

PingFederate IIS INTEGRATION KIT (OPENTOKEN AGENT) for an IIS Application

<https://docs.pingidentity.com/bundle/integrations/page/tok1563995020974.html#>

<https://docs.pingidentity.com/bundle/pingfederate-iis-ik/page/rze1563995020861.html>

<https://docs.pingidentity.com/bundle/pingfederate-iis-ik/page/gaj1563995020916.html>

An application that does not support SAML and you want to enable SSO for it.

SSO enabling for your application means that you are offloading authentication to an external third party.

The objective of SSO is that the IdP authenticates who the user is. It may authenticate the user directly or leverage another system (such as Kerberos or other form based authn).

The IdP then generates a verifiable security token that contains a unique identifier for the user: a digitally signed SAML assertion is an example.

The SAML assertion is sent to a Service Provider (SP), that can validate the integrity and trust of the SAML Assertion. Upon doing so, the SP now knows the unique identifier of the user (e.g. their email address) and can trust this information.

The next objective is to get this unique identifier (and any other attributes of interest) to your web server in a secure and verifiable manner. For this you have chosen to use the IIS Integration kit.

The IIS Integration Kit allows the PingFederate Service Provider to generate a secure token (an Opentoken token) and send it to IIS.

IIS can verify the integrity and trust of the token, and upon doing so will have access to the user's identity information.

IIS then needs to convey this identity information to your web application in a secure manner.

For this, it chooses to inject additional HTTP headers into the request being sent to your web application.

Your web application needs to be modified to support this SSO integration.

If your web application does not have an existing session for the user, it should inspect the headers of the incoming request. If it locates the trusted identity headers, then it should use them directly. It doesn't need to present a login form, it just needs to read the information within the headers, trust it automatically, and simply log the person in.

OpenToken Adapter

In order to transfer identity and other user information between the PingFederate® server and an end application, the product architecture allows for custom adapters to be deployed with the server.

PingFederate ships with a deployed OpenToken Adapter, which uses a secure token format (OpenToken) to transfer user attributes between an application and the PingFederate server.

On the IdP side, the OpenToken Adapter allows the PingFederate server to receive a user's identity from the IdP application.

For SAML connections, the IdP application has the option to provide an authentication context to the SP by including the authnContext attribute with the desired value in the secure token. Standard URIs are defined in the SAML specifications (see the OASIS documents oasis-sstc-saml-core-1.1.pdf and saml-authn-context-2.0-os.pdf).

If the secure token does not contain the authnContext attribute, PingFederate sets the authentication context as follows:

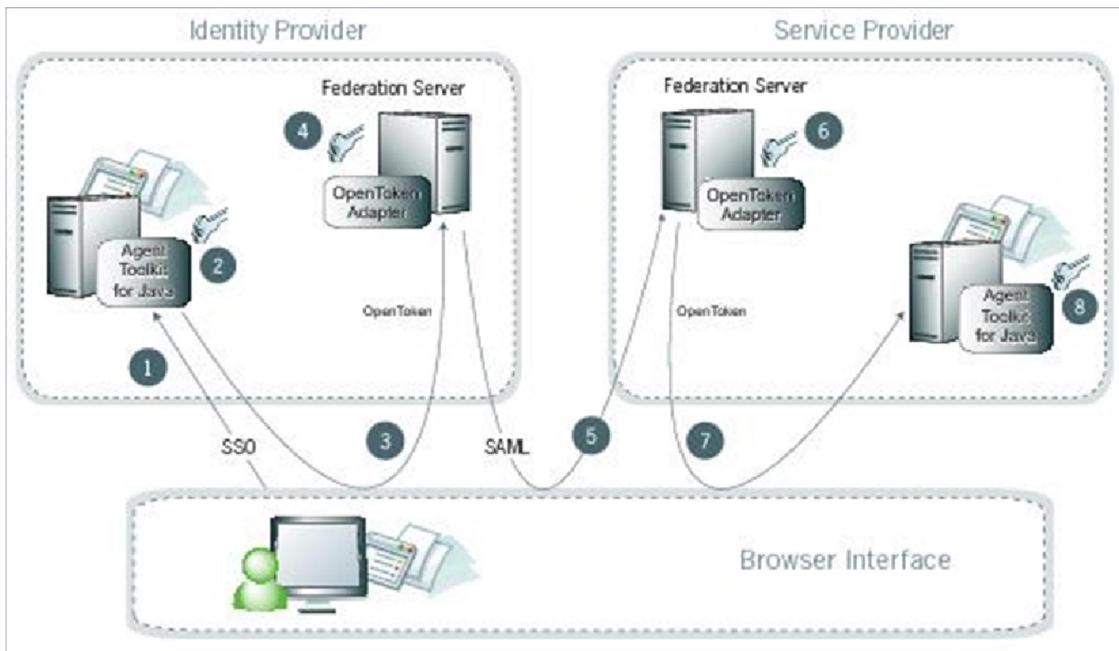
urn:oasis:names:tc:SAML:1.0:am:unspecified for SAML 1.x

urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified for SAML 2.0

As needed, the authentication context can be overridden by either an instance of the Requested AuthN Context Authentication Selector or the SAML_AUTHN_CTX attribute in the SAML attribute contract. (The latter takes precedence.)

On the SP side, the OpenToken Adapter can be used to transfer user-identity information to the target SP application.

Specialized application integration kits are available from the Ping Identity Downloads website. Many kits leverage the OpenToken Adapter to integrate applications with the PingFederate server. The agent portions of the integration kits reside with the application and use the OpenToken to communicate with the OpenToken Adapter.



Processing steps

A user initiates an SSO transaction.

The IdP application inserts attributes into the Agent Toolkit for Java, which encrypts the data internally and generates an OpenToken.

A request containing the OpenToken is redirected to the PingFederate IdP server.

The server invokes the OpenToken IdP Adapter, which retrieves the OpenToken, decrypts, parses, and passes it to the PingFederate IdP server. The PingFederate IdP server then generates a Security Assertion Markup Language (SAML) assertion.

The SAML assertion is sent to the SP site.

The PingFederate SP server parses the SAML assertion and passes the user attributes to the OpenToken SP Adapter. The Adapter encrypts the data internally and generates an OpenToken.

A request containing the OpenToken is redirected to the SP application.

The Agent Toolkit for Java decrypts and parses the OpenToken and makes the attributes available to the SP Application.

SSO configuration at PingFederate end

Creating a SP Adapter of Type OpenToken Adapter 2.5

PingFederate

- < Integration
- SP Connections
- SP Adapters
- Target URL Mapping
- SP Default URLs
- Policy Contract Adapter Mappings
- Adapter-to-Adapter Mappings

SP Adapters | Create Adapter Instance

Type	Instance Configuration	Actions	Extended Contract	Target App Info	Summary
INSTANCE NAME	safe				
INSTANCE ID	safe				
TYPE	OpenToken Adapter 2.5.3				
CLASS NAME	com.pingidentity.adapters.opentoken.SpAuthnAdapter				
PARENT INSTANCE	None				

PingFederate

- < Integration
- SP Connections
- SP Adapters
- Target URL Mapping
- SP Default URLs
- Policy Contract Adapter Mappings
- Adapter-to-Adapter Mappings

