PingFederate® 4.4

Release Notes

PingIdentity™

Part Number 3007-266
Version 4.4
April, 2007
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

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

PingFederate is the industry-leading federated identity server for enabling single sign-on to online services for employees, customers and business partners. No other federated identity solution is as easy to install, integrate and scale. PingFederate reduces complexity, cost, and time-to-production through guided configuration tools and the broadest range of turnkey application integration kits.

PingFederate is a stand-alone federation server that integrates and coexists with homegrown and commercial Identity Management deployments. As a result, enterprise-wide identity federation is achievable without extensive upgrades to entrenched Identity Management systems.

This PingFederate release includes both a Quick Start and a Demo. The Quick Start is intended to assist individuals new to PingFederate and federation protocols such as SAML v2.0 in the learning process. We recommend that all new users start with the Quick Start. The Demo is oriented towards more experienced individuals interesting in exercising PingFederate functionality and gaining a deeper understanding of an example adapter, the Back Channel Reference Adapter.

PingFederate

Key Enhancements for This Release

For a complete list of all enhancements for this version and previous releases see the Complete Change List section which contains references to additional documentation.

- Support for the GSA's E-Authentication v1.0 specification has been removed from PingFederate.

- Signed metadata files may now be imported into PingFederate. Similarly, metadata files generated by PingFederate may now be signed prior to distribution. During metadata file import, the public key used to verify the file signature may either be included in the `<KeyInfo>` element of the metadata file or located on the file system and selected by the administrator. PingFederate does not allow the importation of signed metadata file with invalid signatures. Note that PingFederate continues to support unsigned metadata files.

- Support for CRL checking is now included in PingFederate. Partner certificates, be they signature verification certificates, SSL certificates, or encryption certificates, may now be revoked. In order to be revoked, the certificate must reference a CRL endpoint. Further, the signature on the CRL must be verified using the CA's public key, which must be known to PingFederate. PingFederate does not allow revoked certificates to be used during runtime processing. Runtime exceptions may result from the use of a revoked certificate.

- The SOAP binding has been added to SAML v2.0 connections for both inbound and outbound messages.

- In deployments where PingFederate resides on a server with multiple network interfaces, it is now possible for PingFederate to listen for traffic on a specific interface. PingFederate recognizes three different types of messages: partner, administration, and cluster messages. Each type of message may be bound to a specific interface. Note that all three message types

may share the same network interface. This is the case when the server contains only a single network interface.

- The Main Menu and Local Settings wizard flows have changed. The Main Menu is now organized by federation role providing a more logical layout. The Local Settings section is now called Server Settings and has changed to include fewer steps. Other steps previously contained within Local Settings, such as IdP and SP Adapters, now appear on the Main Menu directly.

- PingFederate now supports a more expressive and flexible syntax for transforming values on the attribute mapping screens. This includes both the attribute contract fulfillment screens in an SP connection and the adapter contract fulfillment screen in an IdP connection. Called “Expression”, this new fulfillment source uses a Java-like syntax for creating more complex logic for values. The existing “Text” fulfillment source continues to be supported.

Installation and Configuration

Refer to the "Installation" chapter of the PingFederate *Administrator's Guide* located in the /docs directory of this distribution. Note that both the PingFederate server and the JDK must be installed in directories whose absolute paths contain no spaces.

If you are new to PingFederate, we recommend that you deploy the Sample Applications located in the /quickstart directory of this distribution. See the Quick Start “Introduction” section of this `README` below for more information.

Known Limitations

- If an IE browser is set to the highest security setting, the system navigation and pop-up windows might not work properly.

- Integration with a FIPS-140-2 approved Hardware Security Module has not been verified for this release.

- With both the Internet Explorer 7.0 and Mozilla 2.0 browsers, a user having open sessions with multiple SPs who performs an SLO over the Redirect binding may receive an error. Issuing an SLO request over the Redirect binding causes the user’s browser to be redirected between the IdP and each SP in turn resulting in a potentially large number of HTTP 302 Redirects. The number of redirects may exceed these browsers’ allowable redirect limit. When this limit is reached, the browser believes that a web site is mistakenly generating these redirects and displays the error.

  We recommend that for federation hubs that support users with multiple simultaneous open sessions, a binding other than Redirect be used for SLO.

- Due to a bug in Internet Explorer 6, users may receive a "HTTP 404 - File Not Found" error when being redirected between applications and PingFederate.

