PingFederate 6.2®

Release Notes

PingIdentity®

PingFederate 6.2 *Release Notes*
February, 2010

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: 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 solution for enabling secure Internet single sign-on (SSO) to online services for employees, customers, and business partners. In addition, the PingFederate Internet-Identity Security Platform provides cross-domain user provisioning and a WS-Trust Security Token Service (STS), which allows user access to identity-enabled Web Services.

This PingFederate release includes separate quick-start applications and an accompanying *Quick-Start Guide* for Internet SSO. The applications and other quick-start components provide a means of rapidly setting up a working, end-to-end identity federation for demonstration purposes. In addition to setup instructions, the *Guide* provides the reader with a view of relevant PingFederate administrative-console settings, plus instructions on configuring further options. We recommend that all users new to federated identity or PingFederate start with the *Quick-Start Guide*.

PingFederate Notes

Major Enhancements for This Release

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

Logging Enhancements

PingFederate logging capabilities have been extended. These enhancements include:

- New audit log for SSO events.

  The following SSO elements are available and are independently configurable for inclusion in the audit log: Transaction Time, Event, User, Source IP, Host, Application URL, Protocol, Federation Role, Partner ID, Attributes, Status, Local SP User.
- Support for writing all PingFederate logs to a separate file server.
- New logfilter utility that allows multiple server logs on the same server to be filtered by user session.
- The tracking ID, which allows tracking of all of the requests for a single user's session across that session, has been reformatted for readability and is included by default in the server log.

Enhanced Automated Configuration Migration

This PingFederate release extends support for configuration migration via the existing command-line tool, configcopy, which previously supported connection and adapter management. These enhancements include:

- Support for moving Trusted CA certificates.
- Support for creating a key pair and a self-signed certificate at the target including the key type, key strength, algorithm, and expiration date. Certificate metadata can be specified during key creation.

- Support for export of a Certificate Signing Request (CSR) for a specified key and import of a CA-issued certificate for the CSR.
- Support for listing key references for all keys, as well as by key type.
- Support for managing import and export of a configuration archive for source and target servers.
- Support for moving ancillary deployment files, including runtime, LDAP, and provisioner logging properties. Support for import of a private key contained in a pkcs12 password-protected file. The password may be specified via an obfuscated input configuration file or obfuscated command-line entry.

JDBC Express Provisioning

JDBC Express Provisioning has been extended to support Microsoft SQL Server identity columns.

LDAP Authentication Adapter Logout Endpoint

The bundled LDAP Authentication Adapter supports a new logout endpoint, which allows the adapter logout functionality to be invoked independently of the normal PingFederate single logout (SLO) process. This allows an Identity Provider (IdP) PingFederate user session to be terminated when a local logout occurs at a Service Provider (SP) who does not support SAML (Security Assertion Markup Language) SLO. The SP must provide a configurable redirect URL so that the LDAP Adapter logout endpoint can be invoked.

Direct IdP-to-SP Adapter Mapping

A new application endpoint in PingFederate allows for IdP adapter attributes to be mapped directly into SP adapters to facilitate special, nonstandard use cases. User attributes from an IdP are used to create an authenticated session or security context at an SP running on the same PingFederate server, without the configuration complexity, certificate maintenance, and performance overhead of a loopback SAML connection in the middle.

Other Updates and New Features

The following additional enhancements and other changes are available with this release:

- For server clustering, the default Inter-Request State Management methodology is now group RPC-based instead of cookie-based (see more information under “Upgrading PingFederate,” below).
- Added ability to extract Common Name (CN) from Distinguished Name (DN) for provisioner attributes.
- Added ability to extract username from email address for provisioner attributes.
- In Luna HSM mode, added the ability to specify the location to store Trusted CA certificates, either in the Sun Java key store or the Luna HSM.

  The Luna HSM has an 80-object limit due to limitations in the Luna JSP. To mitigate this 80-object limitation, Trusted CA certificates can be stored in the Sun Java key store, while all other certificates and keys, i.e., SSL, signing, and verification certificates, are stored in the Luna HSM.
- Corrected a number of customer-reported defects in previous releases.

Installation and Configuration

Refer to the "Installation" chapter of the PingFederate *Getting Started* 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.

Upgrading PingFederate

Note: License keys for Version 4 or 5.x of PingFederate cannot be used with Version 6.x. Request a new license key by contacting your Ping Identity representative or by visiting http://www.pingidentity.com/support-services/licensing.cfm.

This version of PingFederate is designed for compatibility with configuration archives created by PingFederate 4 and PingFederate 5 servers. When upgrading using a configuration archive, this version of PingFederate is designed to fall back to default settings for configuration options not previously available (and therefore, not specifically set) in PingFederate 4 or PingFederate 5 servers. These defaults are considered reasonable but may not be the desired setting for certain customer deployments. We recommend that all server settings and configurations be reviewed following the deployment of such a configuration archive.

Note: To take full advantage of a few new features, configuration archives from prior versions may need manual adjustments before being deployed into the current version of PingFederate. For more information, contact Ping Identity Support.

For information on how to generate and deploy configuration archives, refer to the "System Administration" chapter of the PingFederate *Administrator's Manual* located in the `/docs` directory of this distribution.

Configuration archives created prior to PingFederate 4 may not be compatible with this version of PingFederate. No testing was performed using older configuration archives and no statement regarding their use is made.

Inter-Request State Management

In server-clustering mode, this version of PingFederate uses Group RPC-based session tracking by default. If you are using an alternative method or the previous default (cookie-based) for inter-request state management and wish to continue to do so, you must specify the desired service in the `hivemodule.xml` file. (For more information, refer to the PingFederate *Server Clustering Guide*.)

Google SaaS Provisioning

This version of PingFederate uses a newer version of the Google Apps provisioning API. Only the Google Apps Connector 2.0 (or higher) is compatible with this version of PingFederate. Connector versions prior to 2.0 must be upgraded.

