PingFederate®

Version 7.3

Release Notes

Ping Identity®

PingFederate 7.3 *Release Notes*
January, 2015

Ping Identity Corporation
1001 17th Street, Suite 100
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

Document Lifetime

Ping Identity may occasionally update online documentation between releases of the related software. Consequently, if this PDF was not downloaded recently, it may not contain the most up-to-date information. Please refer to documentation.pingidentity.com for the most current information.

From the Web site, you may also download and refresh this PDF if it has been updated, as indicated by a change in this date: **January 28, 2015**.

Contents

Release Notes Introduction **5**

Enhancements for the 7.3 Release **5**

Federation Hub 5

Administrative API Enhancements 5

Group Support for Inbound Provisioning 5

Support for wreply in WS-Federation SSO 6

Improved Redirect Validation 6

Security Enhancements 6

Improved Customizability 6

Other Enhancements 6

Upgrade Considerations **7**

SSLv3 Disabled 7

New Representation for Multi-valued Attributes in WS-Federation Assertions 7

A New Database Table for OAuth Persistent Grant Extended Attributes 7

LDAP Adapter No Longer Supported 7

LDAP Filter Syntax Checking 7

HTML Form Adapter Enhancement 8

Requested (formerly SAML) AuthN Context Selector Process Order Changed 8

Multi-valued LDAP Attributes Passed to Outbound Provisioning OGNL Expressions 8

Cluster Bind Address Required 9

Decryption and Digital Signing Policy Changes 9

Key Transport Algorithm Deprecated 9

Deprecated Features **10**

DSA Certificate Creation 10

JMX Monitoring Support for Outbound Provisioning 10

Known Issues **10**

Complete Change List by Released Version **13**

PingFederate 7.3 – January 2015 13

PingFederate 7.2 R2 – September 2014 13

PingFederate 7.2.1 – August 2014 14

PingFederate 7.2 – June 2014 14

PingFederate 7.1 R3 – March 2014 15

PingFederate 7.1 R2 – December 2013 16

PingFederate 7.1.4 – June 2014 16

PingFederate 7.1.3 – February 2014 17

PingFederate 7.1.2 – December 2013 17

PingFederate 7.1.1 – November 2013 17

PingFederate 7.1 – August 2013 17

PingFederate 7.0.1 – May 2013 18
PingFederate 7.0 – April 2013 18
PingFederate 6.11 – December 2012 19
PingFederate 6.10.1 – January 2013 20
PingFederate 6.10 – September 2012 20
PingFederate 6.9 – June 2012 20
PingFederate 6.8 – April 2012 20
PingFederate 6.7 – February 2012 20
PingFederate 6.6 – December 2011 21
PingFederate 6.5.2 – November 2011 21
PingFederate 6.5.1 – October 2011 21
PingFederate 6.5 – August 2011 21
PingFederate 6.5-Preview – April 2011 22
PingFederate 6.4.1 – February 2011 22
PingFederate 6.4 – December 2010 22
PingFederate 6.3 – August 2010 23
PingFederate 6.3-Preview – April 2010 23
PingFe*derate 6.2 – February* 2010 23
PingFederate 6.1 – September 2009 24
PingFederate 6.1-Preview – June 2009 24
PingFederate 6.0 – March 2009 25
PingFederate 5.3 – December 2008 25
PingFederate 5.2 – August 2008 26
PingFederate 5.1.1 – July 2008 26
PingFederate 5.1 – April 2008 27
PingFederate 5.0.2 – March 2008 29
PingFederate 5.0.1 – January 2008 29
PingFederate 4.4.2 – October 2007 31
PingFederate 4.4.1 – June 2007 31
PingFederate 4.4 – May 2007 31
PingFederate 4.3 – March 2007 32
PingFederate 4.2 – December 2006 32
PingFederate 4.1 – October 2006 32
PingFederate 4.0 – June 2006 33
PingFederate 3.0.2 - February 2006 34
PingFederate 3.0.1 - December 2005 34
PingFederate 3.0 – November 2005 34
PingFederate 2.1 – July 2005 34
PingFederate 2.0 – February 2005 34

Release Notes Introduction

Welcome to PingFederate, Ping Identity's enterprise identity bridge. PingFederate enables outbound and inbound solutions for single sign-on (SSO), federated identity management, mobile identity security, API security, and social identity integration. Browser-based SSO extends employee, customer, and partner identities across domains without passwords, using only standard identity protocols (Security Assertion Markup Language—SAML, WS-Federation, WS- Trust, and OAuth).

These release notes summarize the changes in current and previous product updates.

Enhancements for the 7.3 Release

Note: For a condensed list of all enhancements for this and previous releases, see the Complete Change List by Released Version section, which also contains references to additional documentation.

Federation Hub

PingFederate now supports the ability to route SSO requests and responses between an IdP and an SP connection, potentially spanning disparate protocols, such as SAML 1.x, SAML 2.0, and WS-Federation. For example, an incoming SAML 2.0 IdP connection can be bridged to a WS-Federation SP connection. Additionally, Federation Hub features can centralize and simplify administrative overhead by multiplexing a single application to many IdP partners.

