Release Notes

ON THIS PAGE

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

Subscribe for automatic updates: PingFederate Release Notes RSS feed

PingFederate enables outbound and inbound solutions for single sign-on (SSO), federated identity management, mobile identity security, API security, social identity integration, and customer identity and access management (CIAM). PingFederate extends employee, customer, and partner identities across domains without passwords, using only standard identity protocols: SAML, WS-Federation, WS-Trust, OAuth, and System for Cross-domain Identity Management (SCIM).

PingFederate 13.1.1 (July 2026)

Resolved issues

Kerberos realm test failure

Fixed PF-39487

We fixed a defect that caused Kerberos realm test connections without explicitly configured Key Distribution Centers (KDCs) to fail.

CIMD loopback URL validation

Fixed PF-39501

We fixed a defect where PingFederate rejected `http://` loopback `client_id` URLs at runtime. Client ID Metadata Documents (CIMD) policies that use those URLs now display a warning.

PingID client-side authenticator failure

Fixed PF-39546

We fixed a defect that caused the PingID client-side authenticator to fail after the PingFederate 13.1 Jakarta migration.

Heartbeat endpoint failure with Redis

Fixed PF-39580

We fixed a defect that caused the heartbeat endpoint to fail when PingFederate was configured with Redis and an internally managed reference token manager.

SSO and SLO failure in Redis mode

Fixed PF-39584

We fixed a defect that caused single sign-on (SSO) and single logout (SLO) requests to fail after authentication through the grant management endpoint when using Redis for the identity provider (IdP) session registry.

Missing subject field in OIDC backchannel SLO audit log

Fixed PF-39587

We fixed a defect that caused the subject field to be missing from the SLO audit log entries after OpenID Connect (OIDC) backchannel logout in Redis mode.

SP adapter session termination failure in Redis mode

Fixed PF-39588

We fixed a defect that prevented SLO from terminating service provider (SP) adapter sessions in Redis mode, allowing users to remain authenticated after SLO.

OAuth client authentication method conflict

Fixed PF-39589

We fixed a defect where enabling **Client TLS Certificate** authentication alongside other authentication methods on an OAuth client caused some methods, such as **Client Secret**, to fail.

CIMD authorization failure with LDAP client storage

Fixed PF-39593

We fixed a defect that caused CIMD authorization requests to fail with HTTP 400 when PingFederate used LDAP client storage, requiring approximately 60 seconds of idle time before requests succeeded.

Token exchange failure with ID-JAG enabled

Fixed PF-39604

We fixed a defect where enabling **Identity Assertion JWT (ID-JAG)** on an SP connection caused token exchange requests for other token types to fail due to an ID-JAG-specific validation check being incorrectly applied.

PingFederate 13.1 (June 2026)

New features and enhancements

Redis cache storage support

New PF-38267 PF-38345 PF-38841 PF-38842 PF-38843 PF-38844

We added support for storing data from the following services in a Redis cache:

- Assertion Replay Prevention Service data
- Dynamic JSON Web Keys
- Session Revocation Service data
- OAuth Reference Bearer Access Token Plugin data
- IdP Session Registry Service data
- SP Session Registry Service data

PingFederate stores short-lived data in a Redis cache to improve resiliency and scalability. It also eases upgrades in clustered environments.

Learn more in Storing PingFederate data with Redis.

SP Connection for OAuth Token Exchange

New PF-38312

We added the ability to configure SP connections for OAuth token exchange.

This allows clients or AI agents to obtain tokens from third-party authorization servers using a cross-domain assertion. It also supports Identity Assertion JWT Authorization Grant (ID-JAG) token exchange.

Learn more in Configuring SP connections for OAuth token exchange.

Mac platform SSO

New PF-38487

We added support for the JWT Bearer Grant Processor IdP connection type.

This connection type facilitates workforce user SSO from their macOS login.

Learn more in JWT Bearer Grant Processors and Configuring Platform SSO for macOS in the PingOne documentation.

Private Key JWT client authentication for REST API datastore

New PF-38489

We added the ability to use private key JWT client assertions to request OAuth 2.0 bearer tokens for accessing REST API datastores.

This feature improves authentication security and ensures compatibility after Microsoft Exchange Online support for basic authentication ends in late 2026.

Learn more in Configuring a REST API datastore.

PUT, PATCH, and DELETE in REST API datastore

New PF-38492

We added support for PUT, PATCH, and DELETE requests to the REST API datastore.

These standard API request types give you more options for managing user data in a REST API datastore.

Learn more in Configuring a REST API datastore.

User and authentication context for authorization details

New PF-38493

We added support for accessing authenticated user details and authentication context in the AuthorizationDetailsProcessor SDK.

This feature allows user-aware validation and enrichment in custom authorization details processors.

Learn more in the PingFederate 13.1 SDK documentation.

Secret managers for OAuth clients

New PF-38494

We added support for secret managers to OAuth clients.

This improves security and convenience by allowing you to centrally manage authentication secrets for clients.

Learn more in Configuring OAuth clients.

OAuth bearer token authentication for SMTP servers

New PF-38500

We added support for OAuth 2.0 bearer token authentication for SMTP servers.

This feature improves authentication security, and ensures compatibility after Microsoft Exchange Online support for basic authentication ends in late 2026.

Learn more in Configuring an SMTP Notification Publisher instance.

Disable automatic IdP adapter validation

New PF-38501

We added a feature that allows you to disable automatic validation of IdP adapters when you go to the **Authentication > Integration > IdP Adapters** menu.

Disabling automatic validation can reduce loading time if you have a large number of IdP adapters configured.

Learn more in Disabling automatic IdP adapter validation.

Identity Assertion JWT Authorization Grant (ID-JAG)

New PF-38825

We added support for Identity Assertion JWT Authorization Grant (ID-JAG) flows in PingFederate.

PingFederate can now issue ID-JAG tokens through OAuth token exchange and accept ID-JAG tokens in OAuth JWT-bearer grant requests. This update also adds a Refresh Token Token Processor for token-exchange processor policies.

Learn more in Configuring a Refresh Token Token Processor instance.

OAuth client tags

New PF-38826

We added the ability to apply tags to resources like OAuth clients.

Tags make it easier for you to categorize, organize, and filter resources. You can also create policies to make decisions based on resource tags.

Learn more in Tag Management.

CIMD for OAuth clients

New PF-38827

We added support for Client ID Metadata Documents (CIMD) for OAuth clients.

This feature allows PingFederate to retrieve and validate client metadata during runtime transactions and dynamically create clients. This is especially useful for AI agents and other automated or short-lived clients that need dynamic access without being pre-registered individually.

Learn more in Client ID metadata documents (CIMD) and the CIMD specification.

Multiple authentication methods for OAuth clients

New PF-38828

We added support for configuring more than one client authentication method for an OAuth client.

This feature helps you transition clients from one authentication method to another without requiring a single cutover event.

Learn more in Configuring OAuth clients and OAuth Client Management Service.

Per-client DPoP settings

New PF-38845

We added support for per-client Demonstrating Proof-of-Possession (DPoP) settings and DPoP defaults for dynamically registered clients.

This feature lets you override global DPoP defaults for individual clients.

Learn more in Configuring OAuth clients and Managing client configuration defaults.

EncryptedKey selection for encrypted SAML attributes

New PF-38882

We added support for `CarriedKeyName`-based decryption key selection for encrypted attributes in SAML 2.0 response processing.

This improves support for certificate rollover and deployments that use different decryption keys across recipients or clusters.

Learn more in Specifying XML encryption policy (for SAML 2.0).

Full JSON response mapping in REST API datastore

Improved PF-34615

We added support for mapping the full JSON response document to a local attribute in a REST API datastore.

This gives you more flexibility when mappings or decisions depend on the complete response structure.

Learn more in Configuring a REST API datastore.

Redesigned OAuth client management

Improved PF-38499

We redesigned the **Clients** page and the client configuration form.

These redesigned pages make it easier to review existing clients at a glance and to find and configure attributes for both new and existing clients.

Learn more in Managing OAuth clients and Configuring OAuth clients.

Pushed Authorization Request request_uri lifecycle

Improved PF-38880

We changed how PingFederate invalidates `request_uri` values in Pushed Authorization Request (PAR) flows.

PingFederate now invalidates the `request_uri` when consent details are presented to the user, or when the **PAR Reference Timeout** expires. If consent details aren't presented, clients can reuse the `request_uri` until the **PAR Reference Timeout** expires.

Learn more in Pushed authorization requests endpoint.

Unconnected cluster node startup

Improved PF-38898

We added the `force.require.replication.data.on.startup` parameter to the `cluster-config-replication.conf` file.

This parameter allows you to prevent an engine node from starting up without establishing a connection to the cluster.

Learn more in Cluster management.

JGroups upgrade

Info PF-35844

We upgraded JGroups to version 5.5.2.Final.

Windows Server 2025

Info PF-36967

We qualified PingFederate for use with Microsoft Windows Server 2025.

Jakarta EE 9 migration

Info PF-37687

We updated PingFederate for Jakarta EE 9 migration, including dependency updates to Spring Framework 6.2.19, Jetty 12.0.36, Jersey 3, and OpenAPI 3.

Oracle Unified Directory

Info PF-38046

We qualified PingFederate for use with Oracle Unified Directory version 14c.

PAR parameters

Info PF-38526

We added a new configuration option to limit the Pushed Authorization Request (PAR) to the parameters mentioned in the specification when the connection is configured to use JWT-secured Authorization Request (JAR).

`log4j-core` update

Info PF-38538

We upgraded `log4j-core` to version 2.25.3.

This upgrade ensures continued alignment with maintained upstream dependencies and resolves a potential security vulnerability.

Java 25 support

Info PF-38798

We qualified PingFederate for use with Java 25.

Identity for AI admin console link

Info PF-38847

We added a **Helpful Link** from the PingFederate admin console to the Identity for AI Solutions documentation. These guides help you learn about how to configure Ping Identity solutions (including PingFederate) to work with artificial intelligence (AI).

OAuth Playground 6.0

Info PF-38902

We released version 6.0 of the OAuth Playground.

Earlier versions of the OAuth Playground aren't compatible with PingFederate 13.1 or later.

Learn more in OAuth Playground.

Amazon Aurora MySQL

Info PF-38913

We qualified PingFederate for use with Amazon Aurora MySQL 3.12.0 (compatible with MySQL 8.0.44)

PostgreSQL

Info PF-38914

We qualified PingFederate for use with PostgreSQL versions 16.13, 17.9, and 18.3.

Amazon Aurora PostgreSQL

Info PF-38915

We qualified PingFederate for use with Amazon Aurora PostgreSQL (compatible with PostgreSQL 16.13 and 17.9).

Opentelemetry

Info PF-39298

We upgraded opentelemetry to the latest versions.

Bundled integration kits

Info PF-39444

We updated the following bundled integration kits to their latest versions:

- Agentless Integration Kit 2.3.1
- PingID Integration Kit 2.30
- PingOne Integration Kit 3.1.1
- PingOne MFA Integration Kit 3.3
- PingOne Protect Integration Kit 1.0.8
- PingOne Verify Integration Kit 2.3.4

Resolved issues

Admin console cookie improvements

Security PF-34376 PF-37650

We updated how the cross-site request forgery (CSRF) cookie is issued and validated in the admin console for more effective CSRF protection.

Private key JWT OAuth client authentication improvements

Security PF-36847

We improved the way the `aud` claim is managed in `private_key_jwt` OAuth authentications. This aligns PingFederate with RFC 7523 specifications and security best practices.

Exposed filepath in end-user error page

Security PF-38109

We fixed a security vulnerability that could've exposed a PingFederate filepath when displaying an error message to end users.

OGNL executable code

Security PF-38241

We fixed a security vulnerability where a misconfigured PingFederate deployment could've executed code included in an OGNL expression.

OGNL code test

Security PF-38742

We improved role-based access control (RBAC) for the administrative expression testing endpoint. Access to expression evaluation is now limited to appropriately-privileged roles, ensuring alignment with intended administrative permissions.

`jackson-core` update

Security PF-38830

We've upgraded `jackson-core` to version 2.21.1 to continue alignment with maintained upstream dependencies and remove potential security vulnerabilities.

SLO failure

Fixed PF-38442

We fixed a defect where front-channel logouts requests to `/idp/startSLO.ping` failed to send logout requests to relying party URIs.

Multiple Sign-On Delay routing

Fixed PF-38801

We fixed a defect that caused PingFederate to route users to the base URL for the Multiple Sign-On Delay page when they should've been routed to the virtual host URL.

Extended properties for password change/reset

Fixed PF-38262

We fixed a defect that prevented extended properties from applying to password change and password reset flows.

`pi.flow response_mode` fix

Fixed PF-38417

We fixed a defect where setting `response_mode` to `pi.flow` in Pushed Authorization Requests (PAR) or standard request objects resulted in an `INVALID_REQUEST` error.

Fixed NPE when updating SP connection

Fixed PF-38508

We fixed a defect that caused a null pointer exception (NPE) error when an SP connection with backchannel authentication inbound authentication type set to **No Client Authentication** and **Require SSL** enabled was created or updated using the Admin API.

Dynamic client registration failure

Fixed PF-38548

We fixed a defect that caused dynamic client registration to fail when **Retain Client Secret** was enabled and **Client Secret Retention Period** was set globally in **Authorization Server Settings**.

Kerberos realm validation error

Fixed PF-38585

We fixed a defect that prevented PingFederate from creating, updating, or testing Kerberos realms when the **`AutoGenerateKrb5Conf`** parameter was set to `false` in the `com.pingidentity.common.util.KerberosConfigUtil` file.

Kerberos realm test connectivity overwriting `krb5.conf`

Fixed PF-38585

We fixed a defect where PingFederate temporarily overwrote the `krb5.conf` file during Kerberos realms testing when **`AutoGenerateKrb5Conf`** was disabled.

Heartbeat endpoint failure

Fixed PF-38595

We fixed a defect that caused the heartbeat endpoint to be potentially unresponsive in rare concurrent access situations.

Authentication policy error

Fixed PF-38623

We fixed a defect that caused an error when authentication policies with a Requested AuthN Context Authentication had **Add or Update AuthN Context Attribute** enabled.

Log settings not applied to new engine nodes

Fixed PF-38627

We fixed a defect where log settings weren't applied to newly-joined engine nodes.

Response code for refresh token exchange failure with revoked user session

Fixed PF-38656

We fixed a defect that caused a refresh token for access token exchange to fail with `500 Internal Server Error` instead of `400 Bad Request` when the user's sessions had been revoked.

Client secret endpoint

Fixed PF-38659

We fixed a defect where the client secret updated even when the request to the `oauth/clients/{id}/clientAuth/clientSecret` endpoint resulted in a validation error.

CIBA token request fails with LDAP persistent grant storage

Fixed PF-38706

We fixed a defect that caused CIBA token requests to fail when persistent grants are stored in an LDAP directory like PingDirectory.

Admin API OAuth authentication failure

Fixed PF-38722

We fixed a defect that caused OAuth and JWT authentication through the Admin API to fail when the **`role attribute name`** parameter used the scope claim containing space-delimited values.

Local identity profile attribute caching

Fixed PF-38824

We fixed a defect that caused PingFederate to cache user registration form attributes for local identity profiles when the registration workflow is configured to run after account creation.

Custom Authentication Selector error

Fixed PF-38875

We fixed a defect that prevented viewing or editing certain custom Authentication Selectors in the admin console.

Serialized Java objects in signed request object

Fixed PF-38889

We fixed a defect that caused parameters added to request objects (signed JWT) sent to the OIDC provider in OIDC IdP connections to lose their original data type.

Extended Property Authentication Selector dependency error warning

Fixed PF-38901

We fixed a defect that caused PingFederate to continue displaying a dependency error warning for the Extended Property Authentication Selector after the selector instance is deleted.

Dynamic JWKS rotation timer

Fixed PF-38903

We fixed a defect that prevented dynamic JWKS rotation timing from resetting after a node joined a cluster.

URL validation for `TargetResource`

Fixed PF-38907

We fixed a defect where PingFederate rejected valid `TargetResource` values.

Cluster node joining failure

Fixed PF-39240

We fixed a defect that prevented an engine node from joining a cluster when both active and passive admin consoles were online during a data upgrade.

Client certificate authentication behind proxy

Fixed PF-39335

We fixed a defect where PingFederate, when deployed behind a proxy with mTLS, used the TLS layer certificate instead of the client certificate forwarded in the client certificate header, which caused certificate authentication failure.

Known issues and limitations

PingOne Verify IK unexpected error

Issue PF-36573

PingFederate returns an unexpected error when you create an instance of the PingOne Verify Integration Kit version 2.2.2 in PingFederate with the Verify feature in PingOne disabled.

Third-party cookie blocking affecting single logout

Issue PF-35772

Due to multiple vendors' recent browser versions that block third-party cookies, you might experience issues related to single logout with OIDC (via Front-Channel) and WS-Federation.

Refer to browsers' documentation regarding third-party cookie management to unblock them, if feasible.

Passive admin console UI refresh

Issue PF-35643

When you promote a passive admin console to active, the UI doesn’t refresh until you perform an action.

Multiple active admin consoles

Issue PF-35439

When you make configuration changes on the active console (especially large configuration changes like bulk imports or data archive imports), then promote a passive console to

active, it can cause multiple consoles to be active at once. This can result in inconsistent configurations.

Learn how to resolve this issue in Resolving multiple active administrative nodes.

Administrative console and administrative API

Issue

- Although PingFederate 11.3 and later support DPoP, a known limitation is that the following features don't support DPoP when PingFederate is the RP:
  - The administrative console authentication scheme using OIDC
  - The administrative API authentication scheme using OAuth 2.0
- /bulk: Only resource types currently supported by the administrative API are included in the exported data. We don't intend to introduce administrative API support to the following areas:
  - SAML 2.0 IdP Discovery
  - SAML 2.0 SP Affiliation
  - SMS Provider
- Previously, the administrative API did not accurately reflect a **Persistent Grant Max Lifetime** setting of 29 days (or shorter) with the selection of the **Grants Do Not Timeout Due To Inactivity** option. As a result, if you have configured such OAuth authorization server settings and have generated a bulk export in version 10.0 through 10.0.2, we recommend that you re-generate a new bulk export after upgrading to version 10.0.3 (or a more recent version). The newly exported data does not contain the aforementioned flaw, and you can safely import it to version 10.0.3 (or a more recent version).
- When enabling mTLS certificate-based authentication, administrators often configure a list of acceptable client certificate issuers. When you use a browser to access the console or the administrative API documentation, PingFederate returns to the browser the list of acceptable issuers as part of the TLS handshake. If the browser's client certificate store contains multiple client certificates, the browser often presents you only the certificates whose issuer matches one of the acceptable issuers. However, when PingFederate runs in a Java 17 environment, Chrome presents you all its

configured client certificates, regardless of whether the issuer matches one of the acceptable issuers or not.

- When using mTLS authentication to authenticate to an LDAP server for administrative console or administrative API access, PingFederate doesn't support using a Microsoft Active Directory server.
- Prior to toggling the status of a connection with the administrative API, you must ensure that any expired certificates or no longer available attributes are replaced with valid certificates or attributes; otherwise, the update request fails.
- When creating or updating a child instance of a hierarchical plugin, the administrative API retains objects with an `"inherited": false` name/value pair (or without such name/value pair altogether), ignores those with a value of `true`, and returns a 200 HTTP status code. No error messages are returned for the ignored objects.
- Using the browser's navigation mechanisms (for example, the **Back** button) causes inconsistent behavior in the administrative console. Use the navigation buttons provided at the bottom of windows in the PingFederate console.
- Using the PingFederate console in multiple tabs on one browser might cause inconsistent behavior which could corrupt its configuration.
- If authenticated to the PingFederate administrative console using certificate authentication, a session that has timed out might 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 sign-on page, and then back to the administrative console after authentication is complete. Similar behavior applies for certificate authentication, in principle. However, because the browser might automatically resubmit the certificate for authentication, the browser might redirect to the administrative console and not the sign on page.

TLS cipher suite customization

Issue

PingFederate's TLS cipher suites can be customized by modifying `com.pingidentity.crypto.SunJCEManager.xml` (or a similarly-named file if BCFIPS or an HSM is configured). After updating the file and replicating, all cluster nodes must be restarted for the change to take effect.

Java

Issue

- Updating Java version 8 to version 11 results in an error when PingFederate is already installed and running on Windows. To work around this issue, uninstall and reinstall the PingFederate Windows service by running the `UninstallPingFederateService.bat` and `InstallPingFederateService.bat` files located in `<pf_install>/pingfederate/sbin/wrapper`.

HSMs

Issue

AWS CloudHSM

- It is not possible to use an elliptic curve (EC) certificate as an SSL server certificate.
- When creating an EC certificate with a `signatureAlgorithm` smaller than the `keySize` value, a `500 Server error` occurs. For example, a `signatureAlgorithm` of `SHA256withECDSA` with a `keySize` of `384` results in an error. Learn more in ECDSA signing fails with "invalid mechanism" error starting with SDK 5.16 in the CloudHSM documentation.
- TLS 1.3 is not currently supported with Oracle JDK 17 or 21.

Thales HSMs

- JWT token decryption using ECDH-ES may fail. This issue only arises if PingFederate is configured with static OAuth and OpenID Connect keys, a static key is stored on the HSM, and PingFederate is consuming a token encrypted with this key.
- It is not possible to use an EC certificate as an SSL server certificate.
- TLS 1.3 isn't currently supported with Oracle JDK 17.