Mutual TLS for SOAP/Artifact Binding

With this version of PingFederate, TLS renegotiation has been disabled by default for all HTTPS listeners/connectors. This change (due to security considerations) affects only those customers who have partners making use of inbound mutual SSL/TLS authentication for the SOAP or artifact SAML bindings. In such cases, administrators will need to reconfigure `run.properties` to enable the secondary HTTPS port, and ensure that the `jboss-service.xml` `needClientAuth` or `wantClientAuth` flag is set to true so that PingFederate will ask for a certificate during the initial handshake. The affected partners will also need to update their configuration to use the new endpoint. (For more information, please refer to the section "Changing Configuration Parameters" in the PingFederate *Administrator's Manual.*)

SSL Cipher Suite Changes

In this version of PingFederate, several "weaker" cipher suites previously permitted for the SSL handshake are no longer allowed by default. However, deploying a configuration archive built on a previous version of PingFederate will allow the server to continue support of weaker cipher suites. For information about which cipher suites the PingFederate no longer supports, see the commented-out suites in the `com.pingidentity.crypto.SunJCEManager.xml` file in `<pf_install>/pingfederate/server/default/data/config-store.`

Importing Application Authentication Settings

A PingFederate security enhancement provides finer-grain control over services available to local applications. These services encompass a variety of capabilities many customers find useful. Specifically, these services include:

- Attribute Query
- JMX
- Connection Management
- SSO Directory Service

On a new PingFederate installation, by default only the SSO Directory Service is active. Requests from client applications for any inactive PingFederate service are rejected. Depending upon specific deployment needs, each of these services can be individually configured after installation.

Data archives created from a previous version of PingFederate may not contain sufficient information for the server to provide the expected behavior. PingFederate attempts to configure client authentication settings for services as a best-effort. However, we recommend that an administrator with Crypto Admin permissions review the "Application Authentication" settings and determine whether further manual configuration is needed to achieve the desired result. For more information, consult the *Administrator's Manual.*

Deploying the Standard Adapter

Starting with PingFederate 5, the installation process no longer deploys the Standard Adapter (pftoken). For PingFederate deployments using the Standard Adapter, you must perform additional steps to complete migration. These steps vary depending upon which Standard Adapter version the current PingFederate deployment uses.

If Standard Adapter 1.1 or 1.2 is deployed in the PingFederate instance, copy the Standard Adapter JAR file, pf4-pftoken-adapter-1.*.jar, from the following location for the source PingFederate instance to the same location for the target PingFederate instance:

```
<pf_install>/pingfederate/server/default/deploy
```

The adapter will be available for use by PingFederate 6 after you restart the server. Note that Standard Adapter 1.3 is backwardly compatible with integration kits that use Standard Adapter 1.1 and 1.2.

The Standard Adapter 1.3 is *not* backwardly compatible with applications that integrate with PingFederate using the Standard Adapter 1.0. If existing applications rely upon this version, then you may choose to continue using it in PingFederate 6. To do so, copy the Standard Adapter 1.0 JAR file from your PingFederate 4 instance to the same deployment location given above.

The JAR file, pf4-pftoken-adapter-1.0.jar, can be found at:

```
<pf4_install>/pingfederate/server/default/deploy
```

For PingFederate clusters containing multiple instances of the server, repeat these steps as needed to deploy the correct version of the Standard Adapter on each instance.

Updating LDAP IdP Adapter Settings

Due to configuration differences between the LDAP Authentication Service 1.0 and LDAP Authentication Service 2.1 IdP adapters, importing a configuration archive containing LDAP 1.0 IdP-adapter instances requires manual intervention. For each adapter instance, an administrator must manually reselect the adapter attributes used to derive a user's Pseudonym (see the *Administrator's Manual*: LDAP Adapter Configuration).

Known Limitations

- Depending on deployments, cookies used by default for state management in a PingFederate cluster can become large enough to exceed size limits set by Internet Explorer. There is at least one known configuration in which this occurs, although there may be others. The known configuration is a configuration in which the "X" cookie is being used for state management in the cluster, and in which Account Linking is turned on in one (or more) connection(s). In this configuration, the "X" cookie may become very large. Some browsers will send oversize cookies anyway, which will crash the PingFederate Jetty container. To avoid this limitation, where applicable, use Group RPC-based state management or in-memory state management instead (see the PingFederate *Server Clustering Guide* in the installation docs directory).
- If an IE browser is set to the highest security setting, navigation in the administrative console and pop-up windows might not work properly.
- With Internet Explorer 7.0 and Mozilla 2.0 browsers, a user with open sessions across multiple SPs may receive an error when attempting to perform a single logout (SLO) via the Redirect binding. 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.