Many PingFederate feature areas have been enhanced to support Federation Hub use cases:

- Adapter Selectors are renamed as Authentication Selectors, and can now be used to choose amongst both IdP Connections and Adapters.
- "Map URLs to Adapter Instances" has been renamed as "Target URL Mapping." It now appears under SP Application Integration Settings in the main Administrative Console page, and supports mapping a target URL pattern to either an SP Adapter or an SP Connection.
- A new SampleAuthenticationSelector SDK example has been created, which allows selection of an IdP Adapter or Connection, based on a user-supplied email address or domain.

Administrative API Enhancements

Creation, update and retrieval of SP Connections is now supported in the Administrative API. As with IdP Connections, SP Connection currently covers IdP and SP-initiated SAML 2.0 browser SSO profiles, including POST and redirect bindings.

Group Support for Inbound Provisioning

This release adds support for inbound provisioning of groups as defined in SCIM 1.1 (http://www.simplecloud.info/). This capability allows groups to be created, updated, and queried in a target identity store via SCIM calls to PingFederate. The provisioning target may be either an Active Directory data store or a custom Identity Store Provisioner plugin.

Support for wreply in WS-Federation SSO

This release includes support for the wreply parameter in WS-Federation SSO, which allows a single PingFederate SP connection to be used with multiple SharePoint 2013 hosted applications.

Improved Redirect Validation

Target Resource Validation has been renamed as Redirect Validation and moved to the central area of the Administrative Console, under Server Settings. Validation can now be applied to the TargetResource for SLO and InErrorResource parameters, in addition to TargetResource for SSO. Redirect validation is enabled by default in new installations of PingFederate. If upgrading from a previous version of PingFederate, it is recommended to enable the new validation options and add appropriate whitelist entries.

Security Enhancements

- For LDAP type data stores with LDAPS enabled, hostname verification of the certificate is now available. This option is enabled by default for all new data stores. When upgrading from a previous version of PingFederate, this option is disabled for existing data stores, but should be turned on for greater security.
- When using the anchored trust model for back-channel authentication or XML signature verification, it is now possible to restrict the certificate issuer DN.
- Elliptic Curve algorithms are now available for certificate creation and XML signatures. Additionally, RSA key based certificate creation has been enhanced to include RSA SHA-2 signing algorithms and 4096 bit keys.

Improved Customizability

- An Application Name and Application Icon URL can now be associated with SP Connections as well as Adapter-to-Adapter mappings. The new fields are accessible in the Adapter SDK.
- The response rendered by PingFederate for requests to the /pf/heartbeat.ping endpoint is now easily customizable via the heartbeat.page.template, and can be configured to include system information such as memory and CPU usage.
- A new template has been created, http.error.page.template.html, which allows customization of the page displayed to end users for standard HTTP errors, such as 404.
- A customizable favicon.ico now ships with PingFederate and applies to all end-user-facing endpoints.

Other Enhancements

- The LDAP Password Credential Validator can now be configured to return additional user attributes beyond the username and user DN. This enhancement simplifies attribute contract fulfillment in cases where additional data is required from the same LDAP directory store.
- The PingOne Directory Password Credential Validator is now bundled as part of the standard PingFederate installation.

- The HTML Form Adapter now supports a configurable maximum session lifetime.
- In Outbound Provisioning, PingFederate now supports provisioning nested LDAP groups.
- In Attribute Contract Fulfillment, PingFederate now supports retrieving nested LDAP groups.
- Upgraded JGroups to version 3.5.1.
- Upgraded Jetty to version 8.1.16.
- Over 60 other defects fixed.

Upgrade Considerations

Several specific modifications made since PingFederate 6.11 may affect existing deployments, as described the following sections.

SSLv3 Disabled

To mitigate the POODLE attack, the SSLv3 protocol is disabled by default starting in PingFederate 7.3. It can be re-enabled by modifying the connector configuration in jetty-runtime.xml and jetty-admin.xml.

New Representation for Multi-valued Attributes in WS-Federation Assertions

Starting in PingFederate 7.3, multi-valued attributes in WS-Federation assertions are now represented as multiple AttributeValue elements under a single Attribute element. Previously, they were represented as a series of Attribute elements with the same name. The new behavior was implemented for compatibility with ADFS 2.0. To revert to the previous behavior, a setting is available in wstrust-global-settings.xml.

A New Database Table for OAuth Persistent Grant Extended Attributes

Starting in PingFederate 7.2 R2, a new database table needs to be created to support OAuth's 'Persistent Grant Extended Attributes'. The database script to create this table can be found in `<pf_install>/pingfederate/server/default/conf/access-grant/sql-scripts/access-grant-attribute-*.sql`.

