PingFederate®

SSO Integration Overview

Ping Identity®

Part Number 3007-321
Version 6.0
April, 2009

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: http://www.pingidentity.com

Trademarks

Ping Identity, the Ping Identity logo, and PingFederate are registered trademarks of Ping Identity Corporation. All other trademarks or registered trademarks are the properties of their respective owners.

Disclaimer

This document is provided for informational purposes only, and the information herein is subject to change without notice. Ping Identity Corporation does not provide any warranties and specifically disclaims any liability in connection with this document.

Contents

Introduction

As a stand-alone server, PingFederate must be integrated programmatically with end-user applications and identity management (IdM) systems to complete the "first- and last-mile" implementation of a federated-identity network. The purpose of this document is to provide an overview of the various approaches to integrating systems and applications with PingFederate for browser-based Internet single sign-on (SSO). To enable both the Identity Provider (IdP) and Service Provider (SP) sides of this integration, PingFederate provides commercial integration kits, which include *adapters* that plug into the PingFederate server and *agents* that interface with local IdM systems or applications.

This document covers the integration kits available from Ping Identity for PingFederate. PingFederate also includes a robust software development kit (SDK), which software developers can use to write their own custom interfaces for specific systems. Please refer to the PingFederate *SDK Developer's Guide* for more information, available in the PingFederate distribution `sdk` directory and on the Ping Identity Web site (pingidentity.com).

Note: Ping Identity offers separate integration solutions for secure Internet SSO to Software-as-a-Service (SaaS) providers—SaaS Connectors, which include automatic user provisioning at the provider site. In addition, for integration with the PingFederate WS-Trust Security Token Service (STS), we provide a range of *Token Translators*. These plug-in Token Processors (for an IdP) and Generators (for an SP) connect the STS with Web Service Providers and Clients for access to identity-enabled Web Services.

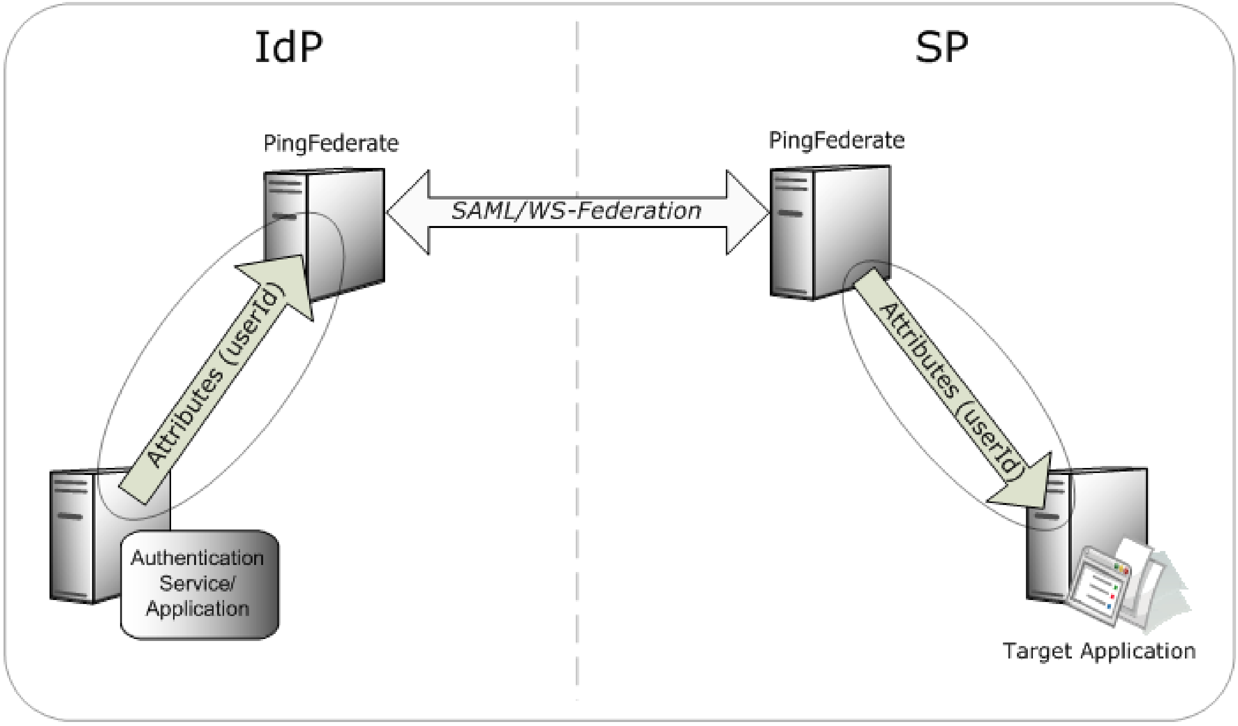
For more information about SaaS Connectors and Token Translators, look for links on the PingFederate Overview page at the Ping Identity Web site and refer to the current product documentation.