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

- On the "Adapter Contract Fulfillment" (IdP Connection) and "Attribute Contract Fulfillment" (SP Connection) screens, attributes cannot contain multi-line expressions, since the Enter key has a specific meaning within PingFederate. A workaround to this limitation is to write the expression in an external editor and then cut and paste the expression into the textbox provided.
- When running as a Windows service, the `NET START` command reports success based upon the ability of the JBoss container to start. This report may not be accurate because the PingFederate server is started by JBoss after `NET START` reports success. An administrator should examine the PingFederate `server.log` file for complete information regarding server status.
- When LDAP authentication is the configured administrative console authentication method, PingFederate does not lock out administrative users based upon the number of failed logon attempts. Responsibility for preventing access to the administrative console is, in this case, delegated to the LDAP server, and is enforced according to the password lockout policy settings maintained by that LDAP server.
- Hypertext cross-reference linking is available between sections in the PingFederate *Getting Started* and *Administrator's Manual* PDFs. However, Adobe Reader 8.x does not have the equivalent of a browser's "back/forward" navigational arrows enabled by default, making it difficult to return to a page view after clicking a hyperlink, particularly if the previous view is in a different PDF. To enable this navigational feature in Adobe Reader, click **Tools** in the top menu, then choose "Customize Toolbars…". In the **More Tools** dialog, scroll down to "Page Navigation Toolbar" and select the "Previous View" and "Next View" checkboxes.
- For a scenario involving SP-initiated SLO with multiple SPs in which the initiating SP is using a SOAP binding and the other SPs are using one of the front-channel bindings (Artifact, Redirect or POST) along with a front-channel adapter within the IdP, logout with the front-channel adapter will fail. When logout fails with the adapter (a technical limitation, since with SOAP-based SLO, the server does not have access to the browser to kill a session established with a front-channel adapter), any other IdP adapters that are configured for the connection, and for which logout needs to occur will not be invoked for logout. This includes back-channel (e.g., SOAP-based) adapters.
- When loading a configuration archive, users must ensure that all JAR files required by the configuration have been deployed to the server, including those for adapters, connectors, token translators, and JDBC and custom data stores. Incomplete JAR deployments may cause PingFederate to work improperly.
- Deploying a new library file to the PingFederate deploy directory requires a PingFederate server restart to pick up the change in configuration. This includes deployment of adapters, connectors, token translators, and JDBC and custom data stores, and any other libraries.
- Using the browser's navigation mechanisms (e.g., the **Back** button) will cause inconsistent behavior in the administrative console. Use the navigation buttons provided at the bottom of screens in the PingFederate console.
- Modifications to an LDAP data-store configuration on the PingFederate Manage Data Store screen do not propagate to an existing LDAP Authentication Service Adapter. In order to propagate the change, the adapter configuration must be resaved from the Manage Adapter Instances screen.
- If you upgrade from a version of PingFederate prior to 5.2 to the current version by deploying a data archive created in your existing installation, you will overwrite the configuration of a new data store used for SaaS provisioning. You can recover the configuration for this data store, but

please note that it is a default for initial setup and demonstration only and *not* recommended for production, due to reliability and performance issues (see the PingFederate *Administrator's Manual* for more details).

To recover the data store, copy the following XML snippet below (everything between ---snip start--- and ---snip end---) into the `pingfederate/server/default/data/pingfederate-jdbc-ds.xml` file, within the `<datasources>` element.

---snip start---

```
<local-tx-datasourcemaskAttributeValues="false">
      <description>jdbc:hsqldb:${jboss.server.data.dir}${/}hypersonic${/}ProvisionerDefaultDB</description>
      <jndi-name>ProvisionerDS</jndi-name>
      <connection-url>jdbc:hsqldb:${jboss.server.data.dir}${/}hypersonic${/}ProvisionerDefaultDB</connection-url>
      <driver-class>org.hsqldb.jdbcDriver</driver-class>
      <user-name>sa</user-name>
      <password>dezQ6UjcMUu35oG/nZD4cA==</password>
      <ping-db-type>Custom</ping-db-type>

</local-tx-datasource>
```

--- snip end---

After this, you can enable SaaS Provisioning on the Server Settings/Roles & Protocols screen (providing you have a license for provisioning). This will enable the SaaS Provisioning screen in the Server Settings task flow. Navigate to this screen and select the data store that you defined in the previous step.

- Editing connections configured for both Google and Salesforce SaaS Provisioning will cause the administrative console to quit unexpectedly unless both Provisioning plug-ins exist within the PingFederate installation. This problem occurs only when the original configuration included both plug-ins and one of them has been removed, or when standing up a new PingFederate instance in which all required libraries have not yet been copied. In this case, the administrator is allowed to edit the connection, but PingFederate will halt when the administrator attempts to save the changes. To prevent this, please ensure before editing a connection that all required plug-ins (JAR files) are deployed.
- Only Google Apps Connector versions 2.x and higher are compatible with PingFederate 6.2 and higher.
- During upgrades from a PingFederate version of either 4.2 or 4.3 (the issue has been verified with these versions, but there may be others) to the current version, SAML 1.1 IdP connections will have the incoming SOAP binding set to true, even though this is not a UI-configurable option for SAML 1.1 in any of the versions listed above. The UI will not allow you to edit/save the connection until you resolve the SOAP configuration dependencies. This is a defect in the way that the older versions of PingFederate store the default binding value for SOAP. Later versions of PingFederate cannot resolve the issue, as they do not know that the default binding value for SOAP should not be set to true, since true is a valid option for this value.

- If you make changes to the Trusted CAs for a running PingFederate installation, those changes will not take place for LDAPS connections until the server has been restarted, because of the way that the container manages LDAPS connections.
- If you run PingFederate under JDK 1.5 (supported only on Windows Server 2003) and you enable, disable, and re-enable the JMX Service endpoint, the service will not restart. This is a known issue in JDK 1.5, causing the service to hold on to the JMX port. To work around this issue, you can reboot the PingFederate server or install and use JDK 1.6, in which the issue is fixed.
- If authenticated to the PingFederate administrative console using certificate authentication, a session that has timed out may not appear to behave as expected. Normally (when using password authentication), when a session has timed out and a user attempts some action in the console, the browser is redirected to the login page and then to the Main Menu once authentication is complete Similar behavior applies for certificate authentication, in principle. However, since the browser may automatically resubmit the certificate for authentication, what appears to happen is that the browser is redirected immediately to the Main Menu.
- If you have specified either an IdP or an SP connection that is configured to support only WS-Trust STS, the Browser SSO protocol will automatically be set to SAML 2.0 even though the Browser SSO protocol is not used for STS-only connections. If you add Browser SSO support to this connection at a later time, the connection must use SAML 2.0.

Note: The remaining items in this list concern limitations that apply to the use of the PingFederate configuration-migration scripting tool, configcopy.