Entrust HSMs

- JWT token decryption using ECDH-ES may fail. This issue only arises if PingFederate is configured with static OAuth and OpenID Connect keys, a static key is stored on the HSM, and PingFederate is consuming a token encrypted with this key.

- It is not possible to import a PKCS12- or PEM-formatted EC certificate.
- It is not possible to use an EC certificate as an SSL server certificate.
- TLS 1.3 isn't currently supported with Oracle JDK 17.

SSO and SLO

Issue

- When consuming SAML metadata, PingFederate does not report an error when neither the `validUntil` nor the `cacheDuration` attribute is included in the metadata. Note that PingFederate does reject expired SAML metadata as indicated by the `validUntil` attribute value, if it is provided.
- The anchored-certificate trust model cannot be used with the single logout (SLO) redirect binding because the certificate cannot be included with the logout request.
- 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.

Composite Adapter configuration

Issue

SLO is not supported when users are authenticated through a Composite Adapter instance that contains another instance of the Composite Adapter.

Self-service password reset

Issue

Passwords can be reset for Microsoft Active Directory user accounts without the permission to change password.

OAuth

Issue

PingFederate does not support a case-sensitive naming convention for OAuth client ID values when client records are stored in a directory server. For example, after creating a client with an ID value of `sampleClient`, PingFederate does not allow the creation of another client with an ID value of `SampleClient`.

Although it's possible to create clients using the same ID values with different casings when client records are stored in XML files, a database server, or custom storage, we recommend not doing so to avoid potential record migration issues.

Customer identity and access management

Issue

Some browsers display a date-picker user interface for fields that have been designed for date-specific inputs. Some browsers do not. If one or more date-specific fields are defined on the registration page or the profile management page (or both), end users must enter the dates manually if their browsers do not display a date-picker user interface for those fields.

Provisioning

Issue

- 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.
- The **`totalResults`** value in SCIM responses indicates the number of results returned in the current response, not the total number of estimated results on the LDAP server.

Logging

Issue

- 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, the **`USER_KEY`** attribute will not be masked in the server logs. Other persistent grant attributes will be masked.

- Even if a source attribute has been configured for masking in an IdP adapter and the source attribute is mapped as the adapter's unique user key, the user key attribute is not masked in the server or audit logs.

Database logging

Issue

- 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, the `USER_KEY` attribute will not be masked in the server logs. Other persistent grant attributes will be masked.
- Even if a source attribute has been configured for masking in an IdP adapter and the source attribute is mapped as the adapter's unique user key, the user key attribute is not masked in the server or audit logs.

RADIUS NAS-IP-Address

Issue

The RADIUS NAS-IP-Address is only included in Access-Request packets when the `pf.bind.engine.address` is set with an IPv4 address. IPv6 is not supported.

Amazon SNS Notification Publisher

Issue

When deploying PingFederate with a forward proxy, plugins based on the AWS SDK, such as the Amazon SNS Notification Publisher, will only honor the `http.proxyHost`, `http.proxyPort`, `http.proxyUser`, and `http.proxyPassword` properties in `run.properties`. The plugin will rely on these properties even if the service URL is `https`.

Deprecated features

No features were deprecated for PingFederate 13.1.

PingFederate 13.0.4 (July 2026)

New features and enhancements

Apache MINA dependency

Info PF-39148

We updated Apache MINA to version 2.2.7.

Resolved issues

Client certificate authentication behind proxy

Fixed PF-39335

We fixed a defect where PingFederate, when deployed behind an mTLS proxy, used the TLS layer certificate (the proxy's server certificate) instead of the client certificate forwarded in the configured client certificate header. This caused client certificate authentication to fail when the proxy terminated mTLS from the client.

Learn more in Configuring incoming proxy settings.

Kerberos realm test failure

Fixed PF-39487

We fixed a defect that caused Kerberos realm test connections without explicitly configured KDCs to fail.

User Count Utility startup failure

Fixed PF-39502

We updated the bundled User Count Utility to version 1.0.20 to fix a startup issue triggered by certain log4j configurations.

PingFederate 13.0.3 (May 2026)

New features and enhancements

Unconnected cluster node startup

Improved PF-38898

We added the `force.require.replication.data.on.startup` parameter to the `cluster-config-replication.conf` file.

This parameter lets you prevent an engine node from starting up without establishing a connection to the cluster.

Learn more in Cluster management.

Jetty library

Info PF-38819

We upgraded the Jetty library to version 12.0.33.

Jetty symbolic links

Info PF-38916

If you configured previous Jetty versions to support symbolic links, those links might no longer work with Jetty 12.0.

You can allow support for the symbolic links by adding the `pf.assets.allowSymlinks=true` parameter to the `run.properties` file.

Resolved issues

Multiple Sign-On Delay routing

Fixed PF-38801

We fixed a defect that caused PingFederate to route users to the base URL for the **Multiple Sign-On Delay** page when they should've been routed to the virtual host URL.

OAuth client management service response format

Fixed PF-38872

We fixed a defect in the OAuth Client Management Service where parameters that support multiple values were always returned as arrays, even with only a single value. Now single values are returned as strings and multiple values are returned as arrays.

This defect affects PingFederate version 13.0.3 or later that was upgraded using the in-place method.

If you want the client management service to return arrays for all parameters, you can set the `writeSingleItemElementAsArray` parameter to `true` in the `com.pingidentity.ws.rest.oauth.client_management.model.converter.SerializerUtil.xml` file.

Learn more in Upgrade considerations.

Custom Authentication Selector error

Fixed PF-38875

We fixed a defect that prevented viewing or editing certain custom Authentication Selectors in the admin console.

Extended Property Authentication Selector dependency error warning

Fixed PF-38901

We fixed a defect that caused PingFederate to continue displaying a dependency error warning for the Extended Property Authentication Selector after the selector instance is deleted.

Dynamic JWKS rotation timer

Fixed PF-38903

We fixed a defect that prevented dynamic JWKS rotation timing from resetting after a node joined a cluster.

URL validation for `TargetResource`

Fixed PF-38907

We fixed a defect where PingFederate rejected valid `TargetResource` values.

PingFederate 13.0.2 (April 2026)

Resolved issues

OGNL code test

Security PF-38742

We improved role-based access control (RBAC) for the administrative expression testing endpoint. Access to expression evaluation is now limited to appropriately-privileged roles, ensuring alignment with intended administrative permissions.

`jackson-core` update

Security PF-38830

We've upgraded `jackson-core` to version 2.21.1 to continue alignment with maintained upstream dependencies and remove potential security vulnerabilities.

Fixed NPE when updating SP connection

Fixed PF-38508

We fixed a defect that caused a null pointer exception (NPE) error when an SP connection with backchannel authentication inbound authentication type set to **No Client Authentication** and **Require SSL** enabled was created or updated using the Admin API.

Log settings not applied on new engine nodes

Fixed PF-38627

We fixed a defect where log settings weren't applied to newly joined engine nodes.

Response code for refresh token exchange failure with revoked user session

Fixed PF-38656

We fixed a defect that caused a refresh token for access token exchange to fail with `500 Internal Server Error` instead of `400 Bad Request` when the user's sessions had been revoked.

CIBA token request fails with LDAP persistent grant storage

Fixed PF-38706

We fixed a defect that caused CIBA token requests to fail when persistent grants are stored in an LDAP directory like PingDirectory.

Admin API OAuth authentication failure

Fixed PF-38722

We fixed a defect that caused OAuth and JWT authentication through the Admin API to fail when the **`role attribute name`** parameter used the scope claim containing space-delimited values.

PingFederate 13.0.1 (February 2026)

New features and enhancements

Disable automatic IdP adapter validation

New PF-38501

We've added a feature that allows you to disable automatic validation of IdP adapters when you go to the **Authentication > Integration > IdP Adapters** menu.

Disabling automatic validation can reduce loading time if you have a large number of IdP adapters configured.

Learn more in Disabling automatic IdP adapter validation.

PAR parameters

Info PF-38526

We've added a new configuration option to limit the Pushed Authorization Request (PAR) to the parameters mentioned in the specification when the connection is configured to use JWT-secured Authorization Request (JAR).

`log4j-core` update

Info PF-38538

We've upgraded `log4j-core` to version 2.25.3.

This upgrade ensures continued alignment with maintained upstream dependencies and resolves a potential security vulnerability.

Resolved issues

`pi.flow` `response_mode` fix

Fixed PF-38417

We've fixed a defect where setting `response_mode` to `pi.flow` in Pushed Authorization Requests (PAR) or standard request objects resulted in an `INVALID_REQUEST` error.

Dynamic client registration failure

Fixed PF-38548

We've fixed a defect that caused dynamic client registration to fail when **Retain Client Secret** was enabled and **Client Secret Retention Period** was set globally in **Authorization Server Settings**.

Kerberos realm validation error

Fixed PF-38585

We've fixed a defect that prevented PingFederate from creating, updating, or testing Kerberos realms when the `AutoGenerateKrb5Conf` parameter was set to `false` in the `com.pingidentity.common.util.KerberosConfigUtil` file.

Kerberos realm test connectivity overwriting `krb5.conf`

Fixed PF-38585

We've fixed a defect where PingFederate temporarily overwrote the `krb5.conf` file during Kerberos realms testing when `AutoGenerateKrb5Conf` was disabled.

Heartbeat endpoint failure

Fixed PF-38595

We've fixed a defect that caused the heartbeat endpoint to be potentially unresponsive in rare concurrent access situations.

Authentication policy error

Fixed PF-38623

We've fixed a defect that caused an error when authentication policies with a Requested AuthN Context Authentication had **Add or Update AuthN Context Attribute** enabled.

PingFederate 13.0 (December 2025)

New features and enhancements

gMSA support for Kerberos realms on Windows

New PF-37270

We've added a feature that lets you use group Managed Service Account (gMSA) credentials in Kerberos realms when running PingFederate on Windows.

With this feature, you can let Active Directory automatically rotate your client password so you don't have to manage it.

Learn more in Configuring a secret manager for Windows gMSA.

Verbose logging lifetime expiration

New PF-37374

We've added a feature that allows you to set an expiration time for verbose logging.

This feature is disabled by default, but you can enable it by configuring the `log4j-categories-settings.conf` file.

Learn more in Enabling verbose logging lifetime expiration.

Externally stored scopes with AWS DynamoDB

New PF-37671

We've added a feature that allows external scope storage using AWS DynamoDB.

This allows administrators to manage a large volume of scopes without replicating for every scope modification.

Learn more in Configuring external databases for scope storage.

Automatically replicate log changes to cluster

New PF-37684

We've added a feature that automatically replicates changes to log settings to cluster servers. This feature is enabled by default, but you can disable it from the **Cluster**

Management page.

This feature makes it easier to change log settings across your cluster without running a full replication cycle.

Learn more in Cluster management.

Redis support

New PF-37691 PF-38064 PF-38065

We've added support for connecting PingFederate to Redis.

PingFederate stores short-lived data in a Redis cache to improve resiliency and scalability. It also eases upgrades in clustered environments. PingFederate currently supports storing the following data in Redis:

- Account locking information
- Authorization artifacts
- Inter-Request State-Management (IRSM) service data

Learn more in Storing PingFederate data with Redis

Custom audience values for OAuth clients

New PF-37693

We've added a feature that allows you to add custom audience values for OAuth clients.

You can use this feature to migrate clients from your existing issuer into PingFederate.

Learn more in Migrating external OAuth clients into PingFederate.

User Count Utility log parsing

New PF-37847

We've added a feature that allows the PingFederate User Count Utility (UCU) to parse JSON logs.

Learn more in PingFederate User Count Utility in the Ping Identity Support Knowledge Base.

Client Side Authenticators

New PF-37909

PingFederate now supports plugins with client-side authenticator functionality.

Client-side authenticators enable PingFederate to leverage authentication methods executed directly by the user's browser or operating system, such as Passkeys. This allows for stronger, often passwordless, authentication flows.

Learn more in HTML Form Adapter advanced fields and Configuring an Identifier First Adapter instance.

Distributed tracing (Open Telemetry)

New PF-38051

We've added the ability to perform distributed tracing for inbound and outbound requests to the PingFederate server.

This feature simplifies troubleshooting by giving you better observability of server processing across request workflows.

Learn more in Distributed tracing.

Expired persistent grants in PingDS

New PF-38062

We've added a feature that allows you to configure time-to-live (TTL) settings in PingDS to remove expired data from your directory server.

Learn more in Managing expired persistent grants in PingDS.

Error handling IdP connections

New PF-38063

We've added a feature that lets you determine how incoming errors are handled before they're relayed to the requesting application or partner.

Learn more in Overriding error handling in an IdP connection.

Authentication session storage in PingDS

New PF-38082

We've added support for storing authentication sessions on a PingDS server.

This update makes it easier to integrate your PingFederate and PingDS deployments.

Learn more in Defining a datastore for persistent authentication sessions.

Support for response_type none

New PF-38114

We've added support for the OIDC `response_type=none`.

This enables clients to request a grant of access from the Authorization Server without requiring the issuance of any tokens or security credentials.

Learn more in None Response Type in the OIDC specification.

Accessible token response in OIDC IdP connection

New PF-38120

We've added a feature that allows you to access additional parameters of an OIDC-enabled IdP's token endpoint response.

You can use the **Token Endpoint Response** context values when creating attribute mappings or issuance criteria in OIDC-enabled IdP connections.

Learn more in Configuring target session fulfillment.

Bulkhead warning email

Improved PF-37011

Bulkhead warning emails now include the IP address and cluster index of the engine node that triggered the bulkhead.

Thread pool management

Improved PF-37547

We've improved Jetty thread pool management so that PingFederate no longer creates unnecessary thread pools. The number of threads allocated to unused servers now depends on the operational mode.

OpenID Connect Policy Selector

Improved PF-38033

The policy list is now sorted alphabetically by name in both the OAuth Client and Client Settings configurations.

AWS DynamoDB scope manager cache configuration

Improved PF-38269

The `cacheExpirySecs` attribute is now exposed by default in the DynamoDB scope manager configuration file.

Learn more in Configuring external databases for scope storage.

Multiple addresses for administrative console runtime

Improved PF-38118

We've added a feature that allows multiple email addresses for administrative console runtime notification email fields.

This update affects several notification features, such as runtime notifications and licensing events.

Documentation restructuring

Improved

The PingFederate 13.0 documentation has been completely restructured to help customers get up and running faster, improve the overall flow, and make it easier to find information. This is an ongoing effort which will continue after the initial 13.0 release.

Jersey library

info PF-5069

We've upgraded the internal Jersey library to version 2.

This change will require you to upgrade some plugins. Learn more in Upgrade considerations.

Jetty library

info PF-36674

We've upgraded the Jetty library to version 12.0.

Log4j2 2.25.1

Info PF-37100

We've upgraded the log4j2 dependencies to version 2.25.1.

Apache Commons Lang libraries update

Info PF-37775

We've upgraded Apache `commons-lang` to version 2.6-p1 and `commons-lang3` to version 3.18.0 to continue alignment with maintained upstream dependencies.

TLS 1.3 support for Oracle Java 21

Info PF-37849

We've added support for TLS 1.3 for Oracle Java 21 with Thales and Entrust HSMs.

Bouncy Castle FIPS

Info PF-37943

We've upgraded Bouncy Castle to version 2.0.1. This version is certified to operate in Federal Information Processing Standards (FIPS) mode 140-3.

Amazon Aurora MySQL

Info PF-38045

We've qualified PingFederate for use with Amazon Aurora MySQL version 3.10 (compatible with MySQL 8.0.42).

PostgreSQL

Info PF-38048

We've qualified PingFederate for use with PostgreSQL version 18.0.

Oracle MySQL

Info PF-38053

We've qualified PingFederate for use with Oracle MySQL version 8.4. This version has an updated database driver. Learn more in Compatible database drivers.

Apache `commons-net` update

Info PF-38250

We've upgraded the Apache `commons-net` version to 3.12.0 to continue alignment with maintained upstream dependencies.

Resolved issues

Exposed credentials

Security PF-36848

We've fixed a security vulnerability in the admin console where passwords entered for certificate and key management were visible when navigating back to the previous page. Password fields are now masked.

Admin console IP exposure

Security PF-33113

We've fixed a security vulnerability that could have allowed malicious parties to extract PingFederate administrative console IP addresses using HTTP Response headers.

Session Revocation After Password Change

Security PF-36426

After a successful PingFederate administrative password change, all other active concurrent sessions for that administrative account are now immediately invalidated, enhancing security and requiring reauthentication with the new credentials.

`jackson-core` update

Security PF-37460

We've upgraded `jackson-core` to version 2.20.0 to continue alignment with maintained upstream dependencies and remove potential security vulnerabilities.

Host header redirect

Security PF-37460

We've fixed a security vulnerability that could have allowed malicious parties to redirect PingFederate admin console traffic using a spoofed Host header.

HTML Form Adapter browser history

Security PF-37902

We've corrected a security regression in the **HTML Form Adapter** to ensure that password credentials are cleared from the browser immediately after form submission, mitigating a risk of residual exposure in the browser's memory.

User Enumeration in Policy Password Reset

Security PF-38044

PingFederate now prevents user enumeration in the **Policy** mode **Password Reset** flow by eliminating the observable difference between valid and invalid usernames.

`jakarta.mail` upgrade

Security PF-38245

We've upgraded `jakarta.mail` to 1.6.8 to continue alignment with maintained upstream dependencies.

Template Fix for Incorrect Language Variable

Fixed PF-25517

We've fixed a defect in several default template files where the language locale wasn't retrieved correctly.

JWT auth to support Azure

Fixed PF-35123

We've added private key JWT authentication support for Microsoft Azure AD as an OIDC provider.

AWS CloudHSM certificate linking

Fixed PF-37156

We've fixed a defect that caused failed AWS CloudHSM certificate linking to appear to succeed when the key alias was a value that was previously used in the environment.

Scope removal error

Fixed PF-37634

We've fixed a defect in the **Client Settings** menu where removing scopes using the search bar could result in removing the wrong scope.

JARM response with `error` parameter

Fixed PF-37688

We've fixed a defect where JARM responses with an `error` parameter caused PingFederate to return a `500` error. It now returns a `200` response with the appropriate error page.

Data Store Filter configuration

Fixed PF-36953

We've fixed a defect in **Authentication Policy Fragments** where input contract values and tracked parameters were missing from the **Data Store Filter** configuration page when setting up an **Attribute Source & User Lookup** for a local identity mapping.

Serialized OGNL Java objects

Fixed PF-37405

We've fixed a defect that caused JSON objects using OGNL expressions included in JWT request objects sent to the OIDC provider in OIDC IdP connections not to be serialized properly.

Removed Jetty log warnings

Fixed PF-37696

We've fixed a defect where unnecessary Jetty log warnings appeared after upgrading to new PingFederate versions.

ATM configuration error

Fixed PF-37716

We've fixed a defect that caused an error in PingFederate when configuring an access token manager if the administrative node (ATM) isn't the coordinator node.

Refresh token error

Fixed PF-37722

We've fixed a defect where PingFederate returned an incorrect error when a refresh token was used by a different client after the original client was deleted.

Data Store naming consistency

Fixed PF-37732

We've fixed a terminology inconsistency in the PingFederate UI and changed **Data-Store** to **Data Store** in **General settings**.

`authorization_details` access token inclusion

Fixed PF-37743

We've fixed a defect that omitted the `authorization_details` parameter from the access token if the value was an empty array.

SNI extension error in BCFIPS mode

Fixed PF-37793

PingFederate now always includes the SNI extension in the ClientHello message during a TLS handshake when running in BCFIPS mode.

Wildcard TLS certificate error in BCFIPS mode

Fixed PF-37794

We've fixed a defect where PingFederate was refusing wildcard TLS certificates when running in BCFIPS mode.

Overly detailed Kerberos error messages

Fixed PF-37798

We've fixed a defect that caused lengthy stacktrace data to be included in ERROR level logging for Kerberos errors.

`PingFailoverAppender` race condition

Fixed PF-37816

We've fixed a defect where a race condition could cause the `PingFailoverAppender` to get stuck in a failed state without switching back to its primary appender.

DPoP proof JWTs with future `iat` value

Fixed PF-37818

We've fixed a defect where PingFederate incorrectly accepted DPoP proof JWTs with a future `iat` value.

`ClassNotFoundException` error

Fixed PF-37819

We've fixed an issue that could cause `ClassNotFoundException` on the admin console.

JWT API authentication method

Fixed PF-37841

We've added JWT as an authentication method for the admin API during upgrade utility validation.

Unused DevOps file

Fixed PF-37846

We've removed an unused file associated with the PingOne Advanced Identity Cloud DevOps deployment that was mistakenly included in the PingFederate Server `.zip` archive.

Forgot password flow failure

Fixed PF-37918

We've fixed a defect that caused the forgot password flow to fail when reCAPTCHA is enabled and the flow is initiated using the Enter key rather than a mouse click.

Password Credential Validator message override error

Fixed PF-37942

We've fixed a defect where overriding the reset password message in a Password Credential Validator incorrectly returned a generic `VALIDATION_ERROR` during the redirectless flow, preventing users who are required to change their password from receiving the necessary `MUST_CHANGE_PASSWORD` status and associated `_links`.