COOKIE PATH	/	AUTHENTICATION	APPLICATIONS	SECURITY	SYSTEM
COOKIE PATH	/				The path for the cookie that contains the token.
TOKEN LIFETIME	600				The duration (in seconds) for which the token is valid. Valid range is 1 to 28800.
SESSION LIFETIME	43200				The duration (in seconds) for which the token may be re-issued without authentication. Valid range is 1 to 259200.
NOT BEFORE TOLERANCE	300				The amount of time (in seconds) to allow for clock skew between servers. Valid range is 0 to 3600.
FORCE SUNJCE PROVIDER	<input type="checkbox"/>				If checked, the SunJCE provider will be forced for encryption/decryption.
USE VERBOSE ERROR MESSAGES	<input checked="" type="checkbox"/>				If checked, use verbose TokenException messages.
OBFUSCATE PASSWORD	<input checked="" type="checkbox"/>				If checked, the password will be obfuscated and password-strength validation will be applied. Clearing the checkbox allows backward compatibility with previous OpenToken agents.
SESSION COOKIE	<input checked="" type="checkbox"/>				If checked, OpenToken will be set as a session cookie (rather than a persistent cookie). Applies only if Transport Mode is set as "Cookie".
SECURE COOKIE	<input checked="" type="checkbox"/>				If checked, the OpenToken cookie will be set only if the request is on a secure channel (https). Applies only if Transport Mode is set as "Cookie".
SEND SUBJECT AS QUERY PARAMETER	<input type="checkbox"/>				Checking this box will send the Subject ID as a clear-text query parameter, if Transport Mode is set to "Query Parameter". If Transport Mode is set to "Form POST", the Subject ID is sent as POST data.
SUBJECT QUERY PARAMETER					The parameter name used for the Subject ID when the "Send Subject ID as Query Parameter" box is checked.
SEND EXTENDED ATTRIBUTES	None				Extended Attributes are typically sent only within the token, but this option overrides the normal behavior and allows the attributes to be included in browser cookies or query parameters.
SKIP TRIMMING OF TRAILING BACKSLASHES	<input type="checkbox"/>				If not checked, it prevents insecure content from affecting the security of your application/agent. We recommend to update your applications with the latest version of the agent. We recommend not to change the value of this flag.

[Hide Advanced Fields](#)

Cancel Previous Next Save

PingFederate

- < Integration
- SP Connections
- SP Adapters
- Target URL Mapping
- SP Default URLs
- Policy Contract Adapter Mappings
- Adapter-to-Adapter Mappings

SP Adapters | Create Adapter Instance

Type	Instance Configuration	Actions	Extended Contract	Target App Info	Summary
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.					
OpenToken Adapter 2.5.3					
Field Name	Field Value	Description			
PASSWORD	Password to use for generating the encryption key.			
CONFIRM PASSWORD	Must match password field.			
TRANSPORT MODE	<input type="radio"/> Query Parameter <input checked="" type="radio"/> Cookie <input type="radio"/> Form POST	How the token is transported to/from the application, either via a query parameter (default), a cookie, or as a form POST. NOTE: Form POST is applicable only for an SP adapter instance.			
TOKEN NAME	opentokan	The name of the cookie or query parameter that contains the token. This name must be unique for each adapter instance.			
CIPHER SUITE	<input type="radio"/> Null <input type="radio"/> AES-256-CBC <input checked="" type="radio"/> AES-128-CBC <input type="radio"/> 3DES-168-CBC	The algorithm, cipher mode, and key size that should be used for encrypting the token.			
AUTHENTICATION SERVICE		The URL to which the user is redirected for an SSO event. This URL overrides the Target Resource which is sent as a parameter to the Authentication Service.			
ACCOUNT LINK SERVICE		The URL to which the user is redirected for Account Linking. This URL is part of an external SP application. This external application performs user authentication and returns the local user ID inside the token.			

PingFederate

AUTHENTICATION APPLICATIONS SECURITY SYSTEM

SP Adapters | Create Adapter Instance

Type Instance Configuration Actions Extended Contract Target App Info Summary

Optional, you can specify the name of the application and the icon URL of the target application.

APPLICATION NAME

APPLICATION ICON URL

[Cancel](#) [Previous](#) [Next](#) [Save](#)

PingFederate

AUTHENTICATION APPLICATIONS SECURITY SYSTEM

SP Adapters | Create Adapter Instance

Type Instance Configuration Actions Extended Contract Target App Info Summary

Actions are available for this instance and can be invoked from here.

Name	Description	Action
Download	Download the configuration file for the agent.	Download

[Cancel](#) [Previous](#) [Next](#) [Save](#)

PingFederate

AUTHENTICATION APPLICATIONS SECURITY SYSTEM

SP Adapters | Create Adapter Instance

Type Instance Configuration Actions Extended Contract Target App Info Summary

This adapter type supports the creation of an extended adapter contract. Add additional attributes here that are required by the target application. This contract must be fulfilled using attributes from the source mapping combined with attributes returned from a local data store lookup.