SSO Integration Concepts

For an IdP, the first step in the integration process involves sending identity attributes from an authentication service or application to PingFederate. PingFederate uses those identity attributes to generate a SAML assertion. (For information about SAML—Security Assertion Markup Language—refer to the PingFederate *Getting Started* manual.) IdP integration typically provides a mechanism through which PingFederate can look up a user's current authenticated session data (for example, a cookie) or authenticate a user without such a session.

For an SP, the last step of the integration process involves sending identity attributes from PingFederate to the target application. PingFederate extracts the identity attributes from the incoming SAML assertion and sends them to the target application to set a valid session cookie or other application-specific security context for the user.

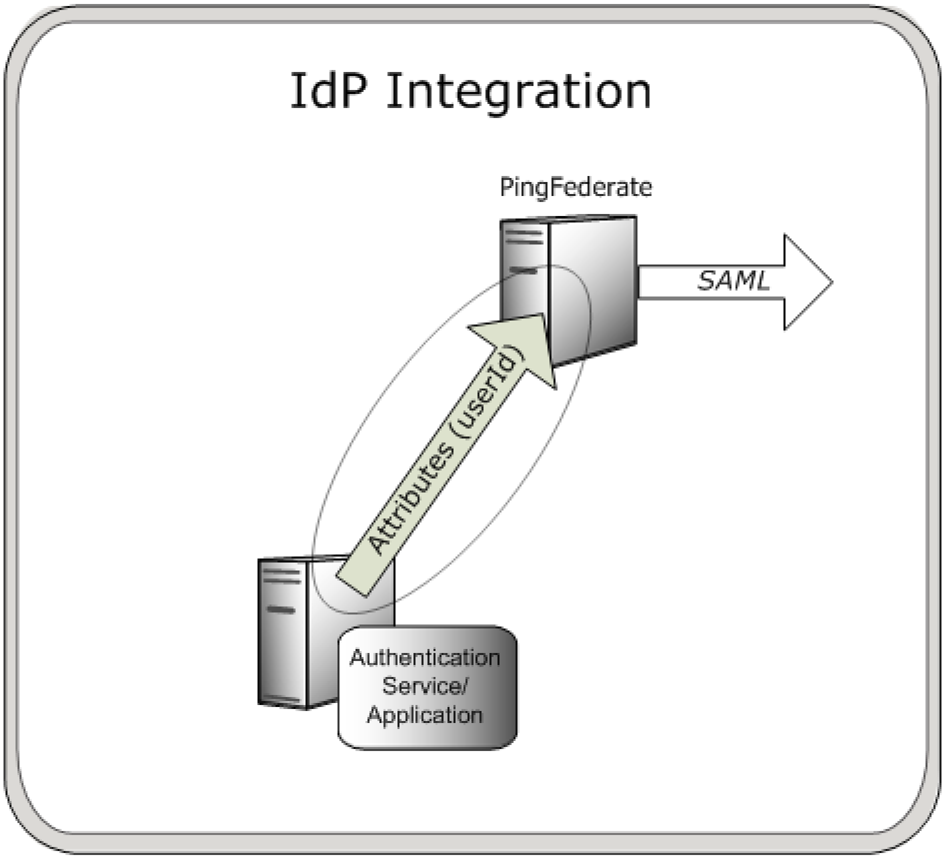
The following diagram illustrates the basic concepts of integration with PingFederate:



Identity Provider Integration

An IdP is a system entity that authenticates a user, or “SAML subject,” and transmits referential identity attributes based on that authentication to PingFederate. The IdP integration involves retrieving user-identity attributes from the IdP domain and sending them to the PingFederate server. Typically, the identity attributes are retrieved from an authenticated user session. For IdP integration, a number of attribute-retrieval approaches can be used, depending upon the IdP deployment/implementation environment. Ping Identity offers a broad range of commercial integration kits that address various IdP scenarios, most of which involve either custom-application integration, integration with a commercial IdM product, or integration with an authentication system.

Note: For IdPs implementing Internet SSO to Google Apps or Salesforce, PingFederate also provides for automated user provisioning. See details under Single Sign-on for SaaS Applications at the Ping Identity Web site.



Custom Application

A federation partner can use a custom authentication service or application to serve as the IdP role in that federation partnership. Integration with a custom application is handled through application-level integration kits, which allow software developers to integrate their custom applications with a PingFederate server acting as an IdP. Each application-level integration kit includes an agent, which resides with the IdP application and provides a simple programming interface to transfer session and attribute information from the application to the PingFederate IdP server.