Enhanced logging for IdP connections

Fixed PF-37952 PF-37953

Logging for IdP connections now includes greater detail when handling invalid state parameters and failing PAR requests.

Virtual hostname accuracy in email notifications

Fixed PF-37964

We've fixed a defect where a template variable incorrectly used the primary PingFederate base URL instead of the virtual hostname in some email notifications.

URL validation for `RelayState`

Fixed PF-38028

We've fixed a defect where PingFederate would reject requests with valid, non-encoded relay state values.

HTML flow login and Authentication API

Fixed PF-38039

We've fixed a defect that could potentially allow a user to access an HTML browser sign-on page when the Authentication API redirectless mode is used.

Learn more in PingFederate unexpected template rendering in redirectless mode in the Ping Identity Support Knowledge Base.

New device speed bump parameter default

Fixed PF-38040

We've fixed a defect where the `show-speed-bump-for-new-devices` parameter in the `org.sourceid.servlet.filter.SimultaneousAuthnRequestCheckingFilter.xml` file was set to `true` instead of `false` by default.

The new behavior enables `show-speed-bump-for-new-devices` by default for new installs, but disables it by default for upgrades, if the source version doesn't have the parameter configured.

LDAP account lockout

Fixed PF-38043

We've fixed a defect where PingFederate could incorrectly lock user accounts during an LDAP connectivity failure with Active Directory. This applies to all LDAP datastore types except for Generic LDAP.

JARM IdP connections

Fixed PF-38052

When PingFederate is configured to expect a JARM-secured JWT response from an IdP, it enforces this requirement by failing the transaction if a plain response is received instead, and logs the details for administrator investigation.

IdP Adapter duplicate attribute sources

Fixed PF-38060

We've fixed a defect that caused IdP adapters to duplicate attribute sources when an SP connection was updated using the Admin API.

Cluster Management message fix

Fixed PF-38116

We've fixed a defect where **Cluster Management** would present an incorrect success message although the replication failed.

Connection ID in Invalid Signature audit logs

Fixed PF-38123

We've fixed a defect in SAML audit logging by making sure that entries recorded for "Invalid signature" failures now correctly include the associated Connection ID.

`$adapterId` population issue

Fixed PF-38146

We've fixed a defect where the `$adapterId` variable wasn't being populated in templates accessed through direct links for the HTML Form Adapter's **Change Password** and **Forgot Password** flows.

Trace logging for error information

Fixed PF-38210

We've added trace logging to the RP-initiated logout endpoint to explicitly detail session and token claims, allowing administrators to pinpoint why the logout confirmation page isn't

bypassed despite successful `id_token_hint` validation.

Server startup validation

Fixed PF-38243

We've added stricter validation during server startup so that PingFederate immediately halts the boot process and logs an error if an invalid or unrecognized value is detected for the `pf.hsm.mode` property in `run.properties`.

Corrected null `SaasGuid`

Fixed PF-38244

We've fixed a provisioning defect where disabled users weren't provisioned once their account was enabled and the **Provision Disabled Users** setting was set to false.

`X-Forward-For` IP

Fixed PF-38251

We've fixed a defect where the `X-Forward-For` IP wasn't logged correctly in the `admin.log`.

Tapestry startup error

Fixed PF-38284

We've fixed a Tapestry error that was incorrectly logged during startup for the SCIM 2.0 Inbound Provisioning component, even when the feature wasn't enabled or configured.

Kerberos Adapter redirect URL

Fixed PF-38328

We've fixed a defect where the Kerberos Adapter failed to authenticate when a context path is configured.

Administrative API authentication fix

Fixed PF-38393

We've fixed a defect that allowed Basic Authentication to access the Administrative API, even when it was disabled in the `pf.admin.api.authentication` property.

OAuth error code fix

Fixed PF-38468

We've fixed a defect where the `/as/introspect.oauth2` endpoint incorrectly returned a `500 Internal Server Error` instead of the expected `400 Bad Request` when the **`token`** parameter contained an invalid character like `%`.

Known issues and limitations

PingOne Verify IK unexpected error

Issue PF-36573

PingFederate returns an unexpected error when you create an instance of the PingOne Verify Integration Kit version 2.2.2 in PingFederate with the Verify feature in PingOne disabled.

Third-party cookie blocking affecting single logout

Issue PF-35772

Due to multiple vendors' recent browser versions that block third-party cookies, you might experience issues related to single logout with OIDC (via Front-Channel) and WS-Federation.

Refer to browsers' documentation regarding third-party cookie management to unblock them, if feasible.

Passive admin console UI refresh

Issue PF-35643

When you promote a passive admin console to active, the UI doesn't refresh until you perform an action.

Multiple active admin consoles

Issue PF-35439

When you make configuration changes on the active console (especially large configuration changes like bulk imports or data archive imports), then promote a passive console to active, it can cause multiple consoles to be active at once. This can result in inconsistent configurations.

Learn how to resolve this issue in Resolving multiple active administrative nodes.

Administrative console and administrative API

Issue

- Although PingFederate 11.3 and later support DPoP, a known limitation is that the following features don't support DPoP when PingFederate is the RP:
  - The administrative console authentication scheme using OIDC
  - The administrative API authentication scheme using OAuth 2.0
- /bulk: Only resource types currently supported by the administrative API are included in the exported data. We don't intend to introduce administrative API support to the following areas:
  - SAML 2.0 IdP Discovery
  - SAML 2.0 SP Affiliation
  - SMS Provider
- Previously, the administrative API did not accurately reflect a **Persistent Grant Max Lifetime** setting of 29 days (or shorter) with the selection of the **Grants Do Not Timeout Due To Inactivity** option. As a result, if you have configured such OAuth authorization server settings and have generated a bulk export in version 10.0 through 10.0.2, we recommend that you re-generate a new bulk export after upgrading to version 10.0.3 (or a more recent version). The newly exported data does not contain

the aforementioned flaw, and you can safely import it to version 10.0.3 (or a more recent version).

- When enabling mTLS certificate-based authentication, administrators often configure a list of acceptable client certificate issuers. When you use a browser to access the console or the administrative API documentation, PingFederate returns to the browser the list of acceptable issuers as part of the TLS handshake. If the browser's client certificate store contains multiple client certificates, the browser often presents you only the certificates whose issuer matches one of the acceptable issuers. However, when PingFederate runs in a Java 17 environment, Chrome presents you all its configured client certificates, regardless of whether the issuer matches one of the acceptable issuers or not.
- When using mTLS authentication to authenticate to an LDAP server for administrative console or administrative API access, PingFederate doesn't support using a Microsoft Active Directory server.
- Prior to toggling the status of a connection with the administrative API, you must ensure that any expired certificates or no longer available attributes are replaced with valid certificates or attributes; otherwise, the update request fails.
- When creating or updating a child instance of a hierarchical plugin, the administrative API retains objects with an `"inherited": false` name/value pair (or without such name/value pair altogether), ignores those with a value of `true`, and returns a 200 HTTP status code. No error messages are returned for the ignored objects.
- Using the browser's navigation mechanisms (for example, the **Back** button) causes inconsistent behavior in the administrative console. Use the navigation buttons provided at the bottom of windows in the PingFederate console.
- Using the PingFederate console in multiple tabs on one browser might cause inconsistent behavior which could corrupt its configuration.
- If authenticated to the PingFederate administrative console using certificate authentication, a session that has timed out might 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 sign-on page, and then back to the administrative console after authentication is complete. Similar behavior applies for certificate authentication, in principle. However, because the browser might automatically resubmit the certificate for authentication, the browser might redirect to the administrative console and not the sign on page.

TLS cipher suite customization

Issue

PingFederate's TLS cipher suites can be customized by modifying `com.pingidentity.crypto.SunJCEManager.xml` (or a similarly-named file if BCFIPS or an HSM is configured). After updating the file and replicating, all cluster nodes must be restarted for the change to take effect.

Java

Issue

- Updating Java version 8 to version 11 results in an error when PingFederate is already installed and running on Windows. To work around this issue, uninstall and reinstall the PingFederate Windows service by running the `UninstallPingFederateService.bat` and `InstallPingFederateService.bat` files located in `<pf_install>/pingfederate/sbin/wrapper`.

HSMs

Issue

AWS CloudHSM

- It is not possible to use an elliptic curve (EC) certificate as an SSL server certificate.
- When creating an EC certificate with a `signatureAlgorithm` smaller than the `keySize` value, a `500 Server error` occurs. For example, a `signatureAlgorithm` of `SHA256withECDSA` with a `keySize` of `384` results in an error. Learn more in ECDSA signing fails with "invalid mechanism" error starting with SDK 5.16 in the CloudHSM documentation.
- TLS 1.3 is not currently supported with Oracle JDK 17 or 21.

Thales HSMs

- JWT token decryption using ECDH-ES may fail. This issue only arises if PingFederate is configured with static OAuth and OpenID Connect keys, a static key is stored on the HSM, and PingFederate is consuming a token encrypted with this key.

- It is not possible to use an EC certificate as an SSL server certificate.
- TLS 1.3 isn't currently supported with Oracle JDK 17.

Entrust HSMs

- JWT token decryption using ECDH-ES may fail. This issue only arises if PingFederate is configured with static OAuth and OpenID Connect keys, a static key is stored on the HSM, and PingFederate is consuming a token encrypted with this key.
- It is not possible to import a PKCS12- or PEM-formatted EC certificate.
- It is not possible to use an EC certificate as an SSL server certificate.
- TLS 1.3 isn't currently supported with Oracle JDK 17.

SSO and SLO

Issue

- When consuming SAML metadata, PingFederate does not report an error when neither the `validUntil` nor the `cacheDuration` attribute is included in the metadata. Note that PingFederate does reject expired SAML metadata as indicated by the `validUntil` attribute value, if it is provided.
- The anchored-certificate trust model cannot be used with the single logout (SLO) redirect binding because the certificate cannot be included with the logout request.
- 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.

Composite Adapter configuration

Issue

SLO is not supported when users are authenticated through a Composite Adapter instance that contains another instance of the Composite Adapter.

Self-service password reset

Issue

Passwords can be reset for Microsoft Active Directory user accounts without the permission to change password.

OAuth

Issue

PingFederate does not support a case-sensitive naming convention for OAuth client ID values when client records are stored in a directory server. For example, after creating a client with an ID value of `sampleClient`, PingFederate does not allow the creation of another client with an ID value of `SampleClient`.

Although it's possible to create clients using the same ID values with different casings when client records are stored in XML files, a database server, or custom storage, we recommend not doing so to avoid potential record migration issues.

Customer identity and access management

Issue

Some browsers display a date-picker user interface for fields that have been designed for date-specific inputs. Some browsers do not. If one or more date-specific fields are defined on the registration page or the profile management page (or both), end users must enter the dates manually if their browsers do not display a date-picker user interface for those fields.

Provisioning

Issue

- 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.
- The **`totalResults`** value in SCIM responses indicates the number of results returned in the current response, not the total number of estimated results on the LDAP server.

Logging

Issue

- 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, the `USER_KEY` attribute will not be masked in the server logs. Other persistent grant attributes will be masked.
- Even if a source attribute has been configured for masking in an IdP adapter and the source attribute is mapped as the adapter's unique user key, the user key attribute is not masked in the server or audit logs.

Database logging

Issue

- 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, the `USER_KEY` attribute will not be masked in the server logs. Other persistent grant attributes will be masked.
- Even if a source attribute has been configured for masking in an IdP adapter and the source attribute is mapped as the adapter's unique user key, the user key attribute is not masked in the server or audit logs.

RADIUS NAS-IP-Address

Issue

The RADIUS NAS-IP-Address is only included in Access-Request packets when the `pf.bind.engine.address` is set with an IPv4 address. IPv6 is not supported.

Amazon SNS Notification Publisher

Issue

When deploying PingFederate with a forward proxy, plugins based on the AWS SDK, such as the Amazon SNS Notification Publisher, will only honor the `http.proxyHost`, `http.proxyPort`, `http.proxyUser`, and `http.proxyPassword` properties in `run.properties`. The plugin will rely on these properties even if the service URL is `https`.

Deprecated features

No features were deprecated for PingFederate 13.0.

PingFederate 12.3.7 (July 2026)

Resolved issues

Log4j update to 2.25.4

Security PF-39063

We updated log4j-core, log4j-1.2-api, and log4j-layout-template-json to version 2.25.4 to address potential security vulnerabilities.

Response code for refresh token exchange failure with revoked user session

Fixed PF-38656

We fixed a defect that caused a refresh token for access token exchange to fail with `500 Internal Server Error` instead of `400 Bad Request` when the user's sessions had been revoked.

Extended Property Authentication Selector dependency error warning

Fixed PF-38901

We fixed a defect that caused PingFederate to continue displaying a dependency error warning for the Extended Property Authentication Selector after the selector instance is deleted.

Kerberos realm test failure

Fixed PF-39487

We fixed a defect that caused Kerberos realm test connections without explicitly configured KDCs to fail.

JWT access token revocation fails with shared signing keys

Fixed PF-39526

We fixed a defect that could prevent revocation of a JWT access token when multiple JWT access token managers (ATMs) shared signing keys. PingFederate now identifies the ATM that issued the token and uses it to perform revocation.

PingFederate 12.3.6 (April 2026)

New features & enhancements

Unconnected cluster node startup

Improved PF-38898

We added the `force.require.replication.data.on.startup` parameter to the `cluster-config-replication.conf` file.

This parameter lets you prevent an engine node from starting up without establishing a connection to the cluster.

Learn more in Cluster management.

Resolved issues

OGNL code test

Security PF-38742

We improved role-based access control (RBAC) for the administrative expression testing endpoint. Access to expression evaluation is now limited to appropriately privileged roles, ensuring alignment with intended administrative permissions.

CIBA token request fails with LDAP persistent grant storage

Fixed PF-38706

We fixed a defect that caused CIBA token requests to fail when persistent grants are stored in an LDAP directory such as PingDirectory.

Admin API OAuth authentication failure

Fixed PF-38722

We fixed a defect that caused OAuth and JWT authentication through the Admin API to fail when the `role attribute name` parameter used the scope claim containing space-delimited values.

Multiple Sign-On Delay routing

Fixed PF-38801

We fixed a defect that caused PingFederate to route users to the base URL for the Multiple Sign-On Delay page when they should've been routed to the virtual host URL.

Custom Authentication Selector error

Fixed PF-38875

We fixed a defect that prevented viewing or editing certain custom Authentication Selectors in the admin console.

Dynamic JWKS rotation timer

Fixed PF-38903

We fixed a defect that prevented dynamic JWKS rotation timing from resetting after a node joined a cluster.

URL validation for `TargetResource`

Fixed PF-38907

We fixed a defect where PingFederate rejected valid `TargetResource` values.

PingFederate 12.3.5 (February 2026)

New features and enhancements

PAR parameters

Info PF-38526

We've added a new configuration option to limit the Pushed Authorization Request (PAR) to the parameters mentioned in the specification when the connection is configured to use JWT-secured Authorization Request (JAR).

Resolved issues

User Enumeration in Policy Password Reset

Security PF-38628

PingFederate now prevents user enumeration in the **Policy** mode **Password Reset** flow by eliminating the observable difference between valid and invalid usernames.

Serialized OGNL Java objects

Fixed PF-37405

We've fixed a defect that caused JSON objects using OGNL expressions included in JWT request objects sent to the OIDC provider in OIDC IdP connections not to be serialized properly.

Kerberos realm validation error

Fixed PF-38585

We've fixed a defect that prevented PingFederate from creating, updating, or testing Kerberos realms when the `AutoGenerateKrb5Conf` parameter was set to `false` in the `com.pingidentity.common.util.KerberosConfigUtil` file.

Authentication policy error

Fixed PF-38623

We've fixed a defect that caused an error when authentication policies with a Requested AuthN Context Authentication had **Add or Update AuthN Context Attribute** enabled.

PingFederate 12.3.4 (December 2025)

Resolved issues

URL validation for `RelayState`

Fixed PF-38028

We've fixed a defect where PingFederate would reject requests with valid, non-encoded relay state values.

LDAP account lockout

Fixed PF-38043

We've fixed a defect where PingFederate could incorrectly lock user accounts during an LDAP connectivity failure with Active Directory. This applies to all LDAP datastore types except for Generic LDAP.

Cluster Management message fix

Fixed PF-38116

We've fixed a defect where **Cluster Management** would present an incorrect success message although the replication failed.

`$adapterId` population issue

Fixed PF-38146

We've fixed a defect where the `$adapterId` variable wasn't being populated in templates accessed through direct links for the HTML Form Adapter's **Change Password** and **Forgot Password** flows.

Corrected null `SaasGuid`

Fixed PF-38244

We've fixed a provisioning defect where disabled users weren't provisioned after their account was enabled and the **Provision Disabled Users** setting was set to false.

`X-Forward-For` IP

Fixed PF-38251

We've fixed a defect where the `X-Forward-For` IP wasn't logged correctly in the `admin.log`.

Kerberos Adapter redirect URL

Fixed PF-38328

We've fixed a defect where the Kerberos Adapter failed to authenticate when a context path is configured.

JWT Admin AI authentication misconfiguration

Fixed PF-38336

We've fixed a defect that caused PingFederate to crash or shut down when attempting to access the Admin API with a misconfigured JSON Web Token (JWT) authentication setup.

Administrative API authentication fix

Fixed PF-38393

We've fixed a defect that allowed Basic Authentication to access the Administrative API, even when it was disabled in the `pf.admin.api.authentication` property.

`pi.flow response_mode` fix

Fixed PF-38417

We've fixed a defect where setting `response_mode` to `pi.flow` in Pushed Authorization Requests (PAR) or standard request objects resulted in an `INVALID_REQUEST` error.

PingFederate 12.3.3 (October 2025)

Resolved issues

TLS 1.3 support for Oracle Java 21

Info PF-37849

We've added support for TLS 1.3 for Oracle Java 21 with Thales and Entrust HSMs.

Forgot password flow failure

Fixed PF-37918

We've fixed a defect that caused the forgot password flow to fail when reCAPTCHA is enabled and the flow is initiated using the Enter key rather than a mouse click.

Virtual hostname accuracy in email notifications

Fixed PF-37964

We've fixed a defect where a template variable incorrectly used the primary PingFederate base URL instead of the virtual host name in some email notifications.

New device speed bump parameter default

Fixed PF-38040

We've fixed a defect where the `show-speed-bump-for-new-devices` parameter in the `org.sourceid.servlet.filter.SimultaneousAuthnRequestCheckingFilter.xml` file

was set to `true` instead of `false` by default.

The new behavior enables **`show-speed-bump-for-new-devices`** by default for new installs, but disables it by default for upgrades, if the source version doesn't have the parameter configured.

IdP Adapter duplicate attribute sources

Fixed PF-38060

We've fixed a defect that caused IdP adapters to duplicate attribute sources when an SP connection was updated using the Admin API.

HTML flow login and Authentication API

Fixed PF-38039

We've fixed a defect that could potentially allow a user to access an HTML browser sign-on page when the Authentication API redirectless mode is used.

Learn more in **PingFederate unexpected template rendering in redirectless mode** in the Ping Identity Support Knowledge Base.

Known issues and limitations

HSMs

Issue

AWS CloudHSM

- It is not possible to use an elliptic curve (EC) certificate as an SSL server certificate.
- When creating an EC certificate with a `signatureAlgorithm` smaller than the `keySize` value, a `500 Server error` occurs. For example, a `signatureAlgorithm` of `SHA256withECDSA` with a `keySize` of `384` results in an error. Learn more in **ECDSA signing fails with "invalid mechanism" error starting with SDK 5.16** in the CloudHSM documentation.
- TLS 1.3 is not currently supported with Oracle JDK 11, 17, or 21.

Thales HSMs

- JWT token decryption using ECDH-ES may fail. This issue only arises if PingFederate is configured with static OAuth and OpenID Connect keys, a static key is stored on the HSM, and PingFederate is consuming a token encrypted with this key.
- It is not possible to use an EC certificate as an SSL server certificate.
- TLS 1.3 isn't currently supported with Oracle JDK 11 or 17.

Entrust HSMs

- JWT token decryption using ECDH-ES may fail. This issue only arises if PingFederate is configured with static OAuth and OpenID Connect keys, a static key is stored on the HSM, and PingFederate is consuming a token encrypted with this key.
- It is not possible to import a PKCS12- or PEM-formatted EC certificate.
- It is not possible to use an EC certificate as an SSL server certificate.
- TLS 1.3 isn't currently supported with Oracle JDK 11 or 17.

PingFederate 12.3.2 (September 2025)

New features and enhancements

Jetty library

info PF-37936

We've upgraded the Jetty library to version 10.0.26

Bouncy Castle FIPS

info PF-37943

We've upgraded Bouncy Castle to version 2.0.1. This version is certified to operate in Federal Information Processing Standards (FIPS) mode 140-3.

Resolved issues

AWS CloudHSM certificate linking

Fixed PF-37156

We've fixed a defect that caused failed AWS CloudHSM certificate linking to appear to succeed when the key alias was a value that was previously used in the environment.

`authorization_details` access token inclusion

Fixed PF-37743

We've fixed a defect that omitted the `authorization_details` parameter from the access token if the value was an empty array.

Overly detailed Kerberos error messages

Fixed PF-37798

We've fixed a defect that caused lengthy stacktrace data to be included in ERROR level logging for Kerberos errors.