Core Contract

subject

Extend the Contract

[Add](#)

[Cancel](#) [Previous](#) [Next](#) [Save](#)

Add the Application URL in Target URL mapping

Creating a IDP Connection where PingFederate acting as a Service Provider

PingFederate		AUTHENTICATION	APPLICATIONS	SECURITY	SYSTEM
< Integration	Virtual Server IDs				
	Restricted Virtual Server ID			(none)	
<input checked="" type="checkbox"/> IdP Connections	Adapter Data Store				
	Attribute location			Use only the attributes available in the SSO Assertion	
<input type="checkbox"/> IdP Adapters	Adapter Contract Fulfillment				
	subject			SAML_SUBJECT (Assertion)	
<input type="checkbox"/> Authentication API Applications	Issuance Criteria				
	Criterion			(None)	
<input type="checkbox"/> IdP Default URL	Protocol Settings				
	SSO Service URLs				
	Endpoint			URL: /idp/SSO.saml2 (POST)	
	Endpoint			URL: /idp/SSO.saml2 (Redirect)	
	SLO Service URLs				
	Endpoint			URL: /idp/SLO.saml2 (POST)	
	Allowable SAML Bindings				
	Artifact			false	
	POST			true	
	Redirect			true	
	SOAP			false	
	Overrides				
	Signature Policy				
	Sign AuthN requests over POST and Redirect			false	
	Require digitally signed SAML Assertion			false	

[Integration](#) [IdP Connections](#) [IdP Adapters](#) [Authentication API Applications](#) [IdP Default URL](#)

IdP Connections | IdP Connection | Browser SSO | User-Session Creation

[Identity Mapping](#) [Attribute Contract](#) [Target Session Mapping](#) **Summary**

PingFederate can create sessions to internal applications and/or identity management system using adapters, or create sessions to partner SPs using Policy Contracts. A session target application on your system. Likewise, map a connection contract for each partner SP(s).

Adapter Instance Name	Virtual Server IDs
-----------------------	--------------------

safe	
------	--

Authentication Policy Contract Name	Virtual Server IDs
-------------------------------------	--------------------

[Map New Adapter Instance](#)[Map New Authentication Policy](#)

PingFederate

AUTHENTICATION APPLICATIONS SECURITY SYSTEM

< Integration

IdP Connections

IdP Adapters

Authentication API Applications

IdP Default URL

IdP Connections | IdP Connection | Browser SSO | User-Session Creation | Adapter Mapping & User Lookup

Adapter Instance Virtual Server IDs Adapter Data Store Adapter Contract Fulfillment Issuance Criteria Summary

Adapter Mapping Summary

Adapter Instance

Selected adapter safe

Virtual Server IDs

Restricted Virtual Server ID (none)

Adapter Data Store

Attribute location Use only the attributes available in the SSO Assertion

Adapter Contract Fulfillment

subject SAML_SUBJECT (Assertion)

Issuance Criteria

Criterion (None)

PingFederate

AUTHENTICATION APPLICATIONS SECURITY SYSTEM

< Integration

IdP Connections

IdP Adapters

Authentication API Applications

IdP Default URL

IdP Connections | IdP Connection | Browser SSO | User-Session Creation | Adapter Mapping & User Lookup

Adapter Instance Virtual Server IDs Adapter Data Store Adapter Contract Fulfillment Issuance Criteria Summary

The list of attributes below, the Adapter Contract, is required for the selected adapter instance.

Adapter Instance

Adapter Contract

subject

OVERRIDE INSTANCE SETTINGS

Manage Adapter Instances

PingFederate

AUTHENTICATION APPLICATIONS SECURITY SYSTEM

< Integration

IdP Connections

IdP Adapters

Authentication API Applications

IdP Default URL

IdP Connections | IdP Connection | Browser SSO | User-Session Creation | Adapter Mapping & User Lookup

Adapter Instance Virtual Server IDs Adapter Data Store **Adapter Contract Fulfillment** Issuance Criteria Summary

You can fulfill the Adapter Contract by using only the attributes from the SAML assertion or by using these attributes to look up additional information from a local data store.