- If you are using the configcopy tool and do not yet have your organizational SSL certificate installed and in use for the PingFederate server, you may encounter an error preventing you from retrieving the configuration from the source PingFederate (or you may be unable to write to the target server). Please refer to the *Administrator's Manual* (in the Security Management chapter) for information on managing SSL certificates. There are several mechanisms provided to allow you to connect to either the source or the target or both.
  - (Recommended) You can install the Issuer certificate for the PingFederate SSL certificate in a separately managed trust store. Then the location of the file that configcopy can be specified either in a properties file or via a command-line parameter when executing configcopy, for either or both servers.
  - Alternatively, you can install the Issuer certificate for the PingFederate SSL certificate into the trust store for the JDK under which configcopy runs.

  Please note that if you have a different SSL certificate installed on the source server than on the target, the configcopy tool must be able to trust both SSL certificates. In this case, both SSL certificates will need to be installed in the trust store used by configcopy, or in the trust store for the JDK under which configcopy runs.
- The configcopy tool does not currently perform any validation of either the correctness or the format of override parameters when updating the target PingFederate instance. Ensure that override parameters are accurate and supplied in a valid format.
- If you are using configcopy to copy all connections, channels, data sources, adapters, or token translators and you choose to set override properties, the override will be applied to all instances. It is recommended that you use care when applying overrides for copy-all operations.

- The configcopy tool supports copying only a single reference for each of the following that are defined for a given connection: adapter, data source, Assertion Consumer Service URL, Single Logout Service URL, and Artifact Resolution Service URL. If you have multiple adapters, data stores, or any of the aforementioned service URLs associated with a given connection, only the first reference to each will be copied.
- The configcopy tool does not support creation of configuration data that does not exist in the source. If you choose to set an override parameter for a parameter that does not exist in the source configuration, the behavior of the target system is not guaranteed.
- If you are using configcopy to copy connection configurations from a source to a target PingFederate installation, all of the adapters, data stores and keys referenced by that connection *must* already exist at the target. (Adapter and other plug-in configurations may be copied using configcopy before or in conjunction with copying the connection configuration. Keys must be created at the target in advance.). Property overrides for the connection-copy command should then be used to modify the references to these entities, as needed, when copying the connection to the target, since the instance IDs for each of these may be different at the target than they are at the source. Refer to the Administrator's Manual "System Administration" chapter for more information.
- The configcopy tool, when used for copying plug-in configurations (including adapters, token translators, and custom data stores), does not currently support overrides of complex data structures, including tables, extended contract attributes, and masked fields.

Known Issues

- When specifying *-logoutput* or *-outputfile* for the logfilter utility, the base directory constructed for relative paths will differ between operating systems. Below are the directories used when relative paths are defined for the logfilter:
  - Windows: <pf-install-dir>/pingfederate
  - Linux: <pf-install-dir>/pingfederate/bin
- PingFederate 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.
- On the "Attribute Requester Mapping" screen accessed from the Main Menu under "My SP Configuration" when SAML v2.0 is enabled, it is possible to map inactive connections. It is also possible to delete connections that are mapped on this screen.
- A connection in an error state cannot be deleted until all errors are corrected.
- If SaaS Provisioning for Salesforce is enabled for your installation and you wish to configure this feature after deploying the Quick-Start Applications, you must first deactivate and delete the "Demo IdP" and "Demo SP" connections in the administrative console.
- If you have a session with the PingFederate administrative console and the session expires, clicking any link will redirect your browser to the session-timeout page (as expected) and will

also log a stack trace in the server log file. Click the "restart" link to resume your session, which will take you back to the login page.

- When editing OGNL expressions used in Express User Provisioning scenarios, when you have multiple identical target attributes, all of which are fulfilled via expressions, there are two issues that you may encounter when updating the values of the expressions:
  - If you click on the Edit link for the value of the expression for the first identical Target Attribute, enter a value, and then click on the update link (which will send you back to the Attribute Fulfillment page), the previous values that you had entered for the other (subsequent) instances of the same Target Attribute will now be empty. The work-around for this is to enter the values for the (now) empty expressions on the Attribute Fulfillment page, rather than clicking on the Edit link to enter the values. You may still click on the Edit link to be able to test your values, but you will be required to re-enter the values for the subsequent identical Target Attribute instances when you click the Update link to go back to the Attribute Fulfillment page.
  - If you click on the Edit link for the value of the expression for any of the subsequent identical Target Attribute instances, enter a value, and then click on the update link (which will send you back to the Attribute Fulfillment page), the value that you had entered will not be saved in the Value column for that Target Attribute. The work-around for this is to enter the value for the expression for the Target Attribute that you wish to change on the Attribute Fulfillment page, rather than clicking on the Edit link to enter the values. You may still click on the Edit link to be able to test your values, but you will be required to re-enter the value for that Target Attribute instance when you click the Update link to go back to the Attribute Fulfillment page.

    Note that the conditions causing this issue should be rare.
- When using Internet Explorer, rendering of the tasks in the top navigation bar in the UI may occur outside the frame of the application if there are a large number of tasks. All tasks are still available for selection, and the user can still navigate within the current configuration.
- When PingFederate is acting as a WS-Trust STS, if it receives a request on the STS endpoint with the namespace element set to an invalid value of http://schemas.xmlsoap.org/ws/2005/02/trust/(i.e., with a trailing slash), it will not normalize this to the valid namespace of http://schemas.xmlsoap.org/ws/2005/02/trust (i.e., without the trailing slash) and will fail the transaction. In this case, the work-around is to have the client set the namespace element to the valid namespace of http://schemas.xmlsoap.org/ws/2005/02/trust.
- If authenticated to the PingFederate administrative console with a client certificate, a session that has timed out may fail upon re-authentication if an administrator had been editing a connection. If this happens, you must restart the session.
- If you are editing an IdP connection configured to support LDAP Express Provisioning and the connection to the LDAP server fails, the PingFederate administrative console will also fail. In this case, correct the issue that caused the connection to the LDAP server to fail and re-authenticate to the administrative console.
- When using configcopy to copy connection data, any SOAP SLO endpoints that have been defined in the source will not be copied to the target, even if the SOAP SLO endpoint is the only SLO endpoint defined at the source. These must be manually added to the target.