LDAP Adapter No Longer Supported

Starting in PingFederate 7.2, the LDAP Java Adapter is no longer supported. This adapter was deprecated in PingFederate 6.6 and replaced by the LDAP Password Credential Validator (PCV), which can be used with the HTML Form or HTTP Basic IdP Adapters.

LDAP Filter Syntax Checking

Starting with PingFederate 7.2, LDAP filters only allow spaces in matched-against values.

Examples

`(|(sAMAccountName=${username})(employeeID=ID for ${username}))` is allowed; spaces in the matched-against value of "`ID for ${username}`" are valid.

`( | (sAMAccountName=${username}) (employeeID=ID for ${username}) )` is not allowed because this filter contain spaces outside of matched-against values.

Invalid filters cause SSO runtime failures. Error messages logged to server.log include:

```
Caused by: javax.naming.NamingException: [LDAP: error code 87 - Expected a
closing parenthesis...
```

```
Caused by: javax.naming.NamingException: [LDAP: error code 87 - Unexpected
closing parenthesis found...
```

We recommend reviewing LDAP filters and removing spaces outside of matched-against values after upgrade.

HTML Form Adapter Enhancement

Starting with version 7.1 R3, PingFederate tracks login attempts in the HTML Form Adapter. When the number of login failures reaches the Challenge Retries threshold defined in the adapter, the user is locked out for one minute. For more information, see *Administrator's Manual*: HTML Form Adapter Configuration.

Requested (formerly SAML) AuthN Context Selector Process Order Changed

In releases prior to 7.1 R2, when the Requested AuthN Context Adapter Selector received a list of authentication contexts, it used the last context that it could match, rather than the first. However, both the SAML and OpenID Connect specifications treat an authentication context list as appearing in order of preference. To align the Requested AuthN Context Adapter Selector with these specifications, the selection order was changed in 7.1 R2. With this release, the selector will use the first authentication context it can match, rather than the last.

Multi-valued LDAP Attributes Passed to Outbound Provisioning OGNL Expressions

In releases before version 7.1, if an OGNL expression was used to populate a SaaS-partner field in Outbound Provisioning, only the first value of a selected multi-valued LDAP attribute was used in the OGNL expression. As of PingFederate 7.1, this behavior was changed to use all values in the expression.

Note: If this new behavior conflicts with existing deployments, it may be reverted via the `supportMultiValuesFromDirectory` property located in `<pf_install>/pingfederate/server/default/data/config-store/com.pingidentity.provisioner.mapping.OgnlFieldMapper.xml`

Cluster Bind Address Required

Starting with PingFederate 6.11, the *pf.cluster.bind.address* property (located in `<pf_install>/pingfederate/bin/run.properties`) is required when running PingFederate in a cluster.

Decryption and Digital Signing Policy Changes

Potential security vulnerabilities have resulted in the following changes to PingFederate as of version 6.11. In some cases, these may impact interoperability with partners:

- When acting as an SP and using the POST binding, PingFederate decrypts an assertion only when the SAML response has been signed. An unsigned SAML response that contains an encrypted assertion is rejected.

  Note: Although strongly discouraged, this policy change may be reverted on a per-connection basis via the `EntityIdsToAllowAssertionDecryptionWithoutResponseSignature` property located in `<pf_install>/pingfederate/server/default/data/config-store/org.sourceid.saml20.profiles.sp.HandleAuthnResponse.xml`

- When acting as an IdP, PingFederate always signs a SAML response (even when the assertion is also signed) if it contains an encrypted assertion.

  Note: Although strongly discouraged, this policy change may be reverted on a per-connection basis via the *`EntityIdsToOmitResponseSignatureOnSignedEncryptedAssertion`* property located in `<pf_install>/pingfederate/server/default/data/config-store/org.sourceid.saml20.profiles.idp.HandleAuthnRequest.xml`

- When acting as an IdP, PingFederate decrypts an encrypted NameID in an Attribute Query only when the request has been signed or the client has authenticated with basic or mutual TLS.

Key Transport Algorithm Deprecated

Due to security risks associated with the RSA-v1.5 algorithm used for key transport, it is no longer available for new connections. Existing connections in which this algorithm is configured continue to support it. However, we recommend upgrading such connections to use the newer algorithm RSA-OAEP (see *Administrator's Manual*: Selecting an Encryption Certificate (SAML) and Choosing an Encryption Certificate).

Note: The JCE provider libraries distributed with Luna and nShield Connect HSMs do not support the RSA-OAEP algorithm at the time of this release (7.1 R2). As a result, RSA-v1.5 is still allowed when deploying PingFederate with an HSM.

Deprecated Features

DSA Certificate Creation

As of PingFederate 7.3, it is no longer possible to create DSA key pairs in the certificate management pages of PingFederate. Import of DSA key pairs continues to be supported.

JMX Monitoring Support for Outbound Provisioning

As of PingFederate 7.2, the JMX Monitoring support for Outbound Provisioning has been deprecated and replaced with an audit file approach that is more inline with other auditing services offered by PingFederate.