Attribute Contract

SAML SUBJECT

USE THE SSO ASSERTION TO LOOK UP ADDITIONAL INFORMATION
 USE ONLY THE ATTRIBUTES AVAILABLE IN THE SSO ASSERTION

PingFederate

AUTHENTICATION APPLICATIONS SECURITY SYSTEM

< Integration

IdP Connections

IdP Adapters

Authentication API Applications

IdP Default URL

IdP Connections | IdP Connection | Browser SSO | User-Session Creation | Adapter Mapping & User Lookup

Adapter Instance Virtual Server IDs Adapter Data Store **Adapter Contract Fulfillment** Issuance Criteria Summary

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
subject	Assertion	SAML SUBJECT

Creating a SP Connection where PingFederate acting as a Identity Provider

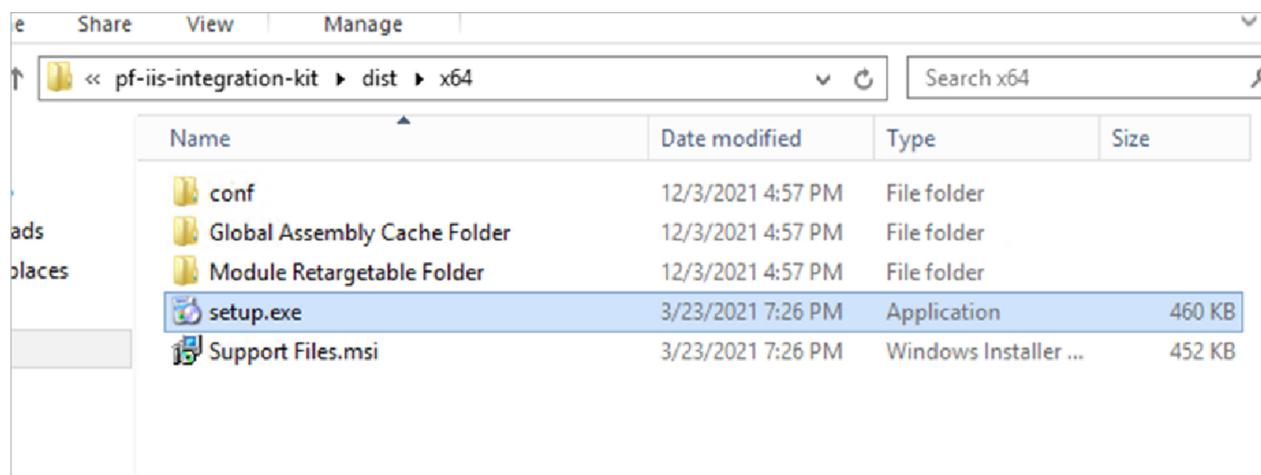
PingFederate	AUTHENTICATION	APPLICATIONS	SECURITY	SYSTEM
Integration	Restricted Virtual Server ID		(none)	
SP Connections	Mapping Method			
	Authentication Policy Contract		AIR Minimum Claims	
SP Adapters	Mapping Method		Use only the Authentication Policy Contract values in the mapping	
Target URL Mapping	Attribute Contract Fulfillment			
	SAML SUBJECT		subject (Authentication Policy Contract)	
SP Default URLs	Issuance Criteria			
	Criterion		(None)	
Policy Contract Adapter Mappings	Protocol Settings			
Adapter-to-Adapter Mappings	Assertion Consumer Service URL			
	Endpoint		URL: /sp/ACS.saml2 (POST)	
	SLO Service URLs			
	Endpoint		URL: /sp/SLO.saml2 (Redirect)	
	Endpoint		URL: /sp/SLO.saml2 (POST)	
	Allowable SAML Bindings			
	Artifact		false	
	POST		true	
	Redirect		true	
	SOAP		false	
	Signature Policy			
	Require digitally signed AuthN requests		false	
	Always Sign Assertion		true	
	Sign Response As Required		false	