- If you create a connection via metadata import and then start to edit Protocol Settings (which are preconfigured based on the metadata that was imported) and click Cancel, the Protocol Settings will be lost. To recover the original Protocol Settings configuration, you will need to delete the current connection and create a new one via metadata import. If you need to edit Protocol Settings, you may do so, but ensure that you do not cancel before saving the configuration (regardless of whether you actually make changes).
- When a Failsafe Attribute Source is configured, the failsafe mapping is used only when all of the mappings configured in the data-store setup fail to return values for any reason. If any mapping succeeds (an attribute mapped to text, for example), failover does not occur.
- When using LDAP filters to select users for SaaS provisioning, error messages may be logged for other users in the Base DN that do not match the filter. These errors can be ignored; users are provisioned correctly.
- LDAP referrals will return an error and cause provisioning to fail if the User or Group objects are defined at the DC level, and not within an OU or within the Users CN.
- The `request.log` does not write to the `pf.log.dir` location defined in run.properties. The `request.log` is always written to the default location `<pf-install>/pingfederate/log`.
- On the Federation Info screen under Server Settings, the PingFederate Base URL must not end with a trailing slash.

Deprecated Feature

SP Affiliations is a deprecated feature. We are considering removal of this feature in future releases. The following limitations are known to exist within the SP Affiliations feature of PingFederate:

> If the SP sends an AuthnRequest to the IdP, the IdP will honor any affiliation request by the SP and will provide an assertion response that contains an SPNameQualifier attribute filled out as requested by the SP in the AuthnRequest. This attribute will be provided regardless of whether SP Affiliations are enabled or configured within the PingFederate IdP instance.

Quick Start Notes

Introduction

The `/quickstart` directory in this distribution contains quick-start 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 read the *Guide* as a means of becoming familiar with PingFederate and testing secure Internet single sign-on (SSO), as well as other optional identity-federation use cases.

For key concepts, detailed configuration information, and additional protocol background, consult the “Key Concepts” chapter of the PingFederate *Administrator's Manual.*

Installation and Configuration

Refer to the "Getting Started" chapter of the *Quick-Start Guide* located in the `quickstart/docs` directory of this distribution.

Known Limitations

N/A

Known Issues

Auto-Connect functionality requires that partner SSL server certificates be signed by a trusted Certificate Authority (CA). The SSL server certificate packaged with the Quick Start is self-signed, so the certificate is also included as a trusted CA. (**Important**: This is for testing only. In a production environment, you must remove all self-signed certificates included with Quick Start from the Trusted CAs.) However, changes to the PingFederate trusted CA store, as they relate to Auto-Connect, do not take effect until the PingFederate server is restarted. Therefore, after deploying the Quick Start configuration archive, restart the server prior to issuing an Auto-Connect request from the SP Quick-Start application.

Complete Change List by Released Version

PingFederate 6.2 – February 2010

- Added IdP-to-SP adapter mapping, which allows user attributes from an IdP adapter to be directly mapped to an SP adapter on the same PingFederate server to create an authenticated session or security context, without the need to generate SAML messages in between (see *Administrator's Manual*: System Settings).
- Provides enhanced logging capabilities including a new audit log, logfilter utility, and ability to log to any accessible file-server directory (see *Administrator's Manual*: System Administration)..
- Provides enhanced support for configuration automation including certificate and key management, configuration archive management, and ancillary deployment files (see *Administrator's Manual*: System Administration).
- Extended JDBC Express Provisioning to support MS SQL Server Identity column types (see *Administrator's Manual*: Service Provider SSO Configuration).
- Added a Logout Endpoint to the LDAP Authentication Adapter (see *Administrator's Manual*: LDAP Adapter Configuration)
- In clustered mode, the default Inter-Request State Management methodology is now group RPC-based instead of cookie-based (see the *Server Clustering Guide*).
- Added ability to extract CN from DN and extract username from email address for provisioner attributes (see *Administrator's Manual*: Identity Provider SSO Configuration).
- In Luna HSM mode, added the ability to specify the location to store Trusted CA certificates, either in the Sun Java key store or the Luna HSM (see the configuration file

`org.sourceid.config.CoreConfig.xml` in the `pingfederate/data/config-store` directory).

PingFederate 6.1 – September 2009

Note: The PingFederate 6.1 release includes the features described below as well features that were added in a limited-distribution "Preview" release, described in the next section.

- Provides support for simplified PingFederate Express connection configuration and export (see *Administrator's Manual*: IdP SSO Configuration).
- Extends support for configuration automation, including listing, copying, and updating features for SaaS Provisioning channels and for Token Translators (see *Administrator's Manual*: System Administration).
- Provides enhanced support for SaaS Provisioning Health and Status Monitoring via JMX (see *Administrator's Manual*: System Settings).
- Provides licensing enhancements including support for organizational licenses, licenses that contain international characters, and Web based license import (see *Administrator's Manual*: System Administration).
- Enhances the trust model to include support for anchored certificates, which allows certificates to be included in federation-transaction messaging and used for signature verification if, the given certificate matches the registered Subject DN and is issued by a certificate authority registered as a Trusted CA with PingFederate (see *Administrator's Manual*: Key Concepts).
- Supports "SP Lite", "IdP Lite", and "e-Gov" Liberty Interoperability profiles for SAML 2.0.