JMX Monitoring for Outbound Provisioning can be re-enabled in 7.2 but will be removed in a future release.

Known Issues

- When using PingFederate with the Thales nShield Connect HSM, it is not possible to use an Elliptic Curve certificate as an SSL server certificate.
- If a source attribute has been configured for masking in an IdP adapter or IdP connection and the source attribute is mapped to OAuth's persistent grant USER_KEY attribute, then the USER_KEY attribute will not be masked in the server logs. Other persistant grant attributes will be masked.
- PingFederate's API Docs is not fully supported in IE9. The response headers will not show up in the API Docs' sandbox, due to limited Cross-origin resource sharing (CORS) support in IE9.
- The administrative API connection support is currently limited to IdP SAML 2 Browser SSO connections. As a result, it is possible to lose settings that are not supported by the administrative API (e.g. WS-Trust or SLO) when these settings are added through the UI and the connection is subsequently modified through the API.
- Concurrent API requests to the administrative API are currently not supported and may result in an unstable system.
- If an IdP connection is configured for multiple virtual server IDs, PingFederate will always use the default virtual server ID for IdP Discovery during an SP-initiated SSO event.
- OpenID Connect single-logout is not supported when the IdP session is created through OAuth attribute mapping.
- The RADIUS NAS-IP-Address is only included in Access-Request packets when the *pf.bind.engine.address* is set to an IPv4 address. IPv6 is not currently supported.
- The **Save Draft** feature is not available for connections that override plug-in settings from within the connection. In this case, the following DEBUG log message may be generated:

  ```
  DEBUG [DraftManagerImpl] There was a NotSerializableException trying to serialize the draft
  ```

  This message can be safely ignored.

- Adapter instances specified as "Sufficient" in a Composite Adapter configuration should be limited to adapter types that explicitly return control to PingFederate after a failure. Otherwise, the next adapter instance in an authentication "chaining" sequence (if any) may not be tried, and other unexpected behavior may occur.

  The following adapters work correctly under the Sufficient authentication policy in failure mode:

  - X509
  - LDAP (legacy adapter)
  - OpenID - Generic
  - OpenID - Google
  - IWA – returns control to PingFederate only if the failure is the result of invalid credentials after the configured number of retries
  - HTML Form
  - HTTP Basic

  Note: This list is updated as other adapters are modified, tested, and released.

- The anchored-certificate trust model cannot be used with the single logout (SLO) redirect binding since the certificate cannot be included with the logout request.
- PingFederate cannot simultaneously log the audit log to multiple databases and/or ArcSight CEF syslog. The audit log can only use a single log4j appender. See the `log4j.xml` file in `<pf_install/pingfederate/server/default/conf>` for additional details.
- 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 fails. 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.
- Using the browser's navigation mechanisms (e.g., the **Back** button) causes inconsistent behavior in the administrative console. Use the navigation buttons provided at the bottom of screens in the PingFederate console.
- 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, the browser may redirect to the Main Menu and not the login page.
- LDAP referrals 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.
- When an nShield Connect HSM in a HA nShield Connect cluster is shutdown, users will receive exceptions in the console when trying to create private keys for both digital signatures and SSL.

Before creating new private keys, the nShield Connect HSM should be restored to a normal state (up on the network up, HSM up with OCS cards in their slots), and PingFederate should be restarted.

- 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.
- 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 does not normalize this to the valid namespace of `http://schemas.xmlsoap.org/ws/2005/02/trust` (i.e., without the trailing slash) and fails the transaction. In this case, the workaround is to have the client set the namespace element to the valid namespace of `http://schemas.xmlsoap.org/ws/2005/02/trust`.
- When upgrading to PingFederate 6.8 or higher, all persistent grants for any existing OAuth deployments using a MySQL database will expire. To address this issue, the `expires` column in the `pingfederate_access_grant` table should be nulled prior to the upgrade. If necessary, contact Ping Identity support for assistance.

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 configcopy to copy all connections, channels, data sources, adapters, or token translators and you choose to set override properties, the override is 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 is 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.
- 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.
- When using configcopy to copy connection data, any SOAP SLO endpoints defined in the source are not 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.

Complete Change List by Released Version

PingFederate 7.3 – January 2015

- Federation Hub
- SampleAuthenticationSelector SDK Sample
- SP Connections API
- Group Support for Inbound Provisioning
- Support for wreply in WS-Federation SSO
- Improved Redirect Validation
- Hostname verification for LDAPS data stores
- Issuer restriction in anchored trust model for back-channel authentication and XML signature verification.
- Elliptic Curve algorithms for certificate creation and XML signatures.
- RSA certificate creation enhanced to include RSA SHA-2 signing algorithms and 4096 bit keys.
- Application Name and Application Icon URL for SP Connections and Adapter-to-Adapter mappings.
- Customizable response from /pf/heartbeat.ping.
- Customizable template for HTTP error pages.
- Customizable favicon.ico
- LDAP Password Credential Validator can now be configured to return additional user attributes beyond the username and user DN.
- PingOne Directory Password Credential Validator is now bundled as part of the standard PingFederate installation.
- Key algorithm and key size are now displayed in certificate management pages and the certificate details popup.
- HTML Form Adapter now supports a configurable maximum session lifetime.
- In Outbound Provisioning, PingFederate now supports provisioning nested LDAP groups.
- In Attribute Contract Fulfillment, PingFederate now supports retrieving nested LDAP groups.
- Upgraded JGroups to version 3.5.1.
- Upgraded Jetty to version 8.1.16.
- Over 60 other product issues resolved.