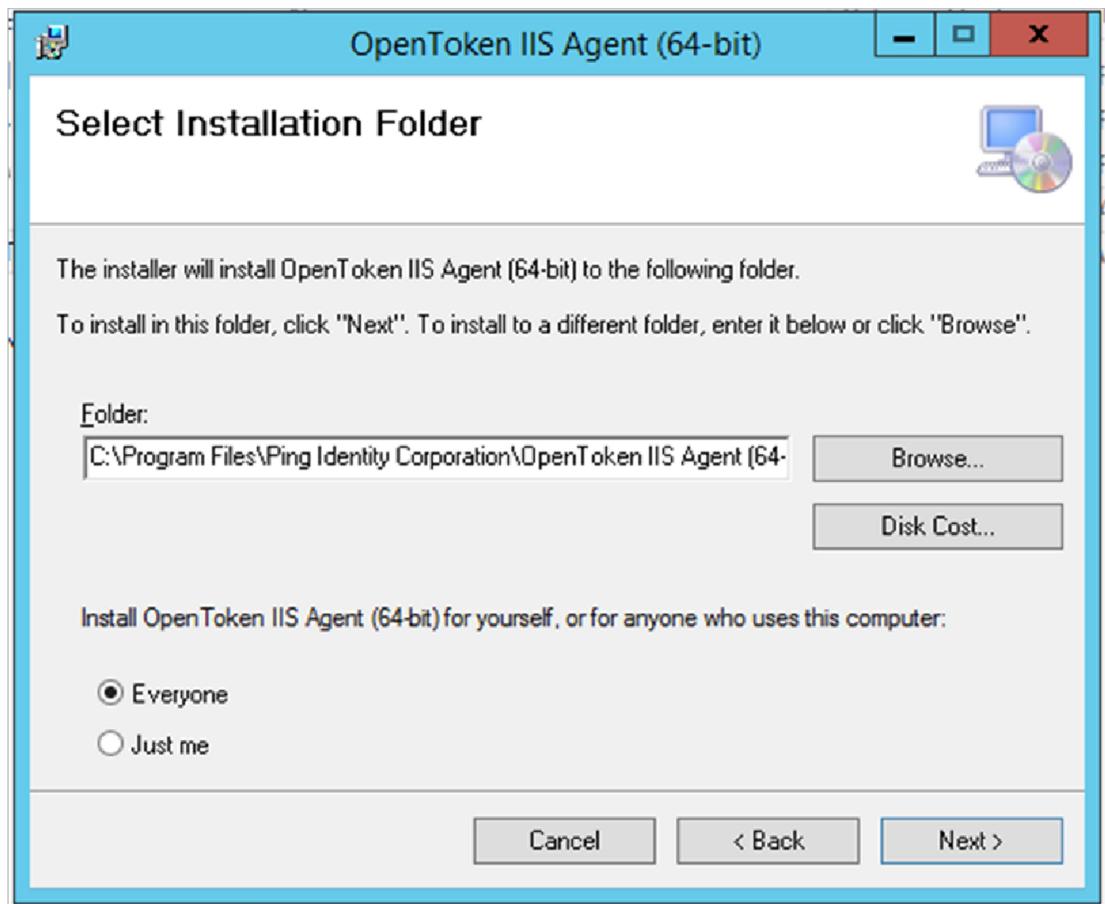
Configuration at IIS end

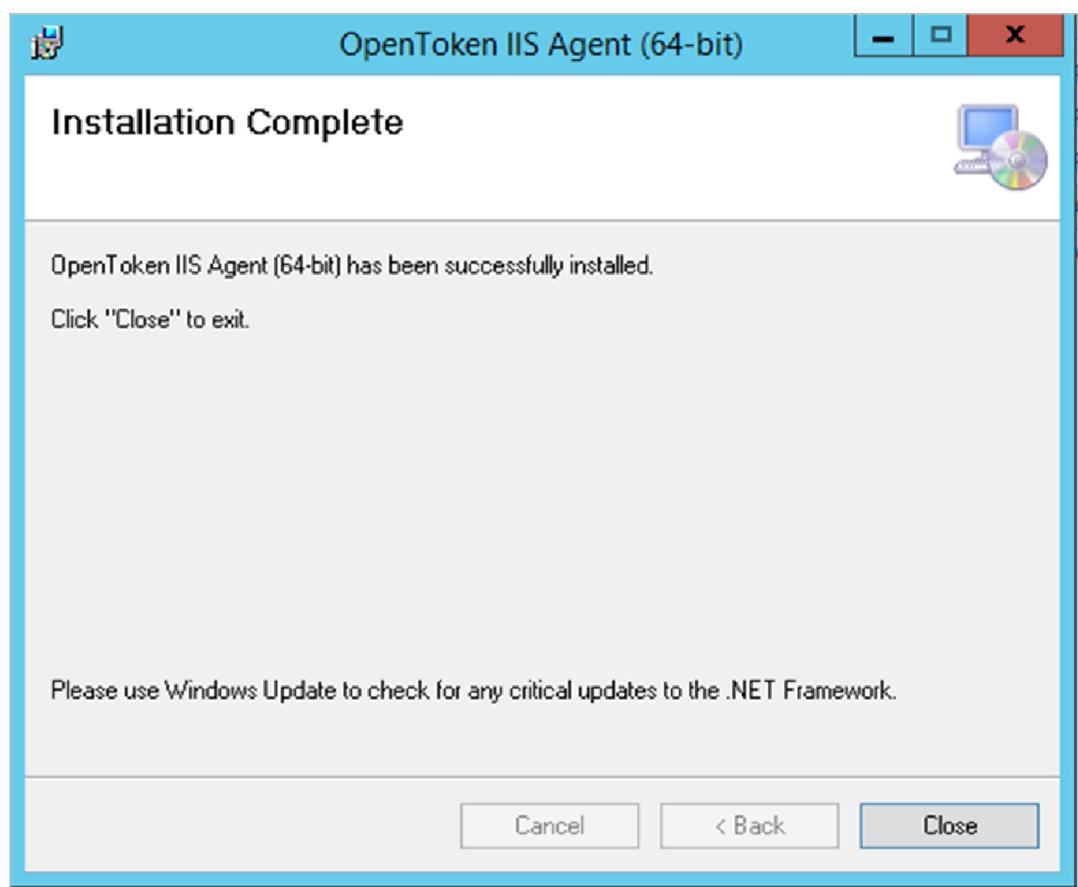