`PingFailoverAppender` race condition

Fixed PF-37816

We've fixed a defect where a race condition could cause the `PingFailoverAppender` to get stuck in a failed state without switching back to its primary appender.

Admin console ClassNotFoundException error

Fixed PF-37819

We've fixed a defect that could cause `ClassNotFoundException` errors in the admin console.

JWT API authentication method

Fixed PF-37841

We've fixed a defect where JWT wasn't a valid authentication method for the admin AP during upgrade utility validation.

Unused DevOps file

Fixed PF-37846

We've removed an unused file associated with the PingOne Advanced Identity Cloud DevOps deployment that was mistakenly included in the PingFederate Server `.zip` archive.

PingFederate 12.3.1 (August 2025)

New features and enhancements

Apache version upgrade

New PF-37674

We've upgraded the Apache `commons-fileupload` version to 1.6.0.

Resolved issues

Admin console IP exposure

Security PF-33113

We've fixed a security vulnerability that could have allowed malicious parties to extract the PingFederate administrative console's IP address through HTTP Response headers.

Host header redirect

Security PF-37460

We've fixed a security vulnerability that could have allowed malicious parties to redirect PingFederate admin console traffic using a spoofed Host header.

PingDirectory PCV error messaging

Fixed PF-37452

We've fixed a defect where disabling `PingDirectory Detailed Password Policy Requirement Messaging` caused password validation errors to not show up in the Authn API.

Firefox Kerberos negotiation

Fixed PF-37559

We've fixed a defect that caused Kerberos negotiations to fail with Firefox after the initial exchange.

CSD error in BCFIPS mode

Fixed PF-37667

We've fixed a defect that caused an error in the CSD when running in BCFIPS mode.

IdP connection Admin API error

Fixed PF-37670

We've fixed a defect that caused a failure when creating or updating an IdP connection with the `CLAIMS` source type in JIT provisioning user attribute mapping using the Administrative API.

Admin console and API alignment

Fixed PF-37673

We've fixed a defect where the Admin Console allowed configuring an IdP connection without a client secret, but the Admin API returned an error. The Admin API no longer returns an error in this case.

JARM response with `error` parameter

Fixed PF-37688

We've fixed a defect where JARM responses with an `error` parameter caused PingFederate to return a `500` error. It now returns a `200` response with the appropriate error page.

ATM configuration error

Fixed PF-37716

We've fixed a defect that caused an error in PingFederate when configuring an access token manager if the administrative node (ATM) isn't the coordinator node.

Write Users attributes causing validation failures

Fixed PF-37776

We've fixed a defect where certain SCIM attribute mappings were incorrectly causing validation failures when updating IdP connections through the Admin API.

SNI extension error in BCFIPS mode

Fixed PF-37793

PingFederate now always includes the SNI extension in the ClientHello message during a TLS handshake when running in BCFIPS mode.

Wildcard TLS certificate error in BCFIPS mode

Fixed PF-37794

We've fixed a defect where PingFederate was refusing wildcard TLS certificates when running in BCFIPS mode.

PingFederate 12.3 (June 2025)

New features and enhancements

Audit log failure behavior

New PF-36795 PF-36817

We've added a feature that allows you to configure how PingFederate responds when writing to the audit log fails.

This feature can improve user experience by allowing PingFederate to continue processing transactions when logging fails.

Learn more in Configuring audit log failure settings.

Remove IP address from account lockout criteria

New PF-36818

We've added the ability to remove a user's IP address from consideration when making account lockout decisions.

This can improve security by preventing malicious actors from masking their IP address to bypass account lockouts.

Learn more in Configuring account lockout protection.

CORS support for admin API endpoints

New PF-36856

We've added a feature that allows you to grant cross-origin resource sharing (CORS) access to administrative API endpoints.

This makes it more secure and convenient for web applications like PingAccess to perform administrative tasks in PingFederate.

Learn more in Configuring administrative API CORS settings.

Validate OIDC ID tokens

New PF-36860

We've added the ability to validate an ID token in the introspection endpoint as part of an OpenID Connect (OIDC) policy. You can enable this feature as part of a policy, but the runtime flows occur at the introspection endpoint.

This improves security by allowing PingFederate to determine whether a user's ID token is valid.

Learn more in Configuring policy and ID token settings and Introspection endpoint.

Always return scopes in client credentials response

New PF-36862

We've added a feature that allows you to always return the scope parameter in the response to client credential requests.

This allows you return scopes if clients require scopes that users haven't authorized.

Learn more in Returning scopes in authorization transactions

Link and store CloudHSM keys

New PF-36871 PF-37272

We've added a feature that allows you to link private keys stored in Amazon Web Services (AWS) CloudHSM with their certificates, and store it in PingFederate's Java keystore.

This allows you to use existing private key and certificate pairs associated with your CloudHSM instance in PingFederate.

Learn more in Link and store CloudHSM keys.

Correlating log events with attributes

New PF-36875

We've added the ability to correlate log events between the `audit.log`, `request.log`, and `server.log` files using shared log attributes.

This can make it easier to trace the cause of runtime errors.

Learn more in Correlating log events using attributes.

Duplicate RSA key

New PF-36970

We've added a feature that gives you the option to include a duplicate RSA key with the RS256 algorithm. You can enable this option by setting the `add-duplicate-rs256-alg-key` parameter in the `<pingfed-install>/pingfederate/server/default/data/config-store/jwks-endpoint-configuration.xml` file to `true`.

HTTP request logging

New PF-36976

We've updated the logging for HTTP requests to the runtime engine and admin console. These requests are now logged to the `runtime-request.log` and `admin-request.log` files. Like other PingFederate logs, you can configure outputs for these files in `log4j2.xml`.

This improves logging efficiency and customization by writing HTTP request logs using the same configurations as other PingFederate log files.

Learn more in HTTP request logging.

Revoke previous client secrets

New PF-37183

We've added a feature that allows you to revoke previous OAuth client secrets.

This improves security by allowing you to revoke secrets that are no longer in use. For example, if you move your client to a new secret before the old secret's grace period ends, you can use this feature to revoke your previous secret.

Learn more in Configuring OAuth clients.

DynamoDB persistent grant storage

New PF-37192

When storing persistent grants in DynamoDB, DynamoDB relies on the DynamoDB Time to Live (TTL) attribute to remove expired persistent grants from the database. Learn more in Configuring external databases for grant storage.

Publish certificate for dynamic keys

New PF-37219

We've added a feature that allows dynamic signing keys to publish their public certificates on the JWKS endpoint as an `x5c` parameter. Learn more in Configuring dynamic signing keys

SCIM 2.0 supported for inbound user provisioning

New PF-37230

PingFederate now supports the SCIM 2.0 protocol for inbound user provisioning. Learn more in System for Cross-domain Identity Management (SCIM).

User session quotas

New PF-37238

We've added a feature that allows you to limit the number of sessions a user can have active at one time and configure how PingFederate responds when that quota is exceeded.

This can improve security by limiting the number of active user sessions that have access to applications and other resources.

Learn more in Configuring session quotas.

`client_assertion` attribute configuration

New PF-37275

We've added a feature that allows you to configure the `client_assertion` for JWT-based authentications by customizing the following attributes:

- `aud`
- `lifetime`
- `typ`
- `nbf`

Learn more in Configuring OpenID Provider information.

Bouncy Castle FIPS 2.0 compatibility

Info PF-36846

We've upgraded Bouncy Castle to version 2.0. This versions is certified to operate in Federal Information Processing Standards (FIPS) mode 140-3.

Java 21 compatibility

Info PF-36857

We've confirmed that PingFederate is compatible with Java 21.

Red Hat Enterprise Linux 8.10 compatibility

Info PF-36972

We've confirmed that PingFederate is compatible with Red Hat Enterprise Linux ES 8.10.

Integration Kit template parameters

Info PF-37102

We've updated PingFederate to use the same default template parameters for all integration kits.

Learn more about template parameters in Customizable user-facing pages.

Authentication policies list readability

Info PF-37221

- The Policies UI in the administrative console now collapses long lists of authentication sources by default. Users can easily expand or collapse these lists as needed, making it easier to navigate and manage policies.
- We've added a **Selectors** column to the Policies overview, providing a list of the selectors used in each policy.

NATIVE_S3_PING update

Info PF-37234

We've updated the behavior of the NATIVE_S3_PING discovery protocol when the `remove_all_data_on_view_change` parameter is active.

Previously, the protocol would delete all files in the S3 bucket, which could lead to the creation of an unwanted subcluster.

Now the protocol deletes all files except for its own to prevent the S3 bucket from being empty.

Learn more in Dynamic cluster discovery.

Java Service Wrapper update

Info PF-37236

We've updated the Java Service Wrapper to the latest version, 3.5.60.

Learn more in the Tanuki release notes.

Amazon Aurora MySQL 3.09 compatibility

Info PF-37277

We've confirmed that PingFederate is compatible with Amazon Aurora MySQL 3.09.

PingOne Singapore region

Info PF-37451

We've added support for the new PingOne Singapore region, `pingone.sg`.

Resolved issues

d3-color library

Security PF-36745

We've fixed a security vulnerability that could allow denial of service attacks using legacy `d3-color` library versions.

Refresh token MySQL deadlocks

Fixed PF-35868

We've fixed a defect that caused multiple refresh token requests in short succession to result in Java database connectivity (JDBC) data source deadlocks and duplicated data entry into the database.

This feature can cause significant performance issues if PingFederate or the JDBC data source have insufficient resources.

Reencrypt data archive failure with KMS

Fixed PF-36487

We've fixed a defect where importing a valid configuration data archive with **Reencrypt Data** enabled failed with a `Could not reencrypt data archive` error message when configured to use the Amazon Web Services or Google Cloud Platform Key Management System (KMS).

Expired grants reuse

Fixed PF-36568

We've fixed a defect that allowed the use of OAuth grants that have passed idle timeout, but not expired, to be retrieved from persistent grant storage.

Access token manager Admin API error

Fixed PF-36845

We've fixed a defect that caused a `500` error when creating or updating an access token manager using the Administrative API.

Refresh token error when authorization bypass enabled

Fixed PF-36851

We've fixed a defect that caused PingFederate to return a revoked or expired consent error when both **Bypass Authorization Approval** and **Bypass Authorization Approval for Previously Approved Consents** are enabled.

This is My Device error on HTML Form Adapter

Fixed PF-36864

We've fixed a defect that caused PingFederate to behave inconsistently when **This is My Device** is selected and an HTML Form Adapter instance has more than one session configuration in the session overrides.

TLS connection in BCFIPS mode

Fixed PF-36865

We've fixed a defect where PingFederate could not accept a TLS 1.2 connection in BCFIPS mode on Java 17.

Group membership loss during provisioning

Fixed PF-36874

We've fixed a defect that caused PingFederate to lose user group membership information when it lost contact with the datastore during provisioning operations.

Jetty Upgrade redirect errors

Fixed PF-36877

We've fixed a defect where upgrading to Jetty library version 9.5.53 caused HTTP header compression errors when redirect URLs included special characters.

Change password failure with PingOne Protect

Fixed PF-37012

We've fixed a defect that caused the HTML Form Adapter Change Password using an authentication policy to fail when PingOne Protect is the risk provider.

OGNL expressions with SDK classes

Fixed PF-37021

We've fixed a defect that caused OGNL expressions to fail to load when they contained SDK classes.

RP-initiated logout error

Fixed PF-37173

We've fixed a defect that caused PingFederate to ignore the `id_token_hint` value during relying party (RP)-initiated logout when the OAuth client logout mode is set to `None`.

Log rotation policy ignored

Fixed PF-37237

We've fixed a defect that caused PingFederate to ignore the log file size limit and rotation configurations set by the `SizeBasedTriggeringPolicy` parameter.

Secondary secret missing ID token claim

Fixed PF-37279

We've fixed a defect that caused the ID token claim to be omitted when an OAuth client uses the secondary secret.

Failed IdP connection with additional issuer

Fixed PF-37404

We've fixed a defect where an "IdP connection not found" error occurs when an authorization response includes an `iss` query parameter that doesn't match the connection's primary issuer, but is added as an additional issuer.

Simultaneous Administrative API requests

Fixed PF-37448

We've fixed a defect that caused configuration replication to fail when two or more simultaneous DELETE requests were sent to the Administrative API.

Unnecessary ID token reissued with secondary client secret

Fixed PF-37450

We've fixed a defect that caused the token endpoint to unnecessarily reissue an ID token when using a secondary client secret and an asymmetric algorithm for token signing and encryption.

Apache Commons BeanUtils

Fixed PF-37507

PingFederate now uses the Apache Commons BeanUtils library version 1.11.0.

Scope Groups Search

Fixed PF-37514

We've fixed a defect where the **Scopes Selection** modal prevented configurations from saving correctly when added using search.

Scopes with URL characters not updating

Fixed PF-37516

We've fixed a defect where OAuth scopes that included URL characters such as `/` couldn't be updated in the Admin portal.

Known issues and limitations

PingOne Verify IK unexpected error

Issue PF-36573

PingFederate returns an unexpected error when you create an instance of the PingOne Verify Integration Kit version 2.2.2 in PingFederate with the Verify feature in PingOne disabled.

Third-party cookie blocking affecting single logout

Issue PF-35772

Due to multiple vendors' recent browser versions that block third-party cookies, you might experience issues related to single logout with OIDC (via Front-Channel) and WS-Federation.

Refer to browsers' documentation regarding third-party cookie management to unblock them, if feasible.

Passive admin console UI refresh

Issue PF-35643

When you promote a passive admin console to active, the UI doesn't refresh until you perform an action.

Multiple active admin consoles

Issue PF-35439

When you make configuration changes on the active console (especially large configuration changes like bulk imports or data archive imports), then promote a passive console to

active, it can cause multiple consoles to be active at once. This can result in inconsistent configurations.

Learn how to resolve this issue in Resolving multiple active administrative nodes.

Administrative console and administrative API

Issue

- Although PingFederate 11.3 and later support DPoP, a known limitation is that the following features don't support DPoP when PingFederate is the RP:
  - The administrative console authentication scheme using OIDC
  - The administrative API authentication scheme using OAuth 2.0
- /bulk: Only resource types currently supported by the administrative API are included in the exported data. We don't intend to introduce administrative API support to the following areas:
  - SAML 2.0 IdP Discovery
  - SAML 2.0 SP Affiliation
  - SMS Provider
- Previously, the administrative API did not accurately reflect a **Persistent Grant Max Lifetime** setting of 29 days (or shorter) with the selection of the **Grants Do Not Timeout Due To Inactivity** option. As a result, if you have configured such OAuth authorization server settings and have generated a bulk export in version 10.0 through 10.0.2, we recommend that you re-generate a new bulk export after upgrading to version 10.0.3 (or a more recent version). The newly exported data does not contain the aforementioned flaw, and you can safely import it to version 10.0.3 (or a more recent version).
- When enabling mTLS certificate-based authentication, administrators often configure a list of acceptable client certificate issuers. When you use a browser to access the console or the administrative API documentation, PingFederate returns to the browser the list of acceptable issuers as part of the TLS handshake. If the browser's client certificate store contains multiple client certificates, the browser often presents you only the certificates whose issuer matches one of the acceptable issuers. However, when PingFederate runs in a Java 11 environment, Chrome presents you all its

configured client certificates, regardless of whether the issuer matches one of the acceptable issuers or not.

- When using mTLS authentication to authenticate to an LDAP server for administrative console or administrative API access, PingFederate doesn't support using a Microsoft Active Directory server.
- Prior to toggling the status of a connection with the administrative API, you must ensure that any expired certificates or no longer available attributes are replaced with valid certificates or attributes; otherwise, the update request fails.
- When creating or updating a child instance of a hierarchical plugin, the administrative API retains objects with an `"inherited": false` name/value pair (or without such name/value pair altogether), ignores those with a value of `true`, and returns a 200 HTTP status code. No error messages are returned for the ignored objects.
- Using the browser's navigation mechanisms (for example, the **Back** button) causes inconsistent behavior in the administrative console. Use the navigation buttons provided at the bottom of windows in the PingFederate console.
- Using the PingFederate console in multiple tabs on one browser might cause inconsistent behavior which could corrupt its configuration.
- If authenticated to the PingFederate administrative console using certificate authentication, a session that has timed out might 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 sign-on page, and then back to the administrative console after authentication is complete. Similar behavior applies for certificate authentication, in principle. However, because the browser might automatically resubmit the certificate for authentication, the browser might redirect to the administrative console and not the sign on page.

TLS cipher suite customization

Issue

PingFederate's TLS cipher suites can be customized by modifying `com.pingidentity.crypto.SunJCEManager.xml` (or a similarly-named file if BCFIPS or an HSM is configured). After updating the file and replicating, all cluster nodes must be restarted for the change to take effect.

Java

Issue

- Updating Java version 8 to version 11 results in an error when PingFederate is already installed and running on Windows. To work around this issue, uninstall and reinstall the PingFederate Windows service by running the `UninstallPingFederateService.bat` and `InstallPingFederateService.bat` files located in `<pf_install>/pingfederate/sbin/wrapper`.

HSMs

Issue

AWS CloudHSM

- It is not possible to use an elliptic curve (EC) certificate as an SSL server certificate.
- When creating an EC certificate with a `signatureAlgorithm` smaller than the `keySize` value, a `500 Server error` occurs. For example, a `signatureAlgorithm` of `SHA256withECDSA` with a `keySize` of `384` results in an error. Learn more in ECDSA signing fails with "invalid mechanism" error starting with SDK 5.16 in the CloudHSM documentation.
- TLS 1.3 is not currently supported with Oracle JDK 11, 17, or 21.

Thales HSMs

- JWT token decryption using ECDH-ES may fail. This issue only arises if PingFederate is configured with static OAuth and OpenID Connect keys, a static key is stored on the HSM, and PingFederate is consuming a token encrypted with this key.
- It is not possible to use an EC certificate as an SSL server certificate.
- TLS 1.3 is not currently supported with Oracle JDK 11, 17, or 21.

Entrust HSMs

- JWT token decryption using ECDH-ES may fail. This issue only arises if PingFederate is configured with static OAuth and OpenID Connect keys, a static key is stored on the HSM, and PingFederate is consuming a token encrypted with this key.

- It is not possible to import a PKCS12- or PEM-formatted EC certificate.
- It is not possible to use an EC certificate as an SSL server certificate.
- TLS 1.3 is not currently supported with Oracle JDK 11, 17, or 21.

SSO and SLO

Issue

- When consuming SAML metadata, PingFederate does not report an error when neither the `validUntil` nor the `cacheDuration` attribute is included in the metadata. Note that PingFederate does reject expired SAML metadata as indicated by the `validUntil` attribute value, if it is provided.
- The anchored-certificate trust model cannot be used with the single logout (SLO) redirect binding because the certificate cannot be included with the logout request.
- 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.

Composite Adapter configuration

Issue

SLO is not supported when users are authenticated through a Composite Adapter instance that contains another instance of the Composite Adapter.

Self-service password reset

Issue

Passwords can be reset for Microsoft Active Directory user accounts without the permission to change password.

OAuth

Issue

PingFederate does not support a case-sensitive naming convention for OAuth client ID values when client records are stored in a directory server. For example, after creating a client with an ID value of `sampleClient`, PingFederate does not allow the creation of another client with an ID value of `SampleClient`.

Although it's possible to create clients using the same ID values with different casings when client records are stored in XML files, a database server, or custom storage, we recommend not doing so to avoid potential record migration issues.

Customer identity and access management

Issue

Some browsers display a date-picker user interface for fields that have been designed for date-specific inputs. Some browsers do not. If one or more date-specific fields are defined on the registration page or the profile management page (or both), end users must enter the dates manually if their browsers do not display a date-picker user interface for those fields.

Provisioning

Issue

- 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.
- The **`totalResults`** value in SCIM responses indicates the number of results returned in the current response, not the total number of estimated results on the LDAP server.

Logging

Issue

- 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, the **`USER_KEY`** attribute will not be masked in the server logs. Other persistent grant attributes will be masked.

- Even if a source attribute has been configured for masking in an IdP adapter and the source attribute is mapped as the adapter's unique user key, the user key attribute is not masked in the server or audit logs.

Database logging

Issue

- 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, the `USER_KEY` attribute will not be masked in the server logs. Other persistent grant attributes will be masked.
- Even if a source attribute has been configured for masking in an IdP adapter and the source attribute is mapped as the adapter's unique user key, the user key attribute is not masked in the server or audit logs.

RADIUS NAS-IP-Address

Issue

The RADIUS NAS-IP-Address is only included in Access-Request packets when the `pf.bind.engine.address` is set with an IPv4 address. IPv6 is not supported.

Amazon SNS Notification Publisher

Issue

When deploying PingFederate with a forward proxy, plugins based on the AWS SDK, such as the Amazon SNS Notification Publisher, will only honor the `http.proxyHost`, `http.proxyPort`, `http.proxyUser`, and `http.proxyPassword` properties in `run.properties`. The plugin will rely on these properties even if the service URL is `https`.

Deprecated features

No features were deprecated for PingFederate 12.3.

PingFederate 12.2.8 (May 2026)

New features & enhancements

Unconnected cluster node startup

Improved PF-38898

We added the `force.require.replication.data.on.startup` parameter to the `cluster-config-replication.conf` file.

This parameter lets you prevent an engine node from starting up without establishing a connection to the cluster.

Learn more in Cluster management.