PingFederate 7.2 R2 – September 2014

- Multiple Access Token Management Plug-in Instances
- Improved Attribute Mapping for OAuth Access Token Contract

- Multiple Data Source Lookup for OAuth Workflows
- OpenID Connect / OAuth 2.0 Form POST Response Mode
- Include User Info in the OpenID Connect ID Token
- Administrative API Enhancements
    - Configuration Archive Management
    - IdP Connection Metadata Export / Import
    - Certificate Management of Trusted CAs, SSL Client Keys, and SSL Server Certificates
    - Data Sources
    - Password Credential Validators
    - IdP-to-SP Adapter Mapping
- Administrative Console Enhancements
- Other Enhancements
    - The OAuth `client_id` parameter is now available in the IdP Adapter SDK interface
    - Support SID encoding for binary LDAP attributes (enabling claims-based authentication to Microsoft Outlook Web Access)
    - Various security enhancements
    - Over 40 other product issues resolved

PingFederate 7.2.1 – August 2014

- Fixed an issue for Office 365 Outlook use cases where user accounts could be locked after changing their passwords in Active Directory.
- Fixed an issue where users would not be provisioned correctly under certain conditions.
- Fixed an issue that prevented additional "Actions" in adapter configuration from executing correctly.

PingFederate 7.2 – June 2014

- Multiple Virtual Server IDs
- OpenID Connect-based Centralized Session Management
- LDAP Enhancements
    - Improved performance on LDAP bind operations
    - Ability to control timeout on LDAP attribute lookups
    - Better connection cleanup when an idle LDAP connection is removed from the pool
- Administrative API Enhancements
    - IdP and SP Adapters
    - Access Token Management (OAuth)

- Custom HTTP Response Headers
- Improved Target Resource Validation
- Outbound Provisioning Monitoring
- New Username Token Processor
- Redesigned Default User-Facing Screens
- Other Enhancements
    - Support for Java 8
    - Support for OAuth Symmetric Proof of Possession for Code Extension
    - Upgraded JGroups to 3.4.4.Final
    - Various security enhancements
    - Over 50 other product issues resolved

PingFederate 7.1 R3 – March 2014

- Administrative API Enhancements
    - Server Settings (OAuth Use Cases)
    - OAuth Settings
    - Authorization Server Settings
    - OpenID Connect Policy Management
    - Client Management
    - IdP Adapter Mapping
    - Access Token Mapping
- OAuth Enhancements
    - OAuth 2.0 Token Revocation (RFC 7009)
    - Access Grant API
- RADIUS Support Extended
    - Challenge-Handshake Authentication Protocol (CHAP) Support
    - Vendor-Specific Attributes
    - NAS-IP-Address Passed in Access-Request
- Enhanced Support for Reverse Proxy Deployments
- Other Enhancements
    - Allow PingFederate's session cookie to be optionally configured to be persistent
    - Allow the Access Token Verification/Validation Grant Type to be used in combination with other grant types
    - Various security enhancements

- Over 20 other product issues resolved

PingFederate 7.1 R2 – December 2013

- Administrative API (see *Administrator's Manual:* PingFederate Administrative API)
- Tracking ID Enhancements
- Outbound Provisioning
  - Microsoft SQL Server Support added for Internal Provisioning Data Store (see *Administrator's Manual*: Configuring Outbound Provisioning Settings)
  - OAuth 2.0 Bearer Token Authorization for SCIM 1.1 Plugin (see *Administrator's Manual*: Defining a Provisioning Target)
  - Ability to Define Deprovision Method for SCIM 1.1 Plugin (see *Administrator's Manual*: Defining a Provisioning Target)
- OAuth and OpenID Connect Enhancements
  - Extended OAuth to allow multiple scopes to be grouped together and referenced as a single scope, enabling scope downgrade during token refresh
  - Allow administrators to define a maximum token lifetime for OAuth Access Tokens
  - OpenID Connect now supports requesting that the Authorization Server use specified authentication contexts when processing the authentication request
- Added TemplateRendererUtil class and template-render-adapter-example to PingFederate SDK
- Allow administrators to define a maximum token lifetime for OAuth Access Tokens
- Extended HTML Form Adapter to allow usernames to be stored and pre-populated in the login form after a user's first successful authentication
- OpenID Connect now supports requesting that the Authorization Server use specified authentication contexts when processing the authentication request
- Partner Entity ID (Connection ID) now available as input parameter to all Identity Store Provisioner requests
- Extended OAuth to allow multiple scopes to be grouped together and referenced as a single scope, allowing scope downgrade during token refresh
- Reintroduced Luna HSM Support
- Upgraded Jetty to 8.1.14
- Upgraded JGroups to 3.3.4.Final
- Various security enhancements
- Over 40 other product issues resolved

PingFederate 7.1.4 – June 2014

- Addressed a potential CSRF issue with the PingFederate Administration console.