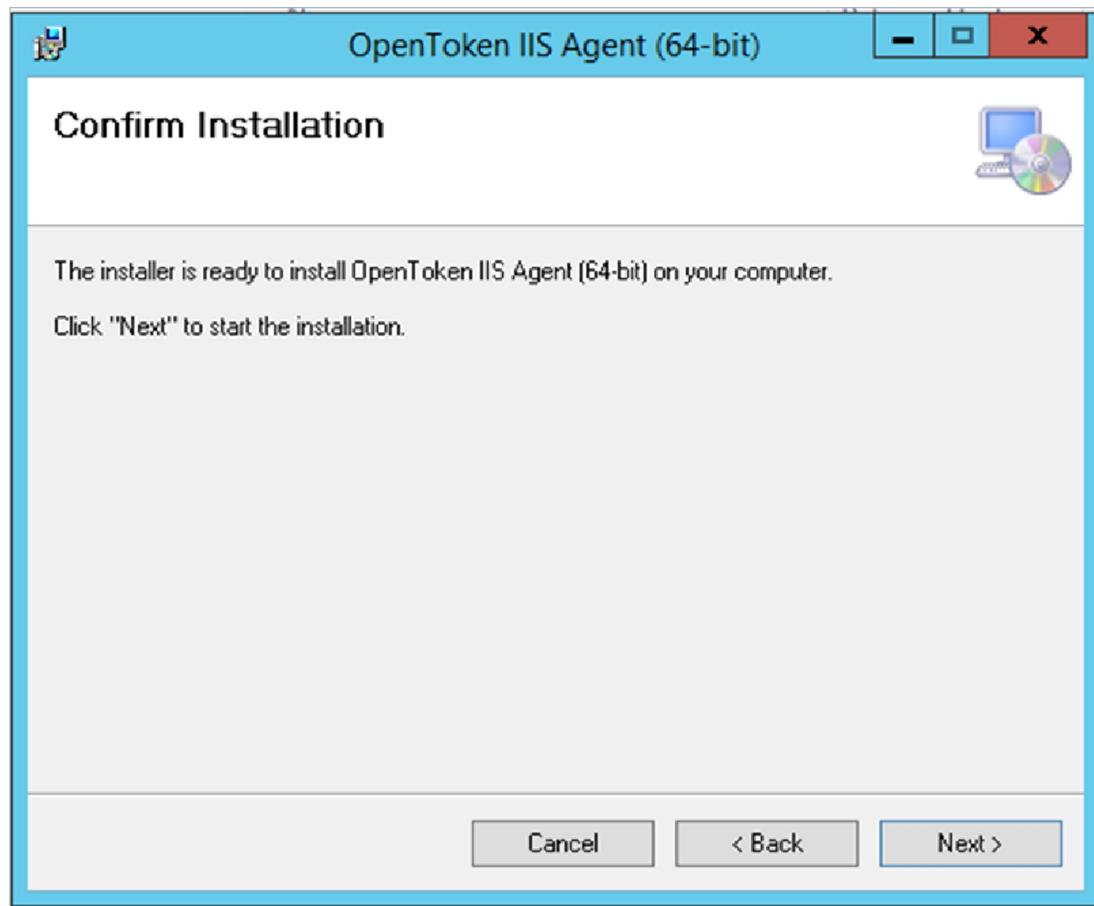
Install and configure the PingFederate IIS web agent