  Please see http://support.microsoft.com/default.aspx?scid=kb;en-us;843518 for more information.

The problem appears to be isolated to the situation where the PingFederate server and the application are running on different ports on the same machine. For instance, if PingFederate is running on 9030 and the application is running on 8080, then the redirect attempts to forward the user onto 9030, resulting in a 404 error. This is due to IE not handling the redirect request correctly.

Use of standard HTTP ports (80 & 443) should resolve the issue.

Known Issues

- PingFederate supplies a default set of roles with associated configuration permissions. It is possible for an administrator to circumvent assigned permissions by directly accessing URLs.
- The PingFederate system can enforce the masking of sensitive attribute values only within its own code base. External code such as adapter implementations and other product extensions may log attribute values in the clear even when they have been designated to be masked in the GUI. If sensitive attribute values are a concern when using such components, the logging level for the specific component can be adjusted in the log4j.xml file to the appropriate threshold to prevent attribute values from appearing in log files.
- When loading a configuration archive, users must ensure that the adapter and JDBC jars required by the configuration have been deployed to the server. Incomplete jar deployments may cause the PingFederate administrator console to crash and will prevent the server from handling SAML messages properly.
- Using the browser's navigation mechanisms (e.g., the Back button) will cause inconsistent behavior in the configuration UI. Use the navigation buttons provided at the bottom of screens in the PingFederate administrative console.
- Minor formatting and content discrepancies with online help. Please refer to the PingFederate Administrator's Manual in the \pingfederate\docs directory if more configuration information is needed.

Quick Start and Sample Applications

Introduction

The `/quickstart` directory in this distribution contains Sample Applications and a Quick Start Guide (in the /docs directory), which can be used to configure PingFederate to handle common use-case scenarios built into the Applications. We recommend that you follow configuration steps in the Guide as a means of becoming familiar with PingFederate and demonstrating federated Single Sign-on (SSO) (as well as other optional identity federation use cases).

Alternatively, the /quickstart/scripts directory provides a means of automatically configuring PingFederate to handle the Sample Application scenarios. You can use these scripts instead of following the manual steps or to correct quickly any errors that might have occurred during manual configuration. Refer to the *Quick Start Guide* for instructions on using the scripts.

For key concepts, detailed configuration information, and additional protocol background, consult the PingFederate *Administrator's Guide*.

Installation and Configuration

Refer to the "Installation" chapter of the Quick Start Guide located in the `quickstart/docs` directory of this distribution.

Known Limitations

- N/A

Known Issues

- N/A

Complete Change List by Released Version

For a list of updates and known issues to the Standard Adapter packaged in this distribution, see the `README.TXT` packaged in the Java and .NET Integration Kits posted for download at PingIdentity.com.

To assist your team with upgrades and staging QA, we refer to the applicable section in documentation or Support Resources for more information for the latest release.

PingFederate 4.4 – June 2007

- Removal of support for GSA's E-Authentication v1.0 specification
- Addition for support of signed metadata files (Manual: System Administration/Signing XML Files)
- Support for partner certificate revocation through CRLs (Manual: System Administration/Certificates, SSL, and XML Encryption)
- Increased flexibility around encryption of Name ID in SAML v2.0 SLO requests when the Name ID is encrypted within an assertion (Manual: Identity Provider Configuration/Configuring XML Encryption Policy)
- Support for the SOAP binding for both inbound and outbound SAML v2.0 messages (Manual: Identity Provider Configuration/Configuring Web SSO)
- Improved support for deployments where the server contains multiple network interfaces (Manual: System Administration/Changing Configuration Parameters)
- Usability enhancements to the Main Menu layout and Local Settings flow (Manual: Console Navigation/Using the Main Menu)

- More sophisticated attribute-fulfillment operations through support of a Java-like syntax for data manipulation (Manual: Identity Provider Configuration/Configuring Web SSO)
- Removal of extraneous credentials settings (“Encryption Certificate” and “Decryption Certificate”) for WS-Federation and SAML v1.x connections
- Improved display of long connection IDs on the Main Menu
- Inclusion of a demo application that complements the existing Sample Applications as described in the Quick Start Guide

