OpenToker` setup matches the domain configured in the `pfisa`
Citrix Web Interface errors: “No applications enumerated“ “Some of your published resources have not been reconnected” “An error occurred while making the requested connection.”	The Citrix server’s XML service does not trust connections.	For additional information, see To configure the Citr Reference source not found.*Presentation Server in *XenApp Integration Kit User Guide*.
“Unreadable token” errors.	Multiple adapters and agents are using the same cookie, which is not supported.	Ensure that the OpenToken name specified in the a instance setup is unique among any additional adap configured.
Upgrading to new version of the PingFederate Citrix Agent does not provide expected new features.	The IIS server was not restarted after the new version was installed.	Restart the IIS server.
“Error - Single Sign-On Could not obtain attributes from OpenToken, please make sure the agent service has been started.”	The PingFederate Agent tries to create a Kerberos ticket, but the call to the Key Distribution Center fails because the user account does not exist.	Ensure that users (defined as the mapped subject a attributes of the `OpenToken`) have an account in th server.
“An Authentication error has occurred. Please contact your administrator”	For IdP-initiated SSO using a query parameter or POST transport, no OpenToken cookie was found in the request headers because the token was not converted to a session cookie.	The target resource in the SAML request must be s the Web Interface protected sites `auth/login.as` `federated.aspx`.

Download manifest

The distribution `.zip` archive for the Citrix 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 run the adapter and agent:
  - `opentoken-adapter-2.5.1.jar` – The OpenToken Adapter JAR file
  - `setup.exe` – Installation program for the PingFederate Citrix IIS Agent
  - `Support Files.msi` – Installation supporting files for the PingFederate Citrix IIS Agent
  - `/conf`– Contains configuration file
  - `/Module Retargetable Folder` – Contains Citrix IIS agent DLL and configuration data