PingFederate 6.1-Preview – June 2009

- Provides support for Express Provisioning to a JDBC data source (see *Administrator's Manual*: SP SSO Configuration).
- Extends support for configuration automation, including listing, copy and update features for data stores and server settings (see *Administrator's Manual*: System Administration).
- Supports certificate-based authentication to the PingFederate administrative console (see *Administrator's Manual*: System Administration).
- Added UI-based data-archive deployment, as well as better error handling for common errors encountered (see *Administrator's Manual*: System Administration).
- Supports mapping of attributes passed in via a WS-Trust STS request to the outgoing token (see *Administrator's Manual*: WS-Trust STS Configuration).
- Supports logging of a transaction ID associated with every log entry for a given request to the PingFederate server.
- Corrects defects reported by customers in the previous release.

PingFederate 6.0 – March 2009

- PingFederate now includes a WS-Trust Security Token Service (STS), enabling organizations to extend identity management to Web Services. The PingFederate STS shares the core functionality of PingFederate, including console administration, identity and attribute mapping, and certificate security management (see *Getting Started*: WS-Trust STS Configuration).
- PingFederate extends support for configuration automation, including connection management and adapter management via the existing command-line tool (see *Getting Started*: Installation).
- PingFederate supports enhanced connection based licensing capabilities.
- PingFederate provides transaction based licensing capabilities for evaluation phase license enforcement.
- PingFederate allows administrators to specify the use of a separate certificate that is used for access to the administrative console and a different certificate for runtime processing. (see *Administrator's Manual*: System Settings)
- PingFederate supports configuration of LDAP Groups who are allowed access to the PingFederate Admin application based on PingFederate defined roles (see *Administrator's Manual*: System Administration).
- PingFederate supports definition of LDAP data stores such that the connection URI for multiple LDAP servers can be specified as the connection string for that LDAP data store (see *Administrator's Manual*: System Settings).
- PingFederate supports the Virtual List View (VLV) paging mechanism for retrieval of subsets of large result sets returned from the source LDAP data store during the provisioning process. This can significantly enhance performance for retrieval of data from Sun Directory Server (SDS) and similar LDAP servers that support VLV paging.
- PingFederate now stores the PingFederate software version within the configuration store.
- A number of defects reported by customers that existed in the previous release of PingFederate were addressed.

PingFederate 5.3 – December 2008

- PingFederate can be run as a service on Windows 64-bit platforms in addition to Windows 32-bit platforms and Linux platforms (see *Getting Started*: Installation).
- PingFederate now supports deployment of SaaS Provisioning plug-ins (JAR files) via a separate installation package (documented in Connector packages).
- PingFederate now supports automating configuration via a command line utility for connection management (see *Administrator's Manual*: System Administration).
- PingFederate now supports capabilities for monitoring and control of the SaaS Provisioning configuration and data via a command line tool (see *Administrator's Manual*: System Administration).
- PingFederate now supports validation of certificate revocation information via OCSP (see *Administrator's Manual*: System Settings).
- PingFederate can now be deployed on Java 6 (JDK 1.6) platforms.

- PingFederate supports access to additional parameters on both the IdP side and the SP side via OGNL expressions (see *Administrator's Manual*: IdP/SP Configuration).
- PingFederate supports "SP Lite" and "IdP Lite" Liberty Interoperability profiles for SAML 2.0.
- PingFederate supports configuration of the name, domain, and path for the cookie used for conveying state information between servers when cookie-based clustering has been configured.
- A number of past Known Issues and Limitations were addressed.

PingFederate 5.2 – August 2008

- A PingFederate IdP server now provides support for provisioning to selected SaaS providers. PingFederate supports provisioning of user account data from LDAP directories including Active Directory and Sun Directory Server. PingFederate stores synchronization data in JDBC data stores including Hypersonic (for demonstration purposes) and Oracle.
- PingFederate supports quick-connection templates to selected SaaS Providers, including Google Apps, and Salesforce.com

PingFederate 5.1.1 – July 2008

This release corrected several issues, including:

- SP signature verification was failing for assertions containing UTF-8 characters.
- In Windows the PingFederate server was unable to start when the `JAVA_HOME` system variable contained a space.
- Versions of the OpenToken library were placed in the wrong directory.
- Single Logout (SLO) with two SPs was not being performed for the IdP session(s).
- For SLO with three or more SPs, SP sessions were being stranded.
- Specific to PingFederate 5.1, Custom Data Sources no longer could be used for Adapter Contract fulfillment.
- When testing certain types of OGNL expressions, important error details were being lost when evaluation of these expressions failed.
- For SLO with at least two SPs, under certain circumstances error messages from SPs that did not initiate the SLO were not being processed correctly by the IdP.
- A PingFederate SP instance, when used with the OpenToken adapter, was converting a plus "+" character to a space " " when constructing the URL for final redirect.
- Signature validation was failing within a PingFederate SP instance when it received an SLO message in which the SAML_SUBJECT was being encrypted.
- PingFederate 5.1 SP instance was no longer supported SiteMinder SSO Zones.

PingFederate 5.1 – April 2008

- The default behavior when PingFederate cannot access a Certificate Revocation List (CRL) is now set correctly. The server no longer treats a non-retrievable CRL as a reason to label certificates as revoked. CRL processing behavior is managed by the revocation-checking-config.xml file in the /pingfederate/server/default/data/config-store directory.