PingFederate 4.3 – March 2007

- Virtual Server Identities allow PingFederate to use distinct protocol identifiers in the context of a particular partner connection.
- Additional customizable end-user error pages for 'page expired' and general unexpected error conditions.
- Increased flexibility by allowing for a list of additional valid host names to be used for incoming protocol message validation.
- Optionally, the SSO Directory Web Services can now be protected with HTTP basic authentication.
- New administrative console error page.
- Improved short-term state management memory utilization for improved system resiliency.
- Improved input-data validation and character-entity encoding of data when displayed--for protection against cross-site scripting attacks.
- An IdP connection configured to use only a single SP Adapter Instance will now ignore the URL-to-Adapter mapping step at runtime and just use the given adapter.
- Blocked directory indexing to limit browsing of static web content.
- Disabled unnecessary JRMP JMX port usage.
- Mitigated HTTP response splitting attacks by disallowing potentially dangerous characters in all redirects.

PingFederate 4.2 – December 2006

- Enhanced transaction logging functionality.
- Sensitive user attribute values can be masked in log files to enhance privacy considerations.
- The administrative console now runs on a distinct port from the runtime engine allowing for more flexible and secure deployment options.
- New filtering functionality on connection management screens enables easier management of large numbers of federation partners.

- Adapter SDK enhancements to facilitate file downloads.
- Usability refinements on X.509 certificate summary screens.
- Less verbose description of certificates in drop down boxes improve look and feel.
- Multiple partner endpoints of the same type can now be configured to use the same binding.
- Improved support for reverse proxy deployments.

PingFederate 4.1 – October 2006

- Liberty Alliance interoperability certified.
- SAML2 x509 Attribute Sharing Profile (XASP).
- Optional Hardware Security Module (HSM) mode, that enables storage of private keys and crypto processing on an external HSM unit that is FIPS-140-2 certified.
- Updated Protocol Configuration Wizard. Updated the flow and number of steps required to onboard a connection partner.
- Error handling templates that can be used to build SSO/SLO landing pages that communicate error status and support instructions to end users.
- Configuration options that enable multiple, simultaneous authentication profiles for the SOAP back-channel. These include HTTP Basic, SSL Client Certificates, and Digital Signatures.
- Digital signature capability for client authentication when using SAML 1.x.
- Pop-up server endpoint display that filters by role and configurations made.
- Two digital signature verification certificates can be assigned to a connection, allowing the partner flexibility in selecting one certificate or the other. When one certificate expires, the other certificate is used without the need for close synchronization.
- A run.properties configuration that allows an admin to specify an alternate port with which to communicate over the back-channel to partner's SAML gateway.
- Support for 32 & 64 bit machine architectures. See data sheet for specific platforms.

PingFederate 4.0 – June 2006

- Deploy multiple adapters as an IdP to look-up different session security contexts across security domains and applications.
- Save a partially completed connection as a draft.
- Copy a connection to rapidly set up other partners or test environments with similar configurations.
- Attribute source SDK enables retrieval of attributes from additional data source interfaces such as SOAP, flat files, or custom interfaces.

- Multi-administrator support. Select from default roles: User Admin, Admin, Auditor, and Crypto Admin.
- Ability to edit SP adapters that are in-use with target systems.
- Encrypt or decrypt entire assertions or select elements. This is of particular value when intermediaries may handle SAML traffic.
- Generate unique, Transient Name Ids each time the user federates to protect their identity.
- Enhanced Client/Proxy support for cell phone providers, smart card applications, and other client applications that interact with an authentication Proxy such as a WAP gateway.
- SAML 2 Compliant IdP Discovery mechanism that enables an SP to dynamically determine the appropriate IdP for the user.
- Integration Kits now provide additional methods that streamline passing of authentication context from an IdP to an SP.
- Single log-out across all connections and protocols that support SLO.
- Using an affiliate id, an SP can instruct an IdP to re-use the same persistent name identifier that was already used at other applications within the portal.
- Non-normative support for SP Initiated SSO with SAML 1.x protocols.

PingFederate 3.0 – November 2005

- This version contains several fixes for LDAP and JDBC connectivity.

PingFederate 2.1 – July 2005

- Patched a concurrency bug in the XML security library.
- Patched a memory leak in the XML-to-object binding library.
- Removed the core protocol processor's reliance on a workflow engine to resolve a memory leak and improve overall performance.
- Fixed a subtle memory leak in the module that tracks assertions in order to prevent replay in the POST profile.
- Updated the default server SSL certificate (extended the expiration date).

PingFederate 2.0 – February 2005

- Initial release.