Unzip the Citrix Integration Kit distribution file into a directory on the Citrix Web Interface server

From the /dist folder in the directory where you unzipped the distribution file, run setup.exe and follow the setup screens.







Once Installation completed get the agent-config.txt file from SSO team and copy into the \conf directory created by the installer.

By default, this directory is located in:

C:\Program Files\Ping Identity Corporation\OpenToken IIS Agent

pf-iis-integration-kit > dist > x64 > conf				Search conf
Name	Date modified	Type	Size	
agent-config.txt	3/23/2021 7:26 PM	Text Document	1 KB	
pfisapi.conf	3/31/2021 12:02 AM	CONF File	6 KB	
start_page_template.html	3/23/2021 7:26 PM	HTML File	3 KB	

1. Update the given **agent-config** File from the SSO Team .

2. Add the **SSOUrl**, **PingFedBaseUrl** And **SecureCookie=YES** in pfisapi.conf

Update Pfisapi.conf file attributes as recommended by Ping SSO

This PC > Windows (C:) > Program Files > Ping Identity Corporation > OpenToken IIS Agent (64-bit) > conf				
Name	Date modified	Type	Size	
agent-config.txt	3/23/2021 7:26 PM	Text Document	1 KB	
agent-config_original.txt	3/23/2021 7:26 PM	Text Document	1 KB	
chglst.vbs	3/23/2021 7:26 PM	VBScript Script File	13 KB	
pfisapi.conf	3/31/2021 12:02 AM	CONF File	6 KB	
postinstall.vbs	3/23/2021 7:26 PM	VBScript Script File	3 KB	
start_page_template.html	3/23/2021 7:26 PM	HTML File	3 KB	
uninstall.vbs	3/23/2021 7:26 PM	VBScript Script File	2 KB	

After Updating the config files update the Module in IIS .

Steps:

In the Internet Information Services (IIS) Manager, select the IIS server.

On the Features View tab, double-click Modules.

On the Modules screen, in the Actions area, click Add Managed Module.

On the Add Managed Module dialog, in the Name field, type a name, such as OpenTokenHttpModule.

In the Type field, enter the following:

OpenTokenModule.HttpModule, OpenTokenModule, Version=3.5.0.0, Culture=neutral, PublicKeyToken=f5ed9639debbca65

Kindly check the below link for more information.

[Adding the OpenToken HTTP Module in IIS \(pingidentity.com\)](http://pingidentity.com)

Once Module has been updated reset the IIS and launch the Application URLs.