Resolved issues

OGNL code test

Security PF-38742

We improved role-based access control (RBAC) for the administrative expression testing endpoint. Access to expression evaluation is now limited to appropriately privileged roles, ensuring alignment with intended administrative permissions.

Multiple Sign-On Delay routing

Fixed PF-38801

We fixed a defect that caused PingFederate to route users to the base URL for the Multiple Sign-On Delay page when they should’ve been routed to the virtual host URL.

Custom Authentication Selector error

Fixed PF-38875

We fixed a defect that prevented viewing or editing certain custom Authentication Selectors in the admin console.

Extended Property Authentication Selector dependency error warning

Fixed PF-38901

We fixed a defect that caused PingFederate to continue displaying a dependency error warning for the Extended Property Authentication Selector after the selector instance is deleted.

Dynamic JWKS rotation timer

Fixed PF-38903

We fixed a defect that prevented dynamic JWKS rotation timing from resetting after a node joined a cluster.

PingFederate 12.2.7 (February 2026)

Resolved issues

Kerberos Adapter redirect URL

Fixed PF-38328

We've fixed a defect where the Kerberos Adapter failed to authenticate when a context path is configured.

JWT Administrative API authentication misconfiguration

Fixed PF-38336

We've fixed a defect that caused PingFederate to crash or shut down when attempting to access the Administrative API with a misconfigured JWT authentication setup.

Administrative API authentication fix

Fixed PF-38393

We've fixed a defect that allowed Basic Authentication to access the Administrative API, even when it was disabled in the `pf.admin.api.authentication` property.

`pi.flow response_mode` fix

Fixed PF-38417

We've fixed a defect where setting **`response_mode`** to `pi.flow` in Pushed Authorization Requests (PAR) or standard request objects resulted in an `INVALID_REQUEST` error.

Authentication policy error

Fixed PF-38623

We've fixed a defect that caused an error when authentication policies with a Requested AuthN Context Authentication had **Add or Update AuthN Context Attribute** enabled.

PingFederate 12.2.6 (November 2025)

Resolved issues

`PingFailoverAppender` race condition

Fixed PF-37816

We've fixed a defect where a race condition could cause the `PingFailoverAppender` to get stuck in a failed state without switching back to its primary appender.

Virtual hostname accuracy in email notifications

Fixed PF-37964

We've fixed a defect where a template variable incorrectly used the primary PingFederate base URL instead of the virtual hostname in some email notifications.

URL validation for `RelayState`

Fixed PF-38028

We've fixed a defect where PingFederate would reject requests with valid, non-encoded relay state values.

Apache Commons BeanUtils and Commons Compress

Fixed PF-38029

PingFederate now uses the Apache Commons BeanUtils library version 1.11.0 and the Apache Commons Compress library version 1.26.1.

HTML flow login and Authentication API

Fixed PF-38039

We've fixed a defect that could potentially allow a user to access an HTML browser sign-on page when the Authentication API redirectless mode is used.

Learn more in PingFederate unexpected template rendering in redirectless mode in the Ping Identity Support Knowledge Base.

LDAP account lockout

Fixed PF-38043

We've fixed a defect where PingFederate could incorrectly lock user accounts during an LDAP connectivity failure with Active Directory. This fix applies to all LDAP datastore types except for Generic LDAP.

IdP Adapter duplicate attribute sources

Fixed PF-38060

We've fixed a defect that caused IdP adapters to duplicate attribute sources when an SP connection was updated using the Admin API.

Corrected null `SaasGuid`

Fixed PF-38244

We've fixed a provisioning defect where disabled users weren't provisioned once their account was enabled and the **Provision Disabled Users** setting was set to false.

PingFederate 12.2.5 (August 2025)

Resolved issues

Admin console IP exposure

Security PF-33113

We've fixed a security vulnerability that could have allowed malicious parties to extract the PingFederate administrative console's IP address through HTTP Response headers.

Host header redirect

Security PF-37460

We've fixed a security vulnerability that could have allowed malicious parties to redirect PingFederate admin console traffic using a spoofed Host header.

PingFederate error messaging

Fixed PF-36991

We've fixed an issue by adding a missing property to `pingfederate-messages.properties`.

JARM response with `error` parameter

Fixed PF-37688

We've fixed a defect where JARM responses with an `error` parameter caused PingFederate to return a `500` error. It now returns a `200` response with the appropriate error page.

ATM configuration error

Fixed PF-37716

We've fixed a defect that caused an error in PingFederate when configuring an access token manager if the administrative node (ATM) isn't the coordinator node.

SNI extension error in BCFIPS mode

Fixed PF-37793

PingFederate now always includes the SNI extension in the ClientHello message during a TLS handshake when running in BCFIPS mode.

Wildcard TLS certificate error in BCFIPS mode

Fixed PF-37794

We've fixed a defect where PingFederate was refusing wildcard TLS certificates when running in BCFIPS mode.

`ClassNotFoundException` error

Fixed PF-37819

We've fixed an issue that could cause `ClassNotFoundException` on the admin console.

JWT API authentication method

Fixed PF-37841

We've added JWT as an authentication method for the admin API during upgrade utility validation.

PingFederate 12.2.4 (June 2025)

New features and enhancements

PingOne Singapore region

Info PF-37451

We've added support for the new PingOne Singapore region, `pingone.sg`.

Resolved issues

Refresh token MySQL deadlocks

Fixed PF-35868

We've fixed a defect that caused multiple refresh token requests in short succession to result in JDBC data source deadlocks and duplicated data entry into the database.

This feature can cause significant performance issues if PingFederate or the JDBC data source has insufficient resources.

Collect support data failure in admin console

Fixed PF-37398

We've fixed a defect that caused the Collect Support Data tool to fail when executed in the admin console when running PingFederate as a Windows service.

Unnecessary ID token reissued with secondary client secret

Fixed PF-37450

We've fixed a defect that caused the token endpoint to unnecessarily reissue an ID token when using a secondary client secret and an asymmetric algorithm for token signing and encryption.

Firefox Kerberos negotiation

Fixed PF-37559

We've fixed a defect that caused Kerberos negotiations to fail with Firefox after the initial exchange.

PingFederate 12.2.3 (May 2025)

New features and enhancements

Bouncy Castle FIPS 2.0 compatibility

Info PF-36846

We've upgraded Bouncy Castle to version 2.0. This versions is certified to operate in Federal Information Processing Standards (FIPS) mode 140-3.

NATIVE_S3_PING update

Info PF-37234

We've updated the behavior of the NATIVE_S3_PING discovery protocol when the `remove_all_data_on_view_change` parameter is active.

Previously, the protocol would delete all files in the S3 bucket, which could lead to the creation of an unwanted subcluster.

Now the protocol deletes all files except for its own to prevent the S3 bucket from being empty.

Learn more in Dynamic cluster discovery.

Resolved issues

RP-initiated logout error

Fixed PF-37173

We've fixed a defect that caused PingFederate to ignore the `id_token_hint` value during RP-initiated logout when the OAuth client logout mode is set to `None`.

Log rotation policy ignored

Fixed PF-37237

We've fixed a defect that caused PingFederate to ignore the log file size limit and rotation configurations set by the `SizeBasedTriggeringPolicy` parameter.

Secondary secret missing ID token claim

Fixed PF-37279

We've fixed a defect that caused the ID token claim to be omitted when an OAuth client uses the secondary secret.

PingFederate 12.2.2 (March 2025)

Resolved issues

SP connection with OGNL expression

Fixed PF-37046

We've fixed a defect where PingFederate failed to create or update service provider (SP) connections when using additional attributes from a data store in OGNL expressions, affecting both the `spConnections` endpoint in the Administrative API and the **Import Connection** process in the Admin console.

HTTP connection pool tracking

Fixed PF-37126

We've fixed a defect that could cause PingFederate to generate a large number of metric objects unnecessarily when making HTTP requests, which affected performance.

PingFederate 12.2.1 (February 2025)

New features and enhancements

Duplicate RSA key

New PF-36970

We've added a feature that gives you the option to include a duplicate RSA key with the RS256 algorithm. You can enable this option by setting the `add-duplicate-rs256-alg-key` parameter in the `<pingfed-install>/pingfederate/server/default/data/config-store/jwks-endpoint-configuration.xml` file to `true`.

Red Hat Enterprise Linux 8.10 compatibility

Info PF-36972

We've confirmed that PingFederate is compatible with Red Hat Enterprise Linux ES 8.10.

Resolved issues

Access token manager Admin API error

Fixed PF-36845

We've fixed a defect that caused a `500` error when creating or updating an access token manager using the Administrative API.

Refresh token error when authorization bypass enabled

Fixed PF-36851

We've fixed a defect that caused PingFederate to return a revoked or expired consent error when both **Bypass Authorization Approval** and **Bypass Authorization Approval for Previously Approved Consents** are enabled.

This is My Device error on HTML Form Adapter

Fixed PF-36864

We've fixed a defect that caused PingFederate to behave inconsistently when **This is My Device** is selected and an HTML Form Adapter instance has more than one session configuration in the session overrides.

TLS connection in BCFIPS mode

Fixed PF-36865

We've fixed a defect where PingFederate could not accept a TLS 1.2 connection in BCFIPS mode on Java 17.

Group membership loss during provisioning

Fixed PF-36874

We've fixed a defect that caused PingFederate to lose user group membership information when it lost contact with the datastore during provisioning operations.

Change password failure with PingOne Protect

Fixed PF-37012

We've fixed a defect that caused the HTML Form Adapter Change Password using an authentication policy to fail when PingOne Protect is the risk provider.

OGNL expressions with SDK classes

Fixed PF-37021

We've fixed a defect that caused OGNL expressions to fail to load when they contained SDK classes.

PingFederate 12.2 (December 2024)

New features and improvements in PingFederate 12.2.

New features and enhancements

Extended properties in adapter contract mapping

New PF-36314

We've added the ability for PingFederate to read extended properties in adapter contract mappings.

This improves flexibility by allowing you to use extended properties as values for attributes fulfilled by your adapter or as lookup values from your datastore.

Learn more in Configuring IdP adapter contract fulfillment and Defining issuance criteria for IdP adapter contract.

Extended properties in token generator and token exchange policy processor mappings

New PF-36315

We've added the ability for PingFederate to read extended properties in token generator mappings and token exchange policy processor mappings.

This improves flexibility by allowing you to use extended properties in token generation and exchange operations. You can also use extended properties as lookup values from your data store.

Extended properties in IdP and SP connections

New PF-36316

We've added the ability for PingFederate to read extended properties in adapter and authentication policy contract (APC) mappings for browser single sign-on (SSO).

This improves flexibility by allowing you to use extended properties in identity provider (IdP) and service provider (SP) connections.

Learn more in Configuring target session fulfillment.

Kerberos token validation without direct KDC communication

New PF-35864

We've added support for Kerberos validation when PingFederate is deployed in the cloud without direct Key Distribution Center (KDC) connectivity.

This can improve performance by allowing PingFederate to validate Kerberos tickets locally without the need for additional components.

Learn more in Adding Active Directory domains and Kerberos realms.

Authentication policy logging improvements

New PF-35343

We've improved the logging of authentication policies and fragments used during authentication. The following items are now included in their respective log files:

- `server.log`
  - Authentication policies that are skipped (DEBUG level)
  - Authentication policies used in the authentication request (DEBUG level)
  - No match found for rules (DEBUG level)
- `audit.log`
  - Policies used in authentication request (INFO level)

Learn more about the `audit.log` changes in Security audit logging.

URL-encoded certificate headers

New PF-36649

We've added a feature that allows PingFederate to consume URL-encoded client certificate headers.

This improves compatibility with NGINX mTLS-terminating reverse proxy.

Learn more in Configuring incoming proxy settings.

Automatic configuration data upgrade

New PF-34426

We've added a feature that automatically upgrades an imported configuration data archive from an older version of PingFederate to be compatible with the current version.

This makes it easier to upgrade to newer versions of PingFederate by allowing you to upgrade your configuration data without using the Upgrade Utility.

Learn more in Upgrading configuration data and Importing and deploying administrative console configuration data.

Automatic configuration data replication

New PF-36296

We've added a feature that allows PingFederate to automatically replicate configuration data archives to clustered server nodes when they uploaded to the drop-in deployer.

This makes it easier to ensure that your clustered nodes have the same configuration data.

Learn more in Upgrading configuration data and Configuration-archive deployment.

Token exchange processor policies in persistent grants

New PF-35857

We've added a feature that allows you to also get a refresh token during OAuth token exchange.

This allows you to make extended interactions without using long-lived access tokens received from token exchange.

Learn more in Managing processor policy grant mapping.

Token Endpoint response customization

New PF-35863

We've added a feature that allows you to customize which attributes are returned in the Token Endpoint response based on the scopes that are included in the request.

This improves flexibility by giving you more control over where PingFederate can return attributes.

Learn more in Defining the token endpoint management contract.

Admin API error response

New PF-36602

We've improved the error output for the Administrative API. When access to the administrative API in configured to use OAuth 2.0 or JWT authorization, and the access token is invalid, the error response now includes both `error` and `error_description` in the WWW-Authentication header.

This improves troubleshooting by providing an error code and description when authorization fails.

CIDR Authentication Selector description field

New PF-36291

We've added an optional description field to the CIDR Authentication Selector.

This helps you keep track of your defined network ranges by giving them an easily identifiable name.

Learn more in Configuring the CIDR Authentication Selector.

ID token included in token exchange

New PF-35859

We've added a feature that allows PingFederate to include an ID token along with an access token and refresh token in OAuth token exchanges.

This can improve your end-user experience by passing ID token information along with access tokens during SSO and other token exchange operations.

Learn more in Configuring policy and ID token settings.

Logs in JSON format

New PF-36317

We've added support for JSON formatted logging for most PingFederate logs through the log4j2 logging library.

This improves your ability to monitor PingFederate perfomance by producing logs in an easily parsed standard format.

Learn more in Logging in JSON format.

Collect support data in the admin console

New PF-35420

We've added a feature that allows you to collect support data using the administrative console and the administrative API.

This will improve your Ping Identity Support experience by allowing you to more easily customize and collect support data.

Learn more in Collecting support data in the admin console.

OAuth client name in HTML form templates

New PF-29353

We've added the ability to include the name of OAuth clients in HTML form login templates. You can use the *$escape* utility with the *$clientName* variable to include the client name.

This allows you to track the name of the client you use when customizing user-facing login pages.

Learn more in Customizable user-facing pages.

TLS 1.3 support for HSMs

New PF-35854

We've added TLS 1.3 support for Hardware Security Modules (HSMs). New installations of PingFederate will have TLS 1.3 enabled by default when in HSM mode.

This improves security by adding TLS by default to your HSM, and streamlines the HSM configuration process by removing a step to manually add TLS.

Device authorization grants include server settings

New PF-35858

We've added a feature that allows PingFederate to return ID tokens when issuing OpenID device authorization grants.

This allows you to personalize response messages during device authorization flows. For example, you can display the user's name as part of the authorization message.

Learn more in Configuring authorization server settings.

Google Cloud KMS Support

New PF-36302

We've added support for Google Cloud Key Management System (KMS).

This improves security by allowing you to encrypt the master key file when PingFederate is running in Google Cloud Platform.

Learn more in Implementing a MasterKeyEncryptor using Google Cloud KMS.

Disable `MaxMaliciousActions` parameter globally

New PF-36298

We've made it possible to globally disable the `MaxMaliciousActions` parameter in the `<pf-install>/pingfederate/server/default/data/config-store/com.pingidentity.common.security.AccountLockingService.xml` file.

This prevents an issue during upgrades where PingFederate unintentionally locks out an OAuth client when it tries to revoke invalid Reference Bearer Access Tokens.

Override `MaxMaliciousActions` parameter for OAuth client

New PF-36299

We've made it possible to override the `MaxMaliciousActions` parameter in the `<pf-install>/pingfederate/server/default/data/config-store/com.pingidentity.common.security.AccountLockingService.xml` file as it applies to an OAuth client.

This prevents an issue during upgrades where PingFederate unintentionally locks out an OAuth client when it tries to revoke Reference Bearer Access Tokens.

We've also improved the error messaging to clarify when it's the client, not the account, that's locked out.

Learn more in Configuring authorization server settings and Managing client configuration defaults.

Admin API JWT authorization

New PF-35855

We've added new feature that allows clients to access the Administrative API using a JWT.

This improves flexibility by adding a new secure method for your applications to access PingFederate administrative functions.

Learn more in Enabling JWT authorization.

OAuth Admin API access token scopes are optional

New PF-36588

PingFederate can now accept OAuth access tokens without scopes through the Admin API.

JGroups maximum thread pool size

New PF-34715

We've moved the setting for JGroups maximum thread pool size from `tcp.xml` and `udp.xml` to `run.properties`.

This new parameter in the `run.properties` file allows you to configure your JGroups thread pool more easily and ensure that changes are carried over during upgrade.

Learn more in Deploying cluster servers.

Customize Jetty runtime logs format

New PF-32832

We've added the `jetty.runtime.requestlog.format` property to the `run.properties` file to allow you to customize the format of the Jetty runtime log request.

You can use this property to add milliseconds to your log format, which is helpful for troubleshooting high volumes of requests.

Learn more in Configuring PingFederate properties.

Google reCAPTCHA Enterprise support

New PF-35861

We've added support for Google reCAPTCHA Enterprise.

reCAPTCHA Enterprise can handle higher volumes of assessment transactions and offers more levels of bot score granularity.

Learn more in Configuring Google reCAPTCHA Enterprise.

UserInfo endpoint JWT support

New PF-35862

We've added JSON web token (JWT) support to PingFederate's UserInfo endpoint when acting as the OpenId provider (OP). As the relying party (RP), PingFederate now supports consuming JWT-based responses from other OPs UserInfo endpoint.

This improves security by replacing information sent in JSON form with a signed token, an encrypted token, or both.

Learn more in Configuring OAuth clients and OAuth Client Management Service.

Improved provisioner logging

Improved PF-28890

We've added a new `provisioner-channel-summary.log` file to capture data about users and groups added, removed, and updated by provisioning cycles. We've also added new information at the INFO level to the `provisioner.log` and `provisioner-audit.log` files.

These updates give you improved summary information about provisioning operations without the unnecessary detail of DEBUG-level logging.

Learn more in PingFederate log files.

PingOne Verify Integration Kit update

Improved PF-36573

The PingOne Verify Integration Kit has been updated to version 2.2.2.

PingOne MFA Integration Kit update

Improved PF-36573

The PingOne MFA Integration Kit has been updated to version 2.5.

Microsoft EAM

PingFederate now supports Microsoft External Authentication Method (EAM) to handle multi-factor authentication (MFA) flows with PingID or other MFA integrations.

Learn more in Microsoft EAM Integration Kit.

Active Directory 2022 compatibility

Info PF-35782

We've confirmed that PingFederate 12.2 and 12.1 are compatible with Microsoft Active Directory 2022.

PostgreSQL 16.4 and 17 compatibility

Info PF-36312 PF-36288

We've confirmed that PingFederate version 12.2 is compatible with PostgreSQL versions 16.4 and 17.

Amazon Aurora PostgreSQL 16.4 compatibility

Info PF-36289

We've confirmed that PingFederate is compatible with Amazon Aurora PostgreSQL version 16.4.

jose4j library

Info PF-36445

PingFederate now uses the jose4j library version 0.9.6.

Apache Commons Compress

Info PF-36446

PingFederate now uses Apache Commons Compress library version 1.27.1.

AWS KMS library

Info PF-36579

We've upgraded the Amazon Web Services (AWS) Key Management Service (KMS) master-key-encryptor library to the latest version as of this release.

Correlation ID request header

Info PF-36675

Forward slashes are now valid characters in the request header for correlation ID.

Learn more in General settings and Correlating PingFederate events with PingDirectory LDAP activities.

Provisioning Flag Comparison Value now case-insensitive

info PF-36276

We've updated the provisioning Flag Comparison Value attribute to be case-insensitive.

Learn more in Modifying source settings.

Resolved issues

Auditor access to LDAP credentials

Security PF-35092

We've fixed a security vulnerability that could have allowed auditors to access LDAP credentials stored in configured datastores.

IP addresses accessible using Partner Metadata URL loader

Security PF-35279

We've fixed a security vulnerability that could have allowed malicious actors to use the Partner Metadata URL loader to list the IP addresses of network assets.

`ValidateRelayStateLength` parameter

Fixed PF-35847

We've fixed a defect that cause the `ValidateRelayStateLength` parameter in the `org.sourceid.saml20.bindings.AbstractAsyncBinding.xml` file to be evaluated only on startup. Now, the parameter is always evaluated in runtime flows.

Unexpected error when replicating an active admin console

Fixed PF-35919

We've fixed a defect that caused PingFederate to return an unexpected error when replicating on a newly promoted passive admin node after deleting connections or clients on the previously active admin node.

Kerberos and Form SSO policy fails in iOS

Fixed PF-35990

We've fixed a defect that caused Kerberos and Form SSO policies to fail when a user attempted SSO using iOS.

Provisioning character limit

Fixed PF-36035

We've fixed a defect that caused outbound provisioning to fail and cease if a source user object exceeded a 255-character limit. In the new behavior, PingFederate will skip user objects that exceed 255 characters and log a warning.

PingDirectory password warning

Fixed PF-36232

We've fixed a defect that prevented PingFederate from issuing a password expiration warning when using PingDirectory as a datastore.

Multiple application requests within a browser

Fixed PF-36239

We've fixed a defect that could cause inconsistent sessions or authentication errors when starting multiple applications in different browser tabs at the same time.