- Updated the default Multiple SSO in Progress template to escape additional input variables (`speed.bump.template.html`).
- Addressed an issue where Office 365 Outlook users can have their user accounts to be locked out after they change their Active Directory passwords.
- Corrected the Content-Type header for interoperability with Office 365 OneDrive.
- Made available the $HttpServletRequest object in the IdP logout template (`template.idp.logout.success.page.template.html`).
- Resolve an issue with body-less HTML Form POST messages sent by Internet Explorer when HTML Form based authentication follows an unsuccessful IWA authentication within a Composite Adapter.
- Made an improvement to correctly handle LDAP queries for Distinguished Names having forward slashes (/).

PingFederate 7.1.3 – February 2014

- Corrected potential security vulnerability.

PingFederate 7.1.2 – December 2013

- Corrected an issue with artifact binding in clustered deployments that resulted in sporadic failed transactions. This issue only applied to version 7.1.1.

PingFederate 7.1.1 – November 2013

- Corrected potential security vulnerability
- Fixed XML namespace issue that resulted in failed SSO transactions at partners with hardcoded dependencies on the `samlp` prefix
- Resolved XML parsing issue that resulted in PingFederate rejecting incoming authentication requests
- Corrected logging issue that resulted in AJP-based transactions to fail

PingFederate 7.1 – August 2013

- Added support for Outbound Provisioning via PingOne (see *Administrator's Manual*: Configuring Outbound Provisioning)
- Added identity store SDK for Inbound Provisioning (see *Administrator's Manual*: Configuring Inbound Provisioning)
- Provided Remote Authentication Dial-In User Service (RADIUS) Support for console logon and password credential validation (see *Administrator's Manual*: Alternative Console Authentication, Validating Password Credentials)
- Added hierarchical (parent/child) configurations for plug-in instances (see *Administrator's Manual*: Configuring Inbound Provisioning)

- Related plug-in instance override capability added for connections (see *Administrator's Manual*: Selecting an Adapter Instance, Choosing an Adapter Instance
- Enabled overriding the global Default Target URL for connections and adapter-to-adapter mapping (see *Administrator's Manual*: SSO configuration sections for IdP and SP connections and for IdP-to-SP adapter mapping)
- Made STS client authentication details available for token authorization (see *Administrator's Manual*: WS-Trust STS Configuration)
- Extended JMX runtime monitoring support (see *Administrator's Manual*: Runtime Monitoring Using JMX)
- Enabled usage checking for certificates, adapters, token translators, credential validators and data stores (see *Administrator's Manual*: relevant configuration sections)
- Store OAuth client configuration as XML files (new default, database storage optional) (see *Administrator's Manual*: Configuring Inbound Provisioning)
- Upgraded Jetty to 8.1.9
- Upgraded JGroups to 3.3.0.Final
- Various security enhancements
- Over 80 other product issues resolved

PingFederate 7.0.1 – May 2013

Addressed potential security vulnerabilities found since the PingFederate 7.0 initial, limited-availability release.

PingFederate 7.0 – April 2013

- Added support for System for Cross-domain Identity Management (SCIM)
    - Inbound Provisioning (see *Administrator's Manual*: Configuring Inbound Provisioning)
    - Outbound Provisioning (see *Administrator's Manual*: Configuring Outbound Provisioning)
- Initial Support for OpenID Connect
- New Context sources available in Token Authorization and Attribute Mapping workflows
    - HTTP Request
    - *Client IP* Request
- Administrative Console Enhancements
- Upgraded Jetty to 8.1.8
- Added support for the SAML AuthnRequest Scoping element Request (see *Administrator's Manual*: Configuring the Requested AuthN Context Selector)
- Created the Cluster Node Adapter Selector for use within Adapter Selection Request (see *Administrator's Manual*: Configuring the Cluster Node Selector)

- Allow PingFederate runtime context path to be customized Request (see *Administrator's Manual*: System Administration)
- Security Enhancements
- Over 50 product issues resolved