- The IP address to which PingFederate's SNMP agent binds is now controlled by the pf.monitor.bind.address property in the run.properties file (*Administrator's Manual*: System Administration).
- Building either of the two example adapters included in the PingFederate SDK no longer fails with an error regarding a missing README.txt.
- The PingFederate server now correctly maintains temporary files within the /pingfederate/server/default/tmp directory. The server no longer writes temporary files to the tmp directory of the user running the server.
- Express Provisioning allows user accounts to be created in an LDAP repository and updated directly by an SP PingFederate. User provisioning occurs as part of SSO processing and may be used with any IdP partner (*Administrator's Manual*: SP Configuration/Managing IdP Connections).
- The Signature Policy screen in SAML IdP connections contains improved language clarifying how signatures are used to guarantee authenticity of SAML messages (*Administrator's Manual*: SP Configuration/Managing IdP Connections).
- The PingFederate package now contains v6.1.7 of Jetty. Jetty is the servlet container used by PingFederate.
- The PingFederate SDK contains a ConfigurationListener interface that may be utilized by developers building adapters. This interface contains methods invoked by the server in response to certain adapter-instance lifecycle events such as creation and deletion.
- Adapter-instance Summary screens now display adapter-instance configuration values specified within a TableDescriptor.
- After the third consecutive failed login attempt, an administrator is blocked from accessing the administrative console for a configurable amount of time (default = 60 seconds).
- When changing an administrator password, the server now forces the new password to differ from the existing password (*Administrator's Manual*: System Administration).
- Access to services exposed by the PingFederate server now requires client authentication. These services include Attribute Query, JMX, and Connection Management. An administrator may choose to require client authentication for access to the SSO Directory Service. An ID and Shared Secret comprise the credentials needed for authentication (*Administrator's Manual*: Security Management; *Administrator's Manual*: Web Service Interfaces).
- For security, the use of "Expression" in contract fulfillment screens is now disallowed by default. For backward compatibility, customers deploying a configuration archive from a previous version of PingFederate in which expressions were used will continue to have access to expressions. Allowing expressions creates a potential security concern in the PingFederate administrative console. (*Administrator's Manual*: Using Attribute Mapping Expressions)
- The Quick-Start SP Application no longer uses an OGNL expression in fulfilling the SP adapter contract.
- HTTP TRACE requests sent to PingFederate now result in an HTTP 403 Forbidden response.

- By default, “weak” ciphers are no longer supported during SSL handshaking. (For more information as to which cipher suites the server supports, examine the `com.pingidentity.crypto.SunJCEManager.xml` file in `pingfederate/server/default/data/config-store`.
- It is no longer possible for an administrator to circumvent role and access permissions within the administrative console by direct URL access. The server evaluates HTTP requests for a URL against an administrator’s assigned role(s) and responds appropriately.
- The PingFederate runtime server’s HTTP listener is now turned off by default. Only messages sent over HTTPS are accepted. This may be controlled in the run.properties file in the pingfederate/bin/directory.
- Use of class and package names specific to a PingFederate version were removed from sample source code contained in the PingFederate SDK.
- The /idp/startSSO.ping endpoint now supports an optional ACSIdx query parameter for SAML v2 partners. When provided, the PingFederate IdP attempts to send the SAML Assertion to the Assertion Consumer Service corresponding to the specified Index (*Administrator’s Manual*: Application Endpoints).
- The initial and maximum JVM heap sizes are set to 256 MB and 1024 MB, respectively, by default. These changes should improve runtime performance on servers with sufficient memory. These settings reside in the run.bat and run.sh files of the pingfederate/bin/directory.
- During server startup, PingFederate now reports relevant environment variables and adapter-instance information to the server.log.
- Existing partner connections can be deleted through a SOAP call from an external client application. (*Administrator’s Manual*: Web Service Interfaces).
- The pf-legacy-runtime.war file is no longer deployed by default. This WAR file allows a PingFederate server to continue support of legacy endpoints (those endpoints supported by PingFederate 2). When replacing an existing PingFederate 2 server deployment, manually move this WAR to the pingfederate/server/default/deploy/ directory.
- The PingFederate server can be configured to support the use of a proxy server when retrieving a CRL from a Certificate Authority. Relevant configuration settings reside in pingfederate/server/default/data/config-store/revocation-checking-config.xml.
- When the PingFederate server relies upon an external LDAP directory to authenticate administrative users, the ldap.password property in the pingfederate/bin/ldap.properties file now supports encrypted credentials (*Getting Started*: Installation).
- The PingFederate server allows imported SSL server certificates containing signatures from one or more intermediate Certificate Authorities. When SSL clients request an SSL connection to the PingFederate server, the entire SSL server certificate chain is presented.
- The Summary and Activation screens for both IdP and SP connections display a valid URL that serves as an example of a startSSO.ping endpoint used by local applications integrating with PingFederate (*Administrator’s Manual*: IdP/SP Configuration/Managing SP/IdP Connections).
- The Web SSO entry screens for both IdP and SP connections include summary information in a table describing relevant configuration settings (*Administrator’s Manual*: IdP/SP Configuration/Managing SP/IdP Connections).

- The PingFederate server prevents auditors from accessing links on the Main Menu that impact external resources. This includes exporting SAML metadata, signing XML files, and creating configuration archives (*Administrator's Manual*: System Administration).

PingFederate 5.0.2 – March 2008

- IdP Persistent Reference Cookie (IPRC) — Provides a mechanism allowing an SP PingFederate server to discover a user's IdP based on a persistent browser cookie that contains a reference to the IdP partner previously used for SSO.

  This feature provides an alternative to standard IdP Discovery for SP-initiated SSO, as defined in the SAML specifications, which uses a common-domain cookie (CDC) written by the IdP (see the PingFederate *Administrator's Manual*). Unlike the IdP Discovery cookie, the IPRC is written by the SP PingFederate each time an SSO event for the user occurs (either IdP- or SP-initiated). The cookie identifies the IdP partner using information in the SAML assertion. For subsequent SP-initiated SSO requests, the SP server can skip a previously required step prompting the user to select an IdP for authentication when multiple IdP partners are configured but none is specifically identified in the SSO call received by the SP PingFederate server.
- Updated the IdP-selection template to make it easier to use. The new selection template is used when no IPRC (or CDC) is available and when there are multiple IdPs to which the user might have previously authenticated.
- Corrected an issue in which a Concurrent Modification Exception was encountered when server clustering is used and debug is turned on for log files. (The workaround for this issue in previous releases is to turn debug off.)
- When no certificate revocation list (CRL) is found during certificate validation checking, the subject certificate is assumed to be valid for the current SSO/SLO transaction. Previously, when no CRL was found, the certificate was deemed invalid and the transaction aborted. The default setting is changed for this release to prevent problems with upgrading to PingFederate 5.x from previous versions.