Unsupported data archive using drop-in deployer

Fixed PF-36478

We've fixed a defect that caused PingFederate to fail to restart when forcing an import of an unsupported configuration data archive using the drop-in deployer.

Replication warning banner

Fixed PF-36546

We've fixed a defect that caused the banner message warning that a configuration is out of date to persist after a configuration had been replicated. This defect occurred when running PingFederate as a Windows service.

Missing log details

Fixed PF-36550

We've fixed a defect that caused PingFederate to log errors excluding details of what error occurred. The fix now includes missing details.

Email verification failure after registration workflow

Fixed PF-36574

We've fixed a defect that caused the email verification screen to fail to appear when a user registered through an authentication source.

Multi-part refresh token revocation failure

Fixed PF-36600

We've fixed an issue that caused PingFederate to fail to revoke multi-part refresh tokens through the `revoke_token.oauth2` endpoint.

Known issues and limitations

PingOne Verify IK unexpected error

Issue PF-36573

PingFederate returns an unexpected error when you create an instance of the PingOne Verify Integration Kit version 2.2.2 in PingFederate with the Verify feature in PingOne disabled.

Reencrypt data archive failure with Google Cloud KMS

Issue PF-36487

When PingFederate is configured to use the Amazon Web Services or Google Cloud Platform Key Management System (KMS), importing a valid configuration data archive with **Reencrypt Data** enabled fails with a `Could not reencrypt data archive` error message. This failure causes PingFederate to fail to restart.

Third-party cookie blocking affecting single logout

Issue PF-35772

Due to multiple vendors' recent browser versions that block third-party cookies, you might experience issues related to single logout with OIDC (via Front-Channel) and WS-Federation.

Refer to browsers' documentation regarding third-party cookie management to unblock them, if feasible.

Passive admin console UI refresh

Issue PF-35643

When you promote a passive admin console to active, the UI doesn’t refresh until you perform an action.

Multiple active admin consoles

Issue PF-35439

When you make configuration changes on the active console (especially large configuration changes like bulk imports or data archive imports), then promote a passive console to

active, it can cause multiple consoles to be active at once. This can result in inconsistent configurations.

Learn how to resolve this issue in Resolving multiple active administrative nodes.

Administrative console and administrative API

Issue

- Although PingFederate 11.3 and later support DPoP, a known limitation is that the following features don't support DPoP when PingFederate is the RP:
  - The administrative console authentication scheme using OIDC
  - The administrative API authentication scheme using OAuth 2.0
- /bulk: Only resource types currently supported by the administrative API are included in the exported data. We don't intend to introduce administrative API support to the following areas:
  - SAML 2.0 IdP Discovery
  - SAML 2.0 SP Affiliation
  - SMS Provider
- Previously, the administrative API did not accurately reflect a **Persistent Grant Max Lifetime** setting of 29 days (or shorter) with the selection of the **Grants Do Not Timeout Due To Inactivity** option. As a result, if you have configured such OAuth authorization server settings and have generated a bulk export in version 10.0 through 10.0.2, we recommend that you re-generate a new bulk export after upgrading to version 10.0.3 (or a more recent version). The newly exported data does not contain the aforementioned flaw, and you can safely import it to version 10.0.3 (or a more recent version).
- When enabling mTLS certificate-based authentication, administrators often configure a list of acceptable client certificate issuers. When you use a browser to access the console or the administrative API documentation, PingFederate returns to the browser the list of acceptable issuers as part of the TLS handshake. If the browser's client certificate store contains multiple client certificates, the browser often presents you only the certificates whose issuer matches one of the acceptable issuers. However, when PingFederate runs in a Java 11 environment, Chrome presents you all its

configured client certificates, regardless of whether the issuer matches one of the acceptable issuers or not.

- When using mTLS authentication to authenticate to an LDAP server for administrative console or administrative API access, PingFederate doesn't support using a Microsoft Active Directory server.
- Prior to toggling the status of a connection with the administrative API, you must ensure that any expired certificates or no longer available attributes are replaced with valid certificates or attributes; otherwise, the update request fails.
- When creating or updating a child instance of a hierarchical plugin, the administrative API retains objects with an `"inherited": false` name/value pair (or without such name/value pair altogether), ignores those with a value of `true`, and returns a 200 HTTP status code. No error messages are returned for the ignored objects.
- Using the browser's navigation mechanisms (for example, the **Back** button) causes inconsistent behavior in the administrative console. Use the navigation buttons provided at the bottom of windows in the PingFederate console.
- Using the PingFederate console in multiple tabs on one browser might cause inconsistent behavior which could corrupt its configuration.
- If authenticated to the PingFederate administrative console using certificate authentication, a session that has timed out might 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 sign-on page, and then back to the administrative console after authentication is complete. Similar behavior applies for certificate authentication, in principle. However, because the browser might automatically resubmit the certificate for authentication, the browser might redirect to the administrative console and not the sign on page.

TLS cipher suite customization

Issue

PingFederate's TLS cipher suites can be customized by modifying `com.pingidentity.crypto.SunJCEManager.xml` (or a similarly-named file if BCFIPS or an HSM is configured). After updating the file and replicating, all cluster nodes must be restarted for the change to take effect.

Java

Issue

- Updating Java version 8 to version 11 results in an error when PingFederate is already installed and running on Windows. To work around this issue, uninstall and reinstall the PingFederate Windows service by running the `UninstallPingFederateService.bat` and `InstallPingFederateService.bat` files located in `<pf_install>/pingfederate/sbin/wrapper`.

HSMs

Issue

AWS CloudHSM

- It is not possible to use an elliptic curve (EC) certificate as an SSL server certificate.
- TLS 1.3 is not currently supported with Oracle JDK 11 and 17.

Thales HSMs

- JWT token decryption using ECDH-ES may fail. This issue only arises if PingFederate is configured with static OAuth and OpenID Connect keys, a static key is stored on the HSM, and PingFederate is consuming a token encrypted with this key.
- It is not possible to use an EC certificate as an SSL server certificate.
- TLS 1.3 is not currently supported with Oracle JDK 11 and 17.

Entrust HSMs

- JWT token decryption using ECDH-ES may fail. This issue only arises if PingFederate is configured with static OAuth and OpenID Connect keys, a static key is stored on the HSM, and PingFederate is consuming a token encrypted with this key.
- It is not possible to import a PKCS12- or PEM-formatted EC certificate.
- It is not possible to use an EC certificate as an SSL server certificate.
- TLS 1.3 is not currently supported with Oracle JDK 11 and 17.

SSO and SLO

Issue

- When consuming SAML metadata, PingFederate does not report an error when neither the `validUntil` nor the `cacheDuration` attribute is included in the metadata. Note that PingFederate does reject expired SAML metadata as indicated by the `validUntil` attribute value, if it is provided.
- The anchored-certificate trust model cannot be used with the single logout (SLO) redirect binding because the certificate cannot be included with the logout request.
- 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.

Composite Adapter configuration

Issue

SLO is not supported when users are authenticated through a Composite Adapter instance that contains another instance of the Composite Adapter.

Self-service password reset

Issue

Passwords can be reset for Microsoft Active Directory user accounts without the permission to change password.

OAuth

Issue

PingFederate does not support a case-sensitive naming convention for OAuth client ID values when client records are stored in a directory server. For example, after creating a client with an ID value of `sampleClient`, PingFederate does not allow the creation of another client with an ID value of `SampleClient`.

Although it's possible to create clients using the same ID values with different casings when client records are stored in XML files, a database server, or custom storage, we recommend not doing so to avoid potential record migration issues.

Customer identity and access management

Issue

Some browsers display a date-picker user interface for fields that have been designed for date-specific inputs. Some browsers do not. If one or more date-specific fields are defined on the registration page or the profile management page (or both), end users must enter the dates manually if their browsers do not display a date-picker user interface for those fields.

Provisioning

Issue

- 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.
- The `totalResults` value in SCIM responses indicates the number of results returned in the current response, not the total number of estimated results on the LDAP server.

Logging

Issue

- 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, the `USER_KEY` attribute will not be masked in the server logs. Other persistent grant attributes will be masked.
- Even if a source attribute has been configured for masking in an IdP adapter and the source attribute is mapped as the adapter's unique user key, the user key attribute is not masked in the server or audit logs.

Database logging

Issue

- 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, the `USER_KEY` attribute will not be masked in the server logs. Other persistent grant attributes will be masked.

- Even if a source attribute has been configured for masking in an IdP adapter and the source attribute is mapped as the adapter's unique user key, the user key attribute is not masked in the server or audit logs.

RADIUS NAS-IP-Address

Issue

The RADIUS NAS-IP-Address is only included in Access-Request packets when the `pf.bind.engine.address` is set with an IPv4 address. IPv6 is not supported.

Amazon SNS Notification Publisher

Issue

When deploying PingFederate with a forward proxy, plugins based on the AWS SDK, such as the Amazon SNS Notification Publisher, will only honor the `http.proxyHost`, `http.proxyPort`, `http.proxyUser`, and `http.proxyPassword` properties in `run.properties`. The plugin will rely on these properties even if the service URL is `https`.

Deprecated features

No features were deprecated for PingFederate 12.2.

PingFederate 12.1.11 (May 2026)

New features and enhancements

Unconnected cluster node startup

Improved PF-38898

PingFederate now supports the `force.require.replication.data.on.startup` parameter in the `cluster-config-replication.conf` file. This parameter allows you to

prevent an engine node from starting up without establishing a connection to the cluster and retrieving replication data.

Learn more in Cluster management.

Resolved issues

OGNL code test access control

Security PF-38742

We improved role-based access control (RBAC) for the administrative expression-testing endpoint. Access to expression evaluation is now limited to appropriately privileged roles, ensuring it aligns with intended administrative permissions.

URL validation for RelayState

Fixed PF-38028

We fixed a defect where PingFederate would reject requests with valid, non-encoded `RelayState` values.

Administrative API authentication

Fixed PF-38393

We fixed a defect that allowed Basic Authentication to access the Administrative API even when Basic Authentication was disabled in the `pf.admin.api.authentication` property.

Authentication policy error

Fixed PF-38623

We fixed a defect that caused an error when authentication policies with a Requested AuthN Context authentication had **Add or Update AuthN Context Attribute** enabled.

Dynamic JWKS rotation timer

Fixed PF-38903

We fixed a defect that prevented the dynamic JWKS rotation timer from resetting after a node joined a cluster.

PingFederate 12.1.10 (October 2025)

Resolved issues

Apache Commons BeanUtils and Commons Compress

Fixed PF-38029

PingFederate now uses the Apache Commons BeanUtils library version 1.11.0 and the Apache Commons Compress library version 1.26.1.

LDAP account lockout

Fixed PF-38043

We've fixed a defect where PingFederate could incorrectly lock user accounts during an LDAP connectivity failure with Active Directory. This fix applies to all LDAP datastore types except for Generic LDAP.

IdP Adapter duplicate attribute sources

Fixed PF-38060

We've fixed a defect that caused IdP adapters to duplicate attribute sources when an SP connection was updated using the Admin API.

PingFederate 12.1.9 (September 2025)

Resolved issues

Admin console IP exposure

Security PF-33113

We've fixed a security vulnerability that could have allowed malicious parties to extract PingFederate administrative console IP addresses using HTTP Response headers.

Host header redirect

Security PF-37460

We've fixed a security vulnerability that could have allowed malicious parties to redirect PingFederate admin console traffic using a spoofed Host header.

Refresh token MySQL deadlocks

Fixed PF-35868

We've fixed a defect that caused multiple refresh token requests in short succession to result in JDBC data source deadlocks and duplicated data entry into the database.

This change can cause significant performance issues if PingFederate or the JDBC data source has insufficient resources.

Unnecessary ID token reissued with secondary client secret

Fixed PF-37450

We've fixed a defect that caused the token endpoint to unnecessarily reissue an ID token when using a secondary client secret and an asymmetric algorithm for token signing and encryption.

Virtual hostname accuracy in email notifications

Fixed PF-37964

We've fixed a defect where a template variable incorrectly used the primary PingFederate base URL instead of the virtual hostname in some email notifications.

HTML flow login and Authentication API

Fixed PF-38039

We've fixed a defect that could potentially allow a user to access an HTML browser login page when the Authentication API redirectless mode is used.

Learn more in PingFederate unexpected template rendering in redirectless mode in the Support Knowledge Base.

PingFederate 12.1.8 (May 2025)

New features and enhancements

NATIVE_S3_PING update

Info PF-37234

We've updated the behavior of the NATIVE_S3_PING discovery protocol when the `remove_all_data_on_view_change` parameter is active.

Previously, the protocol would delete all files in the S3 bucket, which could lead to the creation of an unwanted subcluster.

Now the protocol deletes all files except for its own to prevent the S3 bucket from being empty.

Learn more in Dynamic cluster discovery.

Resolved issues

Secondary secret missing ID token claim

Fixed PF-37279

We've fixed a defect that caused the ID token claim to be omitted when an OAuth client uses the secondary secret.

PingFederate 12.1.7 (March 2025)

Resolved issues

HTTP connection pool tracking

Fixed PF-37126

We've fixed a defect that could cause PingFederate to generate a large number of metric objects unnecessarily when making HTTP requests, which affected performance.

PingFederate 12.1.6 (February 2025)

New features and enhancements

Duplicate RSA key

New PF-36970

We've added a feature that gives you the option to include a duplicate RSA key with the RS256 algorithm. You can enable this option by setting the `add-duplicate-rs256-alg-key` parameter in the `<pingfed-install>/pingfederate/server/default/data/config-store/jwks-endpoint-configuration.xml` file to `true`.

Resolved issues

Group membership loss during provisioning

Fixed PF-36874

We've fixed a defect that caused PingFederate to lose user group membership information when it lost contact with the datastore during provisioning operations.

PingFederate 12.1.5 (January 2025)

Resolved issues

Cross-site scripting

Security PF-36304 PF-36311 PF-36313

We've fixed a security vulnerability where PingFederate accepted cross-site scripting inputs.

Email verification failure after registration workflow

Fixed PF-36574

We've fixed a defect that caused the email verification screen to fail to appear when a user registered through an authentication source.

Multi-part refresh token revocation failure

Fixed PF-36600

We've fixed an issue that caused PingFederate to fail to revoke multi-part refresh tokens through the `revoke_token.oauth2` endpoint.

OAuth Client Set Authentication Selector with DynamoDB

Fixed PF-36662

We've fixed a defect that caused an error in searching for OAuth Client for OAuth Client Set Authentication Selector when DynamoDB is the client storage.

Admin API provisioning connection attributes

Fixed PF-36816

We've fixed a defect when using the PingFederate Administrative API `sp/idpConnections` endpoint to create or update inbound provisioning connections. The API returned errors

about `coreAttributes` values missing from the JSON payload even though the attributes were not required.

Refresh token error when authorization bypass enabled

Fixed PF-36851

We've fixed a defect that caused PingFederate to return a revoked or expired consent error when both **Bypass Authorization Approval** and **Bypass Authorization Approval for Previously Approved Consents** are enabled.

PingFederate 12.1.4 (November 2024)

Resolved issues

Disable `MaxMaliciousActions` parameter

New PF-36298

We've made it possible to globally disable the `MaxMaliciousActions` parameter in the `com.pingidentity.common.security.AccountLockingService` file.

This will prevent an issue during upgrades where PingFederate unintentionally locks out an OAuth client when it tries to revoke Reference Bearer Access Tokens.

Unexpected error when replicating an active admin console

Fixed PF-35919

We've fixed a defect that caused PingFederate to return an unexpected error when replicating on a newly promoted passive admin node after deleting connections or clients on the previously active admin node.

Provisioning character limit

Fixed PF-36035

We've fixed a defect that caused outbound provisioning to fail and cease if a source user object exceeded a 255-character limit. In the new behavior, PingFederate will skip user objects that exceed 255 characters and log a warning.

API Datastore sends Content-Type for GET requests

Fixed PF-36194

We've fixed a defect that caused the PingFederate REST API Datastore to unnecessarily include a Content-Type value when sending GET requests.

PingDirectory password warning

Fixed PF-36232

We've fixed a defect that prevented PingFederate from issuing a password expiration warning when using PingDirectory as a datastore.

Multiple application requests within a browser

Fixed PF-36239

We've fixed a defect that could cause inconsistent sessions or authentication errors when starting multiple applications in different browser tabs at the same time.

Incorrect Swagger docs base path

Fixed PF-36241

We've fixed a defect that caused PingFederate to set the wrong base path for Swagger docs when the `pf.admin.baseurl` parameter includes a file path.

OGNL expression variables in datastore attributes

Fixed PF-36257

We've fixed a defect that caused PingFederate to ignore defined OGNL expression variables in datastore attributes.

Notification publisher validation error

Fixed PF-36260

We've fixed a defect that caused PingFederate to return a validation error when using the `/serverSettings` endpoint to update the notification settings to `LOGGING_ONLY` in an environment with no previously-defined notification publisher.

Device authorization grant time zone error

Fixed PF-36261

We've fixed a defect that caused device authorization grant flow errors when clustered server nodes are in different time zones.

Bulkhead notification validation error

Fixed PF-36269

We've fixed a defect that caused a validation error when sending a valid PUT request to the `/serverSettings` or `/serverSettings/notifications` endpoints when the bulkhead notification is active on the default notification publisher.

Replication warning banner

Fixed PF-36546

We've fixed a defect that caused the banner message warning that a configuration is out of date to persist after a configuration had been replicated. This defect occurred when running PingFederate as a Windows service.

Provisioning Flag Comparison Value now case-insensitive

info PF-36276

We've updated the provisioning Flag Comparison Value attribute to be case-insensitive.

Learn more in Modifying source settings.

PingFederate 12.1.3 (September 2024)

New features and enhancements

Process PKCE parameters outside signed request object

Improved PF-36180

We've added an option to process PKCE parameters from outside the signed request object when the parameters are not included in the request object.

> **Note**
>
> This is an opt-in function, and not recommended for continued use.

Resolved issues

Custom error message not displaying

Fixed PF-36086

We've fixed a defect that caused PingFederate to not display a custom error message when using a custom authorization adapter without an authorization API application.

PingFederate 12.1.2 (August 2024)

Resolved issues

Relative path symbolic links retrieve wrong file

Security PF-35678

We've fixed a defect that caused PingFederate to retrieve the wrong file when using relative paths in symbolic links.

Heartbeat endpoint 500 error

Fixed PF-35842

We've fixed a defect that caused the heartbeat endpoint to return a `500` error after upgrading to PingFederate 12.1.

Refresh token time zone discrepancies

Fixed PF-35867

We've fixed a defect that caused refresh tokens to roll prematurely when making authorization requests to servers in different time zones.

Maintenance upgrade includes entire SDK directory

Fixed PF-35920

We've fixed a defect that caused the incremental update package for PingFederate versions 12.0 and 12.1 to unnecessarily install the entire SDK directory.

Local error handling error

Fixed PF-35952

We've fixed a defect that caused PingFederate to redirect failed IdP sign on attempts rather than handling the error locally.

PingFederate 12.1.1 (July 2024)

Resolved issues

Axis1 patch

Security PF-35631

Included a patch to address multiple vulnerabilities related to Apache Axis1.

Refresh token rolls when configured not to roll

Fixed PF-35166

Fixed a defect that caused PingFederate to roll refresh tokens when **Refresh Token Rolling Policy** is disabled but **Refresh Token Rolling Interval** has a value.

Provisioning group changes continue after user changes failure

Fixed PF-35304

Fixed a defect that caused the provisioner to propagate group updates even if user updates didn't finish.

OAuth client only validates one access token manager when `aud` parameter included

Fixed PF-35737

Fixed a defect that caused PingFederate to validate only the first OAuth client access token manager it found when **Validate Against All Eligible Access Token Managers** was checked, and the `aud` parameter was included in the request.

Custom adapter not returning IPv4 addresses

Fixed PF-35783

Fixed a defect where PingFederate failed to return IPv4 addresses in a custom adapter request using the `request.getRemoteAddr()` method.

Context SRI attribute mapping failure

Fixed PF-35800

Fixed a defect that caused PingFederate to fail to map new attributes added to an existing access token manager to the Context SRI.

Error message after user session expires

Fixed PF-35815

Fixed a defect that caused PingFederate to present an error message when user tries to sign on again after a session expires due to inactivity.

PingFederate 12.1 (June 2024)

New features and improvements in PingFederate 12.1.

New features and enhancements

Active and passive administrative consoles

New PF-34962

We've added a feature that allows you to create an active admin console and one or more passive backup admin consoles in a clustered environment.

Even though only one node can be active, the passive nodes are always kept in sync, so you can easily promote them to the active console. This reduces downtime in the event of an outage on the node with the active admin console.

Learn more in Active and passive administrative nodes.

Runtime threads bulkheads

New PF-35345

We've added the ability to implement runtime thread bulkheads that limit the percentage of threads that can be waiting on external data sources. After the limit is reached, further requests are rejected.

This improves resilience, reliability, and availability by minimizing the impact of a broken data source connection on other connections.

You can configure bulkheads in the `com.pingidentity.common.util.resiliency.BulkheadManagerImpl.xml` file. You can also configure runtime notifications for bulkhead threshold events.

Learn more in Configuring runtime thread bulkheads.