PingFederate 6.11 – December 2012

- Added password update via HTML Form IdP Adapter (see *Administrator's Manual*: Configuring the HTML Form IdP Adapter)
- Enhanced IdP Adapter Selector functionality:
    - Decision Tree Processing (see *Administrator's Manual*: Mapping Selector Results to Adapter Instances)
    - Connection Set Selector (see *Administrator's Manual*: Configuring the Connection Set Selector)
    - HTTP Header Selector (see *Administrator's Manual*: Configuring the HTTP Header Selector)
    - OAuth Scope Selector (see *Administrator's Manual*: Configuring the OAuth Scope Selector)
- Added localization for user-facing Web pages (see *Administrator's Manual*: Localization)
- Added capability of defining globally an HTTP Header containing client IP addresses (see *Administrator's Manual*: Defining an HTTP Header for Client IP Addresses)
- Added OAuth fine-grain scope handling and JWT access-token support (see *Administrator's Manual*: Configuring JSON-Token Management)
- Added Dynamic JVM Resource Allocation
- Upgraded JGroups to 3.3.0.Alpha1 (snapshot from 10/30/12)
- Extended the Consent Form template to include the $entityId parameter
- Extended the OAuth Grants Management template to show grant type, scope, and the date/time a grant was issued and updated
- Improved SLO handling in scenarios where a user performs multiple SSO requests
- Improved the ability for administrators to define validation rules for HTTP request parameters
- Improved JDBC data store attribute lookup functionality to allow for retrieval of multiple values from a single database column (see *Administrator's Manual*: Configuring a JDBC Database Connection)
- Made security enhancements
- Removed the requirement to include TokenProcessorId/TokenGeneratorId query parameters for STS requests to an IdP/SP connection when only a single instance of the token-processor/generator type is configured for the connection
- Enabled PingFederate to use Jetty's NIO (New I/O) backed SSL Connectors by default
- Enhanced Microsoft Office 365 support to allow for Kerberos interoperability with active clients built on top of Microsoft Online Services Sign-In Assistant

- Enhanced LDAP error code handling in the LDAP Username Password Credential Validator to enable more specific error messages to be provided to end users
- Enabled PingFederate to interoperate with Microsoft Dynamics CRM 2011

PingFederate 6.10.1 – January 2013

- Replaced OpenToken adapter with version 2.5.1 to capture security enhancements
- Other changes to address potential security vulnerabilities

PingFederate 6.10 – September 2012

- Token Authorization (see *Administrator's Manual*: About Token Authorization)
- STS token exchange mapping (see *Administrator's Manual*: STS Token Exchange Mapping)
- OAuth client mutual TLS authentication (see *Administrator's Manual*: Configuring a Client)
- OAuth 2.0 final draft compliance

PingFederate 6.9 – June 2012

- Microsoft Office 365 interoperability
- STS transaction events logged to audit log (see *Administrator's Manual*: System Administration)
- Upgraded Jetty and removed underlying JBoss infrastructure

PingFederate 6.8 – April 2012

- Added centralized AD Domain/Kerberos Realm configuration (see *Administrator's Manual*: Security Management)
- Added OAuth Client Management REST API (see *Administrator's Manual*: Web Service Interfaces)
- Added optional expiration of OAuth persistent grants (see *Administrator's Manual*: OAuth Configuration)
- Added multiple redirect URIs per OAuth client (see *Administrator's Manual*: OAuth Configuration)
- Added optional restricted scope subsets per OAuth client (see *Administrator's Manual*: OAuth Configuration)
- Added configurable consent page omission per OAuth client (see *Administrator's Manual*: OAuth Configuration)
- Added OAuth transaction events logged to audit log (see *Administrator's Manual*: System Administration)

PingFederate 6.7 – February 2012

- Added Splunk Application for PingFederate (see *Administrator's Manual*: System Administration)
- Improved administrative console navigation and save performance

- Added LDAP connection pooling options for LDAP data stores (see *Administrator's Manual*: System Settings)

PingFederate 6.6 – December 2011

- Added contextual IdP Adapter selection using Adapter Selectors (see *Administrator's Manual*: Key Concepts)
- Added ability to chain multiple IdP adapters together using the Composite Adapter (see *Administrator's Manual*: Key Concepts)
- Added the ability to use multiple IdP data stores for attribute retrieval and mapping into an IdP attribute contract (see *Administrator's Manual*: Key Concepts)
- Added an HTML Form adapter and HTTP Basic adapter to replace the LDAP Authentication adapter (see *Administrator's Manual*: Key Concepts)
- Support for the OAuth SAML 2.0 Bearer Assertion Grant Type (see *Administrator's Manual*: OAuth Configuration)
- Added an Admin Console Help system updater (see *Administrator's Manual*: System Settings)
- Added IPv6 support

PingFederate 6.5.2 – November 2011

Security update since the PingFederate 6.5.1 release

PingFederate 6.5.1 – October 2011

Security updates since the PingFederate 6.5 release

PingFederate 6.5 – August 2011

Note: The PingFederate 6.5 release includes the features described below as well features that were added in a limited-distribution "Preview" release, described in the next section.