Ping Identity provides custom-application integration kits for several programming environments, including:

- Java
- .NET
- PHP

Identity Management System

An IdP enterprise that uses an IdM system can expand the reach of the IdM domain to external partner applications through integration with PingFederate. IdM integration kits typically use the IdM agent API (if available) to access identity attributes in the IdM proprietary session cookie and transmit those attributes to the PingFederate server.

IdM integration kits do not require any development; integration with PingFederate is accomplished entirely through the PingFederate administrative console.

Ping Identity provides integration kits for many of the leading IdM systems including:

- CA SiteMinder
- Oracle Access Manager (formerly COREid)
- Tivoli Access Manager

Authentication System

Initial user authentication is normally handled outside of the PingFederate server using an authentication application or service. PingFederate authentication-system integration kits leverage this local authentication to access applications outside the security domain. These integration kits access authentication credentials that are validated against a Windows security context, which could be NTLM or Integrated Windows Authentication (IWA), and pass them to the PingFederate IdP server.

The X.509 Certificate Integration Kit uses the PingFederate security infrastructure to perform client X.509 certificate authentication for SSO to SP applications.

PingFederate also packages an LDAP Authentication Service Adapter and logon form that can authenticate users directly against an LDAP data store. This adapter may be used if your organization does not have a centralized local authentication service and your user stores are maintained by LDAP servers. On the IdP side, when the PingFederate IdP server receives an authentication request for SP-initiated SSO or the user clicks a link for IdP-initiated SSO, the IdP server invokes the LDAP adapter and prompts the user for local IdP credentials. The credentials are then compared against the LDAP server and, if they are validated, PingFederate generates a SAML assertion.

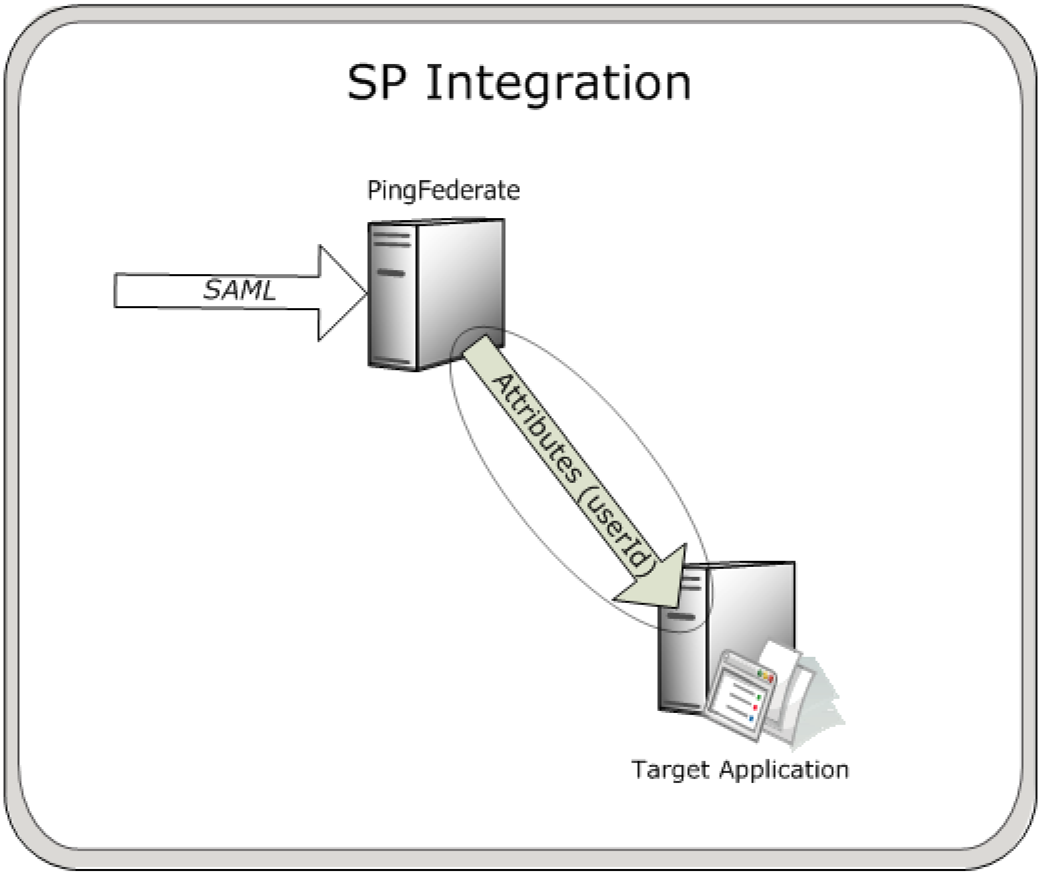
Authentication integration kits do not require any development; integration with PingFederate is accomplished entirely through the PingFederate administrative console.