Decrypting SAML attribute values

New PF-34887

We've added a new special attribute, `SAML_AUTHN_RESPONSE_ASSERTION`, to access the `Assertion` element of the SAML 2.0 response messages during attribute mapping.

Learn more in Special attribute names in contracts.

Custom key identifier

New PF-34883

We've added the ability to define a custom key identifier (KID) for OIDC and OAuth signing and decryption keys for each RSA-based signing algorithm.

Custom KID values help with special environments and custom requirements for RSA-based JSON Web Keys (JWK) published in the JSON Web Keys endpoint.

Learn more in Keys for OAuth and OpenID Connect.

Cookieless authentication API

New PF-34889

We've added the ability to enable a redirectless authentication API OAuth flow through the authorization endpoint without cookies.

You can now use the authentication API without having to manage and process cookies. Instead of cookies, the API includes details within the JSON response that need to be included as a simple HTTP header value in responses to PingFederate.

This improvement is especially useful for native app developers and reduces the implications of third-party cookie issues.

Learn more in Configuring OAuth clients.

Resource indicators for OAuth 2.0

New PF-35341

We've added support for the `resource` parameter to allow clients to indicate the protected resources to which it is requesting access.

The `resource` parameter is available for use during access token mapping.

Learn more in the RFC 8707 specification and Token endpoint.

> **Important**
>
> Reusing a previous version's OAuth authentication calls that contain **Resource URIs** will fail if the required **Resource URIs** aren't defined in the **Access Token Manager**. Learn more in Managing resource URIs.

PingOne Australia region support

New PF-31859

We've added support for the Australia region in the PingOne unified admin feature. You can now configure the `pf.pingone.admin.url.region` property for Australia (.com.au).

The Asia region is deprecated. We recommend using the Australia region instead.

Learn more in Configuring PingFederate properties.

Publish signing keys to JWKS endpoint

New PF-34886

We've added the ability to optionally publish asymmetric signing keys configured in a JWT Access Token Management Plugin instance to the PingFederate JWKS endpoint.

Publishing JWKs to the JWKS endpoint reduces the number of required JWKS endpoints, and allows you to use more standard client libraries and fewer custom clients.

Published keys are discoverable using the OpenID Provider configuration endpoint.

Learn more in Configuring an access token management instance.

Publish x5t thumbprint to JWKS endpoint

New PF-35342

PingFederate now publishes the `x5t` x.509 certificate SHA-1 thumbprint parameter from the JWKS endpoint by default.

Learn more in JSON Web Keys endpoint.

Custom URI schemes for redirect validation

New PF-34891

We've added support for custom URI schemes in redirect validation for OAuth and OIDC clients.

You can now allow redirects to URIs such as native applications or APIs outside of the HTTP/HTTPS scheme. Because application URIs are often company or brand-specific, this feature reduces the potential for naming collisions with other apps on the same device.

Learn more in Configuring redirect validation.

JARM support for IdP connections

New PF-34884

We've added support for JWT Authorization Response Mode (JARM) to identity provider (IdP) connections.

PingFederate already supports JARM in its role as a relying party (RP), and now supports it in its role as an OpenID provider (OP). Instead of having to receive an issued `authorization_code` and `state` parameter as a query component, your connection can process a JWT instead.

Learn more in Creating an OpenID Connect IdP connection.

Configure Refresh Rolling Token Interval in hours, minutes, or seconds

New PF-34885

We've added a feature allowing you to configure the interval of rolling OAuth tokens in hours, minutes, or seconds.

Learn more in Configuring OAuth clients, Configuring authorization server settings, and Managing client configuration defaults.

Magic link integration kit

New PF-34422

We've added support for the PingFederate Magic Link Integration Kit.

Learn more in the Magic Link Integration Kit documentation.

Configurable LDAP health check timeout

New PF-35012

We've added the ability to configure the timeout duration for LDAP health checks.

You can configure this option in the `~/server/default/data/config-store/com.pingidentity.common.util.ldap.LDAPUtil.xml` file using the **`HealthCheckResponseTimeoutMillis`** parameter.

The default value is `2000`.

LDAPv3 with StartTLS command

New PF-35349

PingFederate now supports LDAPv3 with the StartTLS command to secure LDAP connections to a directory server.

This feature allows LDAP connections to be initiated on a non-SSL port (such as 389), and then be upgraded to SSL on the same port. This reduces the number of ports that potentially have to be opened within a firewall.

Learn more in Configuring an LDAP connection.

OpenID Connect `offline_access` scope

New PF-35346

PingFederate now supports the OpenID Connect (OIDC) `offline_access` scope.

You can now configure OAuth and OIDC clients to receive only a `refresh_token` when this scope is requested. You can also optionally configure a resource owner consent as required.

Learn more in Configuring authorization server settings and OAuth Client Management Service.

OpenID Connect user registration

New PF-35347

PingFederate now supports user registration through OIDC 1.0 using the `prompt=create` command.

Including this parameter initiates a user registration flow within the context of OIDC, which reduces developer efforts by eliminating the need for a separate customer registration flow.

Learn more in Configuring request parameters and SSO URLs.

Exposed `pi.sri` to SDK and attribute mapping

New PF-35453

We've added the `IN_PARAMETER_NAME_SRI` parameter to the SDK, which contains the current `pi.sri`.

We've also exposed the `pi.sri` value in the **Context** type for most attribute mappings.

SDK capability for adapters to terminate sessions

New PF-34464

We've added a new `SessionManager` class in the SDK to allow for revoking all sessions or all but the current session.

This works similarly to the **Revoke sessions after password change or reset** option in the HTML Form Adapter.

PingDirectory log tracking ID

New PF-34338

We've added support for the log tracking ID feature in PingDirectory 10.0. PingFederate can use this tracking ID as a `transactionId` value.

Learn more in Security audit logging.

Improved logging for adapters manager

Improved PF-35079

We've improved logging capabilities to associate an adapter ID with adapters that fail to load. This makes misconfigured adapters easier to trace.

OAuth scope reference UI improvements

Improved PF-34952

We've added a pop-up modal to several OAuth scope reference pages to improve the scope management user interface.

Learn more in Configuring scope constraints.

Scope management user interface enhancement

Improved PF-34890

We've improved the user interface for the **Scope Management** page, including pagination, a search feature, and new tabs for managing common and exclusive scope groups.

Learn more in Defining scopes.

New connection pool metrics in heartbeat endpoint

Improved PF-34892

We've added new connection pool metrics to the heartbeat endpoint and JMX MBeans for Java Database Connectivity (JDBC) and LDAP connections.

New metrics include maximum connection pool size, minimum connection pool size, number of active connections, and number of idle connections.

> **Note**
>
> There is no active connections metric for LDAP connectors, because `LDAPConnectionPool` does not track the number of connections that are established and currently in use.

Learn more in Customizing the heartbeat message and Liveliness and responsiveness.

Refresh grants revocation and issuance

Improved PF-35527

Refresh grants are no longer revoked when issuance criteria fail.

Also, new grants or access tokens are not issued due to the failure of issuance criteria.

This is the new default behavior for refresh grants.

PingOne MFA Integration Kit

Improved PF-35325

The PingOne MFA Integration Kit has been updated to version 2.3.1.

Aurora PostgreSQL

Improved PF-35383

PingFederate now supports Aurora PostgreSQL version 16.2.

PostgreSQL

Improved PF-35384

PingFederate now supports PostgreSQL version 16.2.

PingDS support

Info PF-34434

We've added support for PingDS (formerly ForgeRock DS) datastore.

Learn more in System requirements.

Jetty library upgrade

Improved PF-34039

We've upgraded Jetty to version 10.

FAPI and FAPI CIBA certification

Info PF-34897

PingFederate 12.1 is certified for FAPI OpenID Providers (OP) and Profiles, and FAPI CIBA OpenID Providers and Profiles.

Resolved issues

Admin console OIDC login failure

Fixed PF-34523

We've fixed an issue that caused PingFederate's OIDC admin console login to fail when the `node.group.id` value didn't match an existing node id.

PingDirectory user attribute queries

Fixed PF-34333

We've fixed an issue that caused PingFederate to query all attributes for PingDirectory users, rather than just the required attributes.

DPoP token rejection

Fixed PF-35082

We've fixed a defect that caused access token requests to fail due to OAuth 2.0 Demonstrating Proof of Possession (DPoP) proof validation failure when reusing existing persistent access grant is enabled for confidential claims.

License expiration date discrepancy

Fixed PF-35114

We've fixed an issue that caused PingFederate to display the expiration date of a PingFederate license in terms of the browser time zone rather than the server time zone.

Web token processing slowdown

Fixed PF-35272

We've fixed an issue that caused significant slowdown when PingFederate processed an unencrypted JSON web token (JWT) using JSON web encryption (JWE) deobfuscation.

REST API datastore unable to handle malformed cookies

Fixed PF-35352

We've fixed a defect that caused the PingFederate REST API datastore to pass malformed cookies into datastore request headers.

OAuth client in-use detection

Fixed PF-35744

We've fixed a defect where client in-use detection caused an IndexOutOfBoundsException when a custom solution is used for client storage.

ClientManagerDynamoDBImpl changes not implemented

Fixed PF-35753

We've fixed a defect that caused changes in `ClientManagerDynamoDBImpl` not to apply when performing a bulk import or using the configuration store API unless you restarted PingFederate.

License issue dates

Fixed PF-35075

We've fixed a defect that caused PingFederate to ignore valid license files if they were issued prior to the current license file.

Known issues and limitations

Third-party cookie blocking affecting single logout

Issue PF-35772

Due to multiple vendors' recent browser versions that block third-party cookies, you might experience issues related to single logout with OIDC (via Front-Channel) and WS-Federation.

Refer to browsers' documentation regarding third-party cookie management to unblock them, if feasible.

Replication notification when switching passive admin console to active

Issue PF-35642

When you switch a passive console to active, PingFederate might display a notification that the configuration has not been replicated, even though the configuration is up-to-date.

Passive admin console UI refresh

Issue PF-35643

When you promote a passive admin console to active, the UI doesn't refresh until you perform an action.

Multiple active admin consoles

Issue PF-35439

When you make configuration changes on the active console (especially large configuration changes like bulk imports or data archive imports), then promote a passive console to active, it can cause multiple consoles to be active at once. This can result in inconsistent configurations.

Learn how to resolve this issue in Resolving multiple active administrative nodes.

Administrative console and administrative API

Issue

- Although PingFederate 11.3 and later support DPoP, a known limitation is that the following features don't support DPoP when PingFederate is the RP:
  - The administrative console authentication scheme using OIDC
  - The administrative API authentication scheme using OAuth 2.0
- /bulk: Only resource types currently supported by the administrative API are included in the exported data. We don't intend to introduce administrative API support to the following areas:
  - SAML 2.0 IdP Discovery
  - SAML 2.0 SP Affiliation
  - SMS Provider
- Previously, the administrative API did not accurately reflect a **Persistent Grant Max Lifetime** setting of 29 days (or shorter) with the selection of the **Grants Do Not Timeout Due To Inactivity** option. As a result, if you have configured such OAuth authorization server settings and have generated a bulk export in version 10.0 through 10.0.2, we recommend that you re-generate a new bulk export after upgrading to version 10.0.3 (or a more recent version). The newly exported data does not contain

the aforementioned flaw, and you can safely import it to version 10.0.3 (or a more recent version).

- When enabling mTLS certificate-based authentication, administrators often configure a list of acceptable client certificate issuers. When you use a browser to access the console or the administrative API documentation, PingFederate returns to the browser the list of acceptable issuers as part of the TLS handshake. If the browser's client certificate store contains multiple client certificates, the browser often presents you only the certificates whose issuer matches one of the acceptable issuers. However, when PingFederate runs in a Java 11 environment, Chrome presents you all its configured client certificates, regardless of whether the issuer matches one of the acceptable issuers or not.
- When using mTLS authentication to authenticate to an LDAP server for administrative console or administrative API access, PingFederate doesn't support using a Microsoft Active Directory server.
- Prior to toggling the status of a connection with the administrative API, you must ensure that any expired certificates or no longer available attributes are replaced with valid certificates or attributes; otherwise, the update request fails.
- When creating or updating a child instance of a hierarchical plugin, the administrative API retains objects with an `"inherited": false` name/value pair (or without such name/value pair altogether), ignores those with a value of `true`, and returns a 200 HTTP status code. No error messages are returned for the ignored objects.
- Using the browser's navigation mechanisms (for example, the **Back** button) causes inconsistent behavior in the administrative console. Use the navigation buttons provided at the bottom of windows in the PingFederate console.
- Using the PingFederate console in multiple tabs on one browser might cause inconsistent behavior which could corrupt its configuration.
- If authenticated to the PingFederate administrative console using certificate authentication, a session that has timed out might 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 sign-on page, and then back to the administrative console after authentication is complete. Similar behavior applies for certificate authentication, in principle. However, because the browser might automatically resubmit the certificate for authentication, the browser might redirect to the administrative console and not the sign on page.

TLS cipher suite customization

Issue

PingFederate's TLS cipher suites can be customized by modifying `com.pingidentity.crypto.SunJCEManager.xml` (or a similarly-named file if BCFIPS or an HSM is configured). After updating the file and replicating, all cluster nodes must be restarted for the change to take effect.

Java

Issue

- CloudHSM is not supported when using Java 17.
- Updating Java version 8 to version 11 results in an error when PingFederate is already installed and running on Windows. To work around this issue, uninstall and reinstall the PingFederate Windows service by running the `UninstallPingFederateService.bat` and `InstallPingFederateService.bat` files located in `<pf_install>/pingfederate/sbin/wrapper`.

HSMs

Issue

AWS CloudHSM

- It is not possible to use an elliptic curve (EC) certificate as an SSL server certificate.
- TLS 1.3 is not currently supported.

Thales HSMs

- JWT token decryption using ECDH-ES may fail. This issue only arises if PingFederate is configured with static OAuth and OpenID Connect keys, a static key is stored on the HSM, and PingFederate is consuming a token encrypted with this key.
- It is not possible to use an EC certificate as an SSL server certificate.
- TLS 1.3 is not currently supported.

Entrust HSMs

- JWT token decryption using ECDH-ES may fail. This issue only arises if PingFederate is configured with static OAuth and OpenID Connect keys, a static key is stored on the HSM, and PingFederate is consuming a token encrypted with this key.
- It is not possible to import a PKCS12- or PEM-formatted EC certificate.
- It is not possible to use an EC certificate as an SSL server certificate.
- TLS 1.3 is not currently supported.

SSO and SLO

Issue

- When consuming SAML metadata, PingFederate does not report an error when neither the `validUntil` nor the `cacheDuration` attribute is included in the metadata. Note that PingFederate does reject expired SAML metadata as indicated by the `validUntil` attribute value, if it is provided.
- The anchored-certificate trust model cannot be used with the single logout (SLO) redirect binding because the certificate cannot be included with the logout request.
- 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.

Composite Adapter configuration

Issue

SLO is not supported when users are authenticated through a Composite Adapter instance that contains another instance of the Composite Adapter.

Self-service password reset

Issue

Passwords can be reset for Microsoft Active Directory user accounts without the permission to change password.

OAuth

Issue

PingFederate does not support a case-sensitive naming convention for OAuth client ID values when client records are stored in a directory server. For example, after creating a client with an ID value of `sampleClient`, PingFederate does not allow the creation of another client with an ID value of `SampleClient`.

Although it's possible to create clients using the same ID values with different casings when client records are stored in XML files, a database server, or custom storage, we recommend not doing so to avoid potential record migration issues.

Customer identity and access management

Issue

Some browsers display a date-picker user interface for fields that have been designed for date-specific inputs. Some browsers do not. If one or more date-specific fields are defined on the registration page or the profile management page (or both), end users must enter the dates manually if their browsers do not display a date-picker user interface for those fields.

Provisioning

Issue

- 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.
- The **`totalResults`** value in SCIM responses indicates the number of results returned in the current response, not the total number of estimated results on the LDAP server.

Logging

Issue

- 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, the **`USER_KEY`** attribute will not be masked in the server logs. Other persistent grant attributes will be masked.

- Even if a source attribute has been configured for masking in an IdP adapter and the source attribute is mapped as the adapter's unique user key, the user key attribute is not masked in the server or audit logs.

Database logging

Issue

- 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, the `USER_KEY` attribute will not be masked in the server logs. Other persistent grant attributes will be masked.
- Even if a source attribute has been configured for masking in an IdP adapter and the source attribute is mapped as the adapter's unique user key, the user key attribute is not masked in the server or audit logs.

RADIUS NAS-IP-Address

Issue

The RADIUS NAS-IP-Address is only included in Access-Request packets when the `pf.bind.engine.address` is set with an IPv4 address. IPv6 is not supported.

Amazon SNS Notification Publisher

Issue

When deploying PingFederate with a forward proxy, plugins based on the AWS SDK, such as the Amazon SNS Notification Publisher, will only honor the `http.proxyHost`, `http.proxyPort`, `http.proxyUser`, and `http.proxyPassword` properties in `run.properties`. The plugin will rely on these properties even if the service URL is `https`.

Deprecated features

`authorizationDetails` field deprecation

Info PF-34682

The `authorizationDetails` JSON field returned by the OAuth consent management endpoint has been deprecated in favor of the new `authorizationDetail` and `authorizationDetailDescription` fields.

Learn more about the consent management endpoint in OAuth Consent Management Service.

PingFederate 12.0.11 (April 2026)

New features and enhancements

Unconnected cluster node startup

Improved PF-38898

We added the `force.require.replication.data.on.startup` parameter to the `cluster-config-replication.conf` file.

This parameter allows you to prevent an engine node from starting up without establishing a connection to the cluster.

Learn more in Cluster management.

Resolved issues

OGNL code test

Security PF-38742

We improved role-based access control (RBAC) for the administrative expression testing endpoint. Access to expression evaluation is now limited to appropriately privileged roles, ensuring alignment with intended administrative permissions.

SLO failure

Fixed PF-38442

We fixed a defect where front-channel logouts requests to `/idp/startSLO.ping` failed to send logout requests to relying party URIs.

Dyanmic JWKS rotation timer

Fixed PF-38903

We fixed a defect that prevented dynamic JWKS rotation timing from resetting after a node joined a cluster.

PingFederate 12.0.10 (October 2025)

Resolved issues

Host header redirect

Security PF-37460

We've fixed a security vulnerability that could have allowed malicious parties to redirect PingFederate admin console traffic using a spoofed Host header.

Virtual hostname accuracy in email notifications

Fixed PF-37964

We've fixed a defect where a template variable incorrectly used the primary PingFederate base URL instead of the virtual host name in some email notifications.

HTML flow login and Authentication API

Fixed PF-38039

We've fixed a defect that could potentially allow a user to access an HTML browser sign-on page when the Authentication API redirectless mode is used.

Learn more in PingFederate unexpected template rendering in redirectless mode in the Ping Identity Support Knowledge Base.

LDAP account lockout

Fixed PF-38043

We've fixed a defect where PingFederate could incorrectly lock user accounts during an LDAP connectivity failure with Active Directory. This fix applies to all LDAP datastore types except for Generic LDAP.

IdP Adapter duplicate attribute sources

Fixed PF-38060

We've fixed a defect that caused IdP adapters to duplicate attribute sources when an SP connection was updated using the Admin API.

PingFederate 12.0.9 (July 2025)

Resolved issues

Admin console IP exposure

Security PF-33113

We've fixed a security vulnerability that could have allowed malicious parties to extract the PingFederate administrative console's IP address through HTTP Response headers.

Refresh token MySQL deadlocks

Fixed PF-35868

We've fixed a defect that caused multiple refresh token requests in short succession to result in JDBC data source deadlocks and duplicated data entry into the database.

This fix can cause significant performance issues if PingFederate or the JDBC data source has insufficient resources.

Unnecessary ID token reissued with secondary client secret

Fixed PF-37450

We've fixed a defect that caused the token endpoint to unnecessarily reissue an ID token when using a secondary client secret and an asymmetric algorithm for token signing and encryption.

PingFederate 12.0.8 (May 2025)

New features and enhancements

NATIVE_S3_PING update

Info PF-37234

We've updated the behavior of the NATIVE_S3_PING discovery protocol when the `remove_all_data_on_view_change` parameter is active.

Previously, the protocol would delete all files in the S3 bucket, which could lead to the creation of an unwanted subcluster.

Now the protocol deletes all files except for its own to prevent the S3 bucket from being empty.

Learn more in Dynamic cluster discovery.

Resolved issues

Group membership loss during provisioning

Fixed PF-36874

We've fixed a defect where temporary connection loss to the source datastore during provisioning could lead to unintended membership information loss on the target SaaS application.

Secondary secret missing ID token claim

Fixed PF-37279

We've fixed a defect that caused the ID token claim to be omitted when an OAuth client uses the secondary secret.

PingFederate 12.0.7 (January 2025)

Resolved issues

Cross-site scripting

Security PF-36304 PF-36311 PF-36313

We've fixed a security vulnerability where PingFederate accepted cross-site scripting inputs.

Email verification failure after registration workflow

Fixed PF-36574

We've fixed a defect that caused the email verification screen to fail to appear when a user registered through an authentication source.

OAuth Client Set Authentication Selector with DynamoDB

Fixed PF-36662

We've fixed a defect that caused an error in searching for OAuth Client for OAuth Client Set Authentication Selector when DynamoDB is the client storage.