- PingFederate now functions as an OAuth 2.0 Authorization Server (see *Administrator's Manual*: OAuth Configuration)
- Added support for Thales (nCipher) nShield Connect HSM (see *Getting Started*: Using the Thales nShield Connect HSM)
- Account Linking can use an LDAP directory for a persistent data store in addition to a relational database system (see *Administrator's Manual*: System Settings)
- User-Defined Attribute Namespaces can be specified for Browser SSO protocols (similar to what was added to WS-Trust STS) to allow for better Microsoft interoperability (see *Administrator's Manual*: Key Concepts)
- Adapter to Adapter mapping now counts as a licensed connection (see *Administrator's Manual*: System Settings)

- LDAP Adapter updated to 2.2 with new default Web form login template (see *Administrator's Manual*: LDAP Adapter Configuration)
- Jetty version upgrade from 6.1.7 to 6.1.26

PingFederate 6.5-Preview – April 2011

- Full STS metadata Claims Provider and Relying Party interoperability with Microsoft WIF, WCF, and ADFS 2.0
- Support multiple token-processor instances of the same token type (see *Administrator's Manual*: IdP Configuration for STS)
- Added SAML HoK subject confirmation in the SAML Token Generator (see *Administrator's Manual*: SP Configuration for STS)
- Added option for STS SAML token KeyInfo to use a signing certificate reference rather than the full signing certificate (see *Administrator's Manual*: IdP Configuration for STS)
- Session-state modifications to support simultaneous and nested SSO transactions
- IdP adapter session handling for IdP adapters that rely on PingFederate for session management to allow for consecutive requests without prompting for credentials

PingFederate 6.4.1 – February 2011

- Corrected license expiration date calculation

PingFederate 6.4 – December 2010

- Support standard .NET WS-Trust Federation Bindings (see *Administrator's Manual*: Key Concepts)
- Support SAML 2.0 token Holder of Key (HoK) subject confirmation (see *Administrator's Manual*: WS-Trust STS Configuration)
- Added Metadata Exchange (MEX) endpoint for WIF client to generate bindings automatically for Username, X.509, and SAML tokens (see *Administrator's Manual*: Application Endpoints)
- Added support for WS-Trust 1.4 ActAs property
- Added two-factor authentication capability with the VeriSign® Identity Protection (VIP) Authentication Service Adapter (see *Administrator's Manual*: Identity Provider SSO Configuration)
- OpenToken Adapter 2.4.1 updated to correct issue with Cookie Transport Method and Replay Prevention
- Expanded digital signature secure hash algorithm types - SHA1, SHA256, SHA 384, and SHA512 (see *Administrator's Manual*: sections covering applicable certificate-selection screens)
- The provisioning log can be written to a database—Oracle, Microsoft SQL Server, and MySQL databases supported (see *Administrator's Manual*: System Administration)
- Added SAML protocol support for AuthnContextDeclRefs (see *Administrator's Manual*: Application Endpoints)

PingFederate 6.3 – August 2010

Note: The PingFederate 6.3 release includes the features described below as well features that were added in a limited-distribution "Preview" release, described in the next section.

- PingFederate STS claims-based identity capabilities extended to support interoperability with Microsoft WIF and WCF client frameworks (see *Administrator's Manual*: Key Concepts)
- Expanded SNMP monitoring variables available in the management information base (MIB) (see *Administrator's Manual*: System Settings)
- Increase the default PingFederate HTTP header buffer size to 8k
- Key stores and key store passwords are dynamically generated per installation
- The default SSL server certificate is generated upon initial startup if an SSL certificate does not exist
- LDAPS trust configuration no longer requires a server restart to take effect

PingFederate 6.3-Preview – April 2010

- Added support for logging to the ArcSight Common Event Format (CEF) (see *Administrator's Manual*: System Administration)
- Added ability to log to a database with failover to file—Oracle, SQL Server, and MySQL databases supported (see *Administrator's Manual*: System Administration)
- Added ability to disable automatic multi-connection validation if the validation time is causing excessive delay (see *Administrator's Manual*: System Settings)
- Extended JDBC Express Provisioning to support MS SQL Server stored procedures (see *Administrator's Manual*: Service Provider SSO Configuration)
- Added replay prevention capability to the OpenToken IdP Adapter bundled with PingFederate

PingFe*derate 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*: Identity Provider 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*: Service Provider 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*: Identity Provider SSO Configuration and Service Provider SSO 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*: 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*: 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*: Managing SP Connections and Managing 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*: Managing SP Connections and Managing 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*: Managing SP Connections and Managing 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*: Managing SP Connections and Managing 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*: Managing SP Connections and Managing IdP Connections).
- Administrators can specify a descriptive "Connection Name" for partner connections (*Administrator's Manual*: General Information and General Connection Information).
- The "Web SSO" portion of partner configuration is distinct from first/last-mile configuration (*Administrator's Manual*: Managing SP Connections and Managing 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*: Importing Metadata and Importing IdP Metadata).
- PingFederate communicates with an SNMP network-management console using standard SNMP Get and Trap operations (*Administrator's Manual*: 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).
- 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*: 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*: Identity Provider SSO Configuration and Service Provider SSO 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
- 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, including 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

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
- Ability to edit SP adapters that are in-use with target systems
- Encrypt or decrypt entire assertions or select elements, 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