Ping Identity offers integration kits for authentication systems including:

- IWA/NTLM
- X.509 Certificate
- LDAP Authentication Service

Service Provider Integration

An SP is the consumer of identity attributes provided by the IdP through a SAML assertion. SP integration involves passing the identity attributes from PingFederate to the target SP application. The SP application uses this information to set a valid session or other security context for the user represented by the identity attributes. Session creation can involve a number of approaches, and as for the IdP, Ping Identity offers commercial integration kits that address the various SP scenarios. Most SP scenarios involve custom-application integration, server-agent integration, integration with an IdM product, or integration with a commercial application.



Custom Application

Many applications use their own authentication mechanisms, typically through a database or LDAP repository, and are responsible for their own user-session management. Custom-application integration is necessary when there is limited or no access to the Web or application server hosting the application. Integration with these custom applications is handled through application-level integration kits, which allow software developers to integrate their applications with a PingFederate server acting as an SP.

With these integration kits, PingFederate sends the identity attributes from the SAML assertion to the SP application, which can then use them for its own authentication and session management. As for the IdP, application-level integration kits include an SP agent, which resides with the SP application and provides a simple programming interface to extract the identity attributes sent from the PingFederate server. The information can be used to start a session for the SP application.

Ping Identity provides custom-application integration kits for a variety of programming environments, including:

- Java
- .NET
- PHP

Server Agent

Server-agent integration with PingFederate allows SP enterprises to accept SAML assertions and provide SSO to all applications running on that Web and/or application server; there is no need to integrate each application. Since integration occurs at the server level, ease of deployment and scalability are maximized. Applications running on the Web/application server must delegate authentication to the server; if the application employs its own authentication mechanism, integration must occur at the application level.

With server-agent integration kits, PingFederate sends the identity attributes from the SAML assertion to the server agent, which is typically a Web filter or JAAS Login Module. The server agent extracts the identity attributes, which the server then uses to authenticate and create a session for the user.

SP server-agent integration kits do not require any development; integration with PingFederate is accomplished entirely through the PingFederate administrative console.

Ping Identity provides integration kits for many Web and application servers, including:

- Internet Information Services (IIS)
- Apache
- WebLogic
- WebSphere
- SAP NetWeaver®

Identity Management System

IdM integration with PingFederate allows an SP enterprise to accept SAML assertions and provide SSO to applications protected by the IdM domain. IdM integration kits typically use the IdM agent API (if available) to create an IdM proprietary session token based on the identity attributes received from PingFederate.

IdM integration kits do not require any development; integration with PingFederate is accomplished through the PingFederate administrative console and the IdM administration tool.

Ping Identity provides integration kits for many of the leading IdM systems including:

- CA SiteMinder
- Oracle Access Manager (COREid)
- Tivoli Access Manager

Commercial Application

Commercial-application integration with PingFederate allows an SP enterprise to accept SAML assertions and provide SSO to those commercial applications.

These integration kits do not require any development; integration with PingFederate is accomplished entirely through the PingFederate administrative console.

Ping Identity offers integration kits for these commercial applications:

- Citrix
- SharePoint
- Salesforce.com

  Note: For PingFederate 5.2 and later versions, the Salesforce.com Integration Kit is called the PingFederate Salesforce *Connector*. Connectors feature complete user provisioning, as well as SSO configuration templates, for SaaS providers.

Summary

The following table summarizes IdP- and SP-integration deployment scenarios and the Ping Identity integration kits that suit each scenario. Ping Identity continues to develop new integration kits; check the Ping Identity Web site (www.pingidentity.com) for the most up-to-date list of available kits.

Type	**IdP**	**SP**
Custom Application	• Java Integration Kit • .NET Integration Kit • PHP Integration Kit	• Java Integration Kit • .NET Integration Kit • PHP Integration Kit
Identity Management System (IdM)	• CA SiteMinder Integration Kit • OAM (COREid) Integration Kit	• CA SiteMinder Integration Kit • OAM (COREid) Integration Kit
Authentication System	• Windows IWA/NTLM Integration Kit • X.509 Certificate Integration Kit • LDAP Authentication System (Bundled with PingFederate)	N/A
Server Agent	• Integration Kit for SAP NetWeaver	• IIS Integration Kit • Apache Integration Kit • WebLogic Integration Kit • WebSphere Integration Kit • Integration Kit for SAP NetWeaver

Type	IdP	SP
Commercial Application	N/A	• Salesforce.com Connector • Citrix Integration Kit • SharePoint Integration Kit