PingFederate 5.0.1 – January 2008

- Support for rapid provisioning of partner connections is available using Auto-Connect technology. Leveraging the existing SAML 2.0 specification, Auto-Connect allows PingFederate deployments to scale easily with minimal manual involvement. The majority of partner connection configuration occurs at runtime through the exchange of dynamically generated metadata (*Administrator's Manual*: IdP/SP Configuration/Managing SP/IdP Connections).
- Administrators can authenticate to the administrative console using credentials in an external LDAP directory. This allows organizations with existing admin accounts to provide access to the console without creating and managing individual accounts within PingFederate (*Getting Started*: Installation).
- Partner connections may be created by importing them programmatically into PingFederate through a SOAP interface. This allows administrators to provision partner connections without accessing the administrative console manually. The Connection Management screens (both IdP and SP) contain an "Export" action that creates an XML file containing a connection's configuration (*Administrator's Manual*: Web Service Interfaces).

- Server configuration data may be replicated to a cluster through a SOAP call to the administrative console. This allows cluster deployments to receive configuration changes without accessing the administrative console manually (*Administrator's Manual*: Web Service Interfaces).
- The SAML 2 Attribute Query Profile is supported by PingFederate. This allows SPs to request user attributes from an IdP independent of user authentication (*Administrator's Manual*: IdP/SP Configuration/Managing SP/IdP Connections).
- Multi-valued attributes passed in an Assertion to a WS-Federation partner conform to how ADFS expects them.
- SAML metadata may be generated with a digital signature to guarantee authenticity (*Administrator's Manual*: System Administration).
- The Protocol Endpoints popup contains online help links. These links may be used to learn more about the server's endpoints from a partner perspective.
- The User-Session Creation screen in the IdP connection flow contains summary information that provides administrators with insight into the current configuration. Similarly, the Assertion Creation screen in the SP connection flow also provides administrators with useful configuration information (*Administrator's Manual*: IdP/SP Configuration/Managing SP/IdP Connections).
- Administrators can specify a descriptive "Connection Name" for partner connections (*Administrator's Manual*: IdP/SP Configuration/Managing SP/IdP Connections/General Information).
- The "Web SSO" portion of partner configuration is distinct from first/last-mile configuration (*Administrator's Manual*: IdP/SP Configuration/Managing SP/IdP Connections).
- Connection summary screens contain +/- buttons to show/hide major sections.
- Metadata import extracts the Base URL from the metadata file and populates relative URLs within the connection (*Administrator's Manual*: IdP/SP Configuration/Managing SP/IdP Connections/Importing Metadata).
- PingFederate communicates with an SNMP network-management console using standard SNMP Get and Trap operations (*Administrator's Manual*: System Settings/Managing Server Settings/Configuring Runtime Reporting).
- The PingFederate engine exposes a URL designed for load balancers to determine whether a PingFederate server is available to process transactions (*Administrator's Manual*: Application Endpoints/Maintenance Endpoint).
- Certificate-management usability is improved (*Administrator's Manual*: Security Management).
- Certificate expirations are tracked by PingFederate, and impending expirations may result in a notification sent via email, when configured (*Administrator's Manual*: System Settings/Managing Server Settings/Configuring Runtime Notifications).
- New, more user-friendly sample applications focus on demonstrating PingFederate server functionality (Quick-Start Guide).
- The entry screen into the "Credentials" area of connections contains useful information about the credentials used (*Administrator's Manual*: IdP/SP Configuration).
- The server ID is no longer displayed to the administrator.

- A cluster's administrative console no longer aggregates transactions counts.
- The "Cluster Management" link replaces "High Availability" on the Main Menu (Server Clustering Guide).
- Clustering supports TCP and UDP, node authentication, optional encryption, and use of a single port for all communication (Server Clustering Guide).
- CRL processing updated to support the U.S. GSA's E-Authentication v2 specification.
- The "About" pop-up contains additional license-key information.

PingFederate 4.4.2 – October 2007

Mitigated a number of potential security vulnerabilities regarding XML document processing.

PingFederate 4.4.1 – June 2007

Addresses user-interface defects related to attribute query, XML encryption, and LDAP data store lookups.

PingFederate 4.4 – May 2007

- Removal of support for the U.S. GSA's E-Authentication v1.0 specification.
- Addition for support of signed metadata files.
- Support for partner certificate revocation through CRLs.
- Increased flexibility around encryption of Name ID in SAML v2.0 SLO requests when the Name ID is encrypted within an assertion.
- Support for the SOAP binding for both inbound and outbound SAML v2.0 messages.
- Improved support for deployments where the server contains multiple network interfaces.
- Usability enhancements to the Main Menu layout and Local Settings flow.
- More sophisticated attribute-fulfillment operations through support of a Java-like syntax for data manipulation.
- Removal of extraneous credentials settings 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 hostnames to be used for incoming protocol message validation.
- Optionally, the SSO Directory Web Services can 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 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 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 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 toned 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-and 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.
- SAML 2-compliant IdP Discovery mechanism that enables an SP to dynamically determine the appropriate IdP for the user.
- Integration Kits 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 3.0.2 - February 2006

Upgrade of Jetty component to v5.1.10 in response to a security warning from the National Vulnerability Database.

PingFederate 3.0.1 - December 2005

- Complete clustering support.
- Optional email notification on licensing issues.
- You can edit a previously configured connection (either IdP or SP) that uses a data store that is unavailable.

PingFederate 3.0 – November 2005

- Support for SAML 2.0.
- Use-case wizard for partner connection configurations.
- Support for multiple security domains.
- Redesigned user interface.
- Embedded clustering.
- 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.