PingFederate 12.0.6 (November 2024)

Resolved issues

Provisioning character limit

Fixed PF-36035

We've fixed a defect that caused outbound provisioning to fail and cease if a source user object exceeded a 255-character limit. In the new behavior, PingFederate will skip user objects that exceed 255 characters and log a warning.

PingDirectory password warning

Fixed PF-36232

We've fixed a defect that prevented PingFederate from issuing a password expiration warning when using PingDirectory as a datastore.

Multiple application requests within a browser

Fixed PF-36239

We've fixed a defect that could cause inconsistent sessions or authentication errors when starting multiple applications in different browser tabs at the same time.

Device authorization grant time zone error

Fixed PF-36261

We've fixed a defect that caused device authorization grant flow errors when clustered server nodes are in different time zones.

PingFederate 12.0.5 (August 2024)

Resolved issues

Relative path symbolic links retrieve wrong file

Security PF-35678

We've fixed a defect that caused PingFederate to retrieve the wrong file when using relative paths in symbolic links.

Refresh token time zone discrepancies

Fixed PF-35867

We've fixed a defect that caused refresh tokens to roll prematurely when making authorization requests to servers in different time zones.

Maintenance upgrade includes entire SDK directory

Fixed PF-35867

We've fixed a defect that caused the incremental update package for PingFederate versions 12.0 and 12.1 to unnecessarily install the entire SDK directory.

PingFederate 12.0.4 (July 2024)

Resolved issues

Refresh token rolls when configured not to roll

Fixed PF-35166

We've fixed a defect that caused PingFederate to roll refresh tokens when **Refresh Token Rolling Policy** is disabled but **Refresh Token Rolling Interval** has a value.

OAuth client only validates one access token manager when `aud` parameter included

Fixed PF-35737

We've fixed a defect that caused PingFederate to validate only the first OAuth client access token manager it found when **Validate Against All Eligible Access Token Managers** was checked, and the `aud` parameter was included in the request.

Custom adapter not returning IPv4 addresses

Fixed PF-35783

We've fixed a defect where PingFederate failed to return IPv4 addresses in a custom adapter request using the `request.getRemoteAddr()` method.

Error message after user session expires

Fixed PF-35815

We've fixed a defect that caused PingFederate to present an error message when user tries to sign on again after a session expires due to inactivity.

OIDC admin login failure

Fixed PF-34523

We've fixed a defect that caused the OIDC administrative console login to fail when the `node.group.id` didn't match a server's node id.

OAuth client in-use detection

Fixed PF-35744

We've fixed a defect where client in-use detection caused an IndexOutOfBoundsException when a custom solution is used for client storage.

ClientManagerDynamoDBImpl changes not implemented

Fixed PF-35753

We've fixed a defect that caused changes in `ClientManagerDynamoDBImpl` not to apply when performing a bulk import or using the configuration store API unless you restarted PingFederate.

Davinci integration kit

Info PF-35838

The Davinci integration kit has been updated to version 1.2.

PingFederate 12.0.3 (May 2024)

New features and enhancements

PingOne admin URL property

New PF-31859

Added support for the Australia region to the `pf.pingone.admin.url.region` property.

The Asia region is deprecated. We recommend using the Australia region instead.

Learn more in Configuring PingFederate properties.

Resolved issues

Authentication API allows different user for change password flow

Fixed PF-35609

Fixed a defect that caused the authentication API to allow a different user to proceed with the `MUST_CHANGE_PASSWORD` function than the user who initiated the flow.

> **Note**
>
> In all cases, the target user's password was required to complete the change password operation.

Memory heap increase when using admin API on policy tree

Fixed PF-35423

Fixed a defect that caused PingFederate not to release memory when using the admin API on the policy tree.

Authentication API password change flow ignores credentials

Fixed PF-35618

Fixed a defect that caused the authentication API to ignore credentials for password changes provided after user authentication.

Authentication API validation error

Fixed PF-35430

Fixed a defect that caused a validation error in the authentication API when including the `ui_locales` parameter.

Provisioner uses wrong time zone when data source and PingFederate are in different time zones

Fixed PF-35286

Fixed a defect that caused redundant user provisioner updates when the data source and PingFederate were in different time zones.

Bypass authorization approval

Fixed PF-35395

Fixed a defect that caused PingFederate to ignore the **Bypass Authorization Approval** setting when **Bypass Authorization For Previously Approved Consents** is enabled.

PingFederate 12.0.2 (April 2024)

Resolved issues

Java thread exhaustion in PingOne Advanced Services

Fixed PF-35411

Fixed a defect that caused repeated looping in authentication policy involving a local Identity profile.

OAuth clients In Use detection

Fixed PF-35407

Fixed a defect with In Use detection when DynamoDB is used for OAuth client storage.

OIDC policy DELETE request timeout

Fixed PF-35357

Fixed a defect where deleting an OIDC policy fails when using DynamoDB storage for a large number of OAuth clients.

Authentication policy extended properties using OGNL

Fixed PF-35111

Fixed a defect where extended properties retrieved by OGNL are not populated.

Policy fragment rules processing

Fixed PF-35134

Fixed a defect that caused PingFederate to not process authentication policy rules for fragment nodes that do not contain an output contract.

Active Directory binary attribute caused thread proliferation

Fixed PF-35142

Fixed a defect that caused LDAP data source connection pools to close when still in use after the LDAP data source is modified and replicating under heavy load.

Mixed maintenance release cluster caused JWKS errors

Fixed PF-35195

Fixed a defect that caused errors in synchronization and accessing dynamic JSON Web Key Set (JWKS) keys when running a cluster that was a mix of PingFederate versions 12.0 and

12.0.1.

JWKS algorithm parameter not populated after processing shared keys from cluster

Fixed PF-35309

Fixed a defect that caused the `alg` parameter to fail to populate when EC dynamic keys are rotated on a lead cluster node and shared to the cluster.

PingOne MFA Integration Kit

Improved PF-35325

Upgraded the PingOne MFA Integration Kit to version 2.3.1.

Lightning LDAP library

Improved PF-35310

Upgraded the lightning LDAP library to version 1.5.22.

Upgraded Jetty Library

Improved PF-35184

Upgraded the Jetty library to version 9.4.54.v20240208.

PingFederate 12.0.1 (February 2024)

New features and enhancements

Runtime notification when thread dumps are enabled but `log4j2.xml` is not configured

Improved PF-34832

Added a feature to generate a warning message on the **Runtime Notifications** tab if you have enabled thread dumps, but you have not configured the `ThreadDumpAppender` and `ThreadDumpLogger` properties in the `log4j2.xml` file.

To learn more about configuring thread pool exhaustion events, see Configuring runtime notifications.

Randomly-generated provisioner node ids

Improved PF-30913

Added a feature allowing you to generate random `provisioner.node.id` values.

To learn more about configuring provisioners, see Deploying provisioning failover.

Custom KeyID

Improved PF-34883

Added a feature allowing administrators to define custom KeyID values for static OAuth and OIDC keys and token signing keys.

Fixed an defect that caused PingFederate to not publish the `alg` parameter on the JWKS endpoint. This issue occurred for dynamically-generated EC signing keys on engine nodes.

To learn more about keys, see Keys for OAuth and OpenID Connect.

Resolved issues

Rest datastore security vulnerability

Security PF-34720

Fixed a JSON injection vulnerability in REST datastores described in security advisory SECADV044.

Runtime nodes security vulnerability

Security PF-34896

Fixed a path traversal vulnerability in Runtime nodes described in security advisory SECADV044.

OpenID Connect policy management editor security vulnerability

Security PF-35081

Fixed a Cross-Site Scripting vulnerability in the OpenID Connect Policy Management Editor described in security advisory SECADV044.

GET SAML request signature processing error

Fixed PF-34641

Fixed a defect where SAML requests using HTTP GET method with multiple signature-related parameters encoded in the *RelayState* parameter were causing errors in processing signature validation.

NPE notification error

Fixed PF-34813

Fixed a defect that caused PingFederate to issue null pointer exception (NPE) errors when querying the token endpoint.

Certificate expiry notification error

Fixed PF-34854

Fixed a defect that caused the certificate expiry warning notification icon to remain when there were no notifications to display.

Reencyption causes connection or client to fail on engine

Fixed PF-34409

Fixed a defect where changes made on the administrative console were not replicated to the engine during reencryption.

JMX registration failure for imported archives

Fixed PF-34796

Fixed a defect that caused the JMX monitoring to fail to register archive files that are imported to PingFederate.

Content type changes if `well_known` endpoint response is too large

Fixed PF-34865

Fixed a defect that caused the `content-type` of a response from the `well_known` endpoint to change from JSON to HTML if a response is too large.

PingFederate displays unlock your account page for unlocked users

Fixed PF-34701

Fixed a defect that caused PingFederate to display an **unlock your account** page during self-service password reset to accounts that are not locked.

RHEL 8 using OS-level FIPS causes PingFederate failure

Fixed PF-34879

Fixed a defect that caused PingFederate to fail on startup when installed on a Red Hat Enterprise Linux (RHEL) server with OS-levels FIPS enabled.

Error message for authentication policy fragment with invalid `localIdentityRef`

Fixed PF-34882

Fixed a defect that returned a `500` error with no details when an authentication policy fragment had a `LOCAL_IDENTITY_MAPPING` action with an invalid `localIdentityRef` ID.

Unable to deobfuscate grant attributes

Fixed PF-34839

Fixed a defect where PingFederate was unable to deobfuscate grant attributes of a certain length.

Valid Authorization policy generates "Configuration Error" message

Fixed PF-34853

Fixed a defect that caused PingFederate to incorrectly return an `Invalid Configuration` error for a valid authentication policy.

PingFederate 12.0 (December 2023)

New features and improvements in PingFederate 12.0.

New features and enhancements

Support for RP-initiated logout

New PF-34418

OpenID Connect (OIDC) relying party (RP) initiated logout allows OAuth clients to request that the OpenID Provider (OP) perform a federated logout. PingFederate now supports this standard, both when PingFederate acts as the OP as well as when it acts as the RP via an OIDC IdP connection.

For more information, see OAuth Client Management Service, Configuring OpenID Provider information, and OpenID Connect RP-initiated logout endpoint.

Add risk provider to Identifier First Adapter

New PF-34415

You can now add risk provider such as CAPTCHA to Identifier First adapters.

For more information, see Configuring an Identifier First Adapter instance

Skip redirect to authentication application if no action is required

New PF-34413

API-capable IdP adapters can now prevent a redirect to the authentication application if no user interaction is required.

For more information, see Upgrade considerations introduced in PingFederate 12.x.

Alert and report when approaching `maxThreads`

New PF-34437

You can now configure runtime notifications to alert you when the number of threads in use exceeds a set threshold. You can also use this feature to initiate and log a thread dump event.

For more information, see Configuring runtime notifications.

Persist consent decision when revoking `refresh_token`

New PF-33318

You can now configure your authorization server settings for OAuth and OIDC users so that their decisions to grant access can be persisted after a `refresh_token` is revoked.

For more information, see **Authorization Consent** in Configuring authorization server settings.

Admin console notification of expiring certificates

New PF-34428

PingFederate will now issue a notification in the admin console before a certificate expires. You can configure the duration of the notification before and after expiry in the **Runtime Notifications** menu.

Deleted certificates are removed from the notifications menu.

For more information, see Configuring runtime notifications.

Selective replication for connections and OAuth clients

New PF-33989

We further improved support for self-service and application on-boarding use cases. OAuth applications and SAML connections can now be replicated to PingFederate engine nodes without affecting any dependencies. This enhancement lets development teams manage their applications without the help of PingFederate administrators. For more information, see Cluster management.

OpenID Connect Front-Channel Logout support

New PF-33986

Continuing the PingFederate tradition of recognizing open identity standards, it now supports the OpenID Connect Front-Channel Logout specification. This feature enables global sign-off user journeys. It's available in addition to PingFederate's proprietary front-channel logout protocol. For more information, see Configuring OAuth clients.

Log category to capture details of protocol requests and responses

New PF-33987

For OpenID Connect IDP connections, log files now include more details so that you can analyze and resolve connection problems easier. You can enable this feature just by selecting a checkbox in the **Log Settings**. For more information, see Log settings.

Creating short-lived or non-persistent sessions when This is my device isn't selected

New PF-33982

Now you can configure PingFederate to enable sessions on shared devices. Devices can be configured as private or public (unspecified) and maintain persistent sessions. This feature is available through the HTML Form Adapter. For more information, see Configuring authentication sessions.

The CyberArk Secret Manager can pull different username values from CyberArk

New PF-33985

The integration with the CyberArk Secret Manager now allows access to all values available through the CyberArk interface. This gives you more freedom when building user journeys. For more information, see Configuring instances of the secret manager plugin for the CyberArk Credential Provider.

Password reset email OTL returns users to authentication API applications when using redirectless mode

New PF-33983

When you use OAuth and OpenID Connect flows with `response_mode=pi.flow`, users are redirected back to the associated authentication application rather than to PingFederate. This is enables more consistent user journeys. For more information, see Configuring self-service account recovery.

Amazon DynamoDB account linking

New PF-33988

To further support Amazon DynamoDB use cases, now you can also use account linking with this NoSQL database. For more information, see Configuring an Amazon DynamoDB for account-link storage.

Optional input and output contracts for policy fragments

New PF-33332

This feature simplifies the use of PingFederate policies because it no longer requires input or output contracts for certain fragments. This improves the readability, maintainability, and performance of these policies. For more information, see Policy fragments.

OpenBanking plugin support for the `dpop_bound_access_tokens` parameter

New PF-33631

Enhancing PingFederate's support for OAuth DPoP, this release includes support for this type of access token. It lets developers learn more about the use and importance of the `dpop_bound_access_tokens` parameter. For more information about the parameter, see the PingFederate Open Banking Software Assertion Validator plug-in on GitHub.

Toggle plugin creation/initialization during startup

New PF-34640

In rare cases where plugin creation and initialization significantly slows down PingFederate startup, you can now turn off plugin creation and initialization. Plugins will then only be initialized on first use.

The default startup behavior is recommended for most customers. For more information about this option and the tradeoffs involved in enabling it, open a support case.

PingOne Protect Integration Kit

New PF-34147

The PingOne Protect Integration Kit is now bundled with PingFederate.

PingID Integration Kit

Improved PF-34369

The PingID Integration Kit has been updated to version 2.26.

PingOne MFA Integration Kit

Improved PF-34368

The PingOne MFA Integration Kit has been updated to version 2.2.1.

Java 17 support for Thales Luna Network HSM integration

Improved PF-34168

When integrating with Thales Luna Network hardware security modules (HSMs), you can now use Java 17.

For more information, see Integrating with Thales Luna Network HSM

Improved OGNL expression logging

Improved PF-34050

The administrator audit log file (`admin.log`) now logs any OGNL expression tests performed and the expression variables used with an event type of `TEST_EXPRESSION`. For more information, see Administrator audit logging.

Improved CSD

Improved PF-33095

The Collect Support Data (CSD) script has been improved to capture more details.

Authenticating to Azure SQL Managed Instance through Azure Active Directory

Improved PF-33621

Now PingFederate supports authentication to Azure SQL Managed Instance through Azure Active Directory without a username and password. For more information, see Configuring a JDBC connection.

Upgraded BCFIPS library

Improved PF-32747

Upgraded the BCFIPS library to 1.0.2.4, which now supports enabling BCFIPS mode with Java 17.

For more information, see Bouncy Castle FIPS provider and Integrating Bouncy Castle FIPS providers.

Upgraded third-party libraries

Improved

- Upgraded Jetty to version 9.4.53.v20231009.
- Upgraded JGroups to version 4.2.24.Final.

Resolved issues

Improved client authentication security

Security PF-34645

Fixed a potential security vulnerability described in SECADV040.

Resolved a vulnerability in the Initial Setup Wizard

Security PF-34646

Fixed a Server-Side Request Forgery vulnerability in the Initial Setup Wizard described in security advisory SECADV041.

Prevent JGroups thread pool exhaustion in large clusters

Fixed PF-34718

For fresh installs, we changed the default value of **`pf.cluster.TCPPING.return_entire_cache`** in `jgroups.properties` from `true` to `false`.

This prevents an issue where remote procedure calls (RPCs) can be dropped in large clusters that use TCPPING.

For more information, see Upgrade considerations introduced in PingFederate 12.x.

Swagger response for oauth/accessTokenMappings

Fixed PF-34500

Fixed an issue with the administrative API doc on the `/oauth/accessTokenMappings` endpoint not matching the actual endpoint response.

`multi-value contains DN` in policy rule check no longer case-sensitive

Fixed PF-33560

Policy Rules conditions that use `multi-value contains DN` now ignore case while comparing the DN value.

Log messages about illegal characters in API calls

Fixed PF-33305

Now log messages about illegal characters in API calls are logged at the DEBUG level rather than the WARN level.

Support for `none` as a valid token endpoint value

Fixed PF-34115

Added the value `none` to `/.well-known/openid-configuration/token_endpoint_auth_methods_supported`

The `id_token_jti` property in token endpoint responses

Fixed PF-34210

The `id_token_jti` property is no longer included in token endpoint responses.

*Administrative API defect when fragment rules have **Default to Success** disabled*

Fixed PF-34216

Fixed an administrative API defect when a fragment rule had **Default to Success** disabled

Fixed `/idp/startSLO.ping` `404` caused by virtual issuer configuration

Fixed PF-34322

Fixed an issue that was returning a `404` error if the `/idp/startSLO.ping` endpoint was hit while a virtual issuer was configured. You can now configure virtual issuers with a context path.

Client JWKS now sets properly when using DynamoDB storage

Fixed PF-34504

Clients that maintain a JWKS endpoint can now use private key JWT based authentication when requesting an access token.

Fixed NPE when checking an existing persistent grant that is expired with DynamoDB

Fixed PF-34606

Checking for existing but expired grants with DynamoDB no longer causes a null pointer exception error (NPE).

Connections close after getting a `401` or `403` from PingOne API

Fixed PF-34545

Fixed an issue preventing PingFederate from closing connections after receiving a `401` or `403` response from PingOne MFA.

PingFederate systematically adds server-side sort control

Fixed PF-33466

You can now turn off server-side sorting via a configuration option.

Unable to copy and paste policy contract in specific situations

Fixed PF-34433

You can now copy and paste a policy contract below a selector node.

XML decryption failing with `KeyName` element

Fixed PF-34536

Fixed an issue where decryption of an encrypted SAML element could fail if a `KeyName` was specified.

One-time link in password-reset email messages

Fixed PF-33983

When using redirectless mode, now the one-time link (OTL) in password-reset email messages returns users to the authentication API application configured for the policy, rather than to PingFederate.

Incorrect error template when using service provider authentication policies

Fixed PF-34111

When a service provider (SP) authentication policy fails, PingFederate now renders the `sp.sso.error.page.template.html` page instead of the `idp.sso.error.page.template.html` page.

Updating OAuth clients with dynamic client registration

Fixed PF-34146

Fixed a defect where an OAuth client created with dynamic client registration (DCR) couldn't be updated with DCR after it was modified with the administrative console.

Idle JDBC datastore connections

Fixed PF-34163

Now PingFederate closes idle JDBC datastore connections until the minimum pool size is reached instead of closing and recreating all of them.

The `id_token_jti` property in token endpoint responses

Fixed PF-34210

The `id_token_jti` property is no longer included in token endpoint responses.

Administrative API defect when fragment rules have Default to Success disabled

Fixed PF-34216

Fixed an administrative API defect when a fragment rule had **Default to Success** disabled

Email notifications for licensing events even when disabled

Fixed PF-34225

Resolved an issue that caused PingFederate to send email notifications for licensing events even though they were disabled in the **Runtime Notifications** configuration.

Jetty library upgrade

Fixed PF-31865

We upgraded the Jetty library, resolving CVE-2022-2047 and CVE-2022-2048.

OAuth scope names

Fixed PF-33056

Using `submit` and `onSubmit` as OAuth scope names in the administrative UI drop-down no longer causes front-end JavaScript errors.

Empty `authorization_details` omitted

Fixed PF-33174

The `authorization_details` claim in a JWT access token manager configuration is no longer sent if it's empty.

Policy fragment validation error

Fixed PF-33156

Policy fragments with valid authentication sources no longer fail with an Invalid Configuration error during runtime.

Eliminating redundant group updates

Fixed PF-33441

PingFederate, when configured with PingDirectory as an outbound provisioning data source, no longer sends redundant group updates in each provisioning cycle when the entry remains unchanged.

Potential security vulnerability

Fixed PF-33449

We've resolved a potential security vulnerability that is described in security advisory SECADV037.

PingFederate as a Windows service

Fixed PF-33450

We fixed an issue so that PingFederate as a Windows service now runs on Java 17. When updating to the latest maintenance release using an in-place update method (for example, from 11.3.0 to 11.3.x), in addition to the steps in Updating to the latest maintenance release, you must remove the existing PingFederate Windows service. After removal, re-install the PingFederate Windows Service to apply this fix.

Authentication policy fail path

Fixed PF-33519

When an OIDC identity provider (IdP) connection fails in an authentication policy, PingFederate now continues on to the fail path of the authentication policy.

Fragment mapping validation error

Fixed PF-33722

We resolved an issue that incorrectly produced an administrative API validation error when the fragment mapping references `context.RequestedUser` as the mapping source.

Authorization details within a RAR

Fixed PF-33863

PingFederate now processes authorization details within a rich authorization request (RAR) as a JSON Array in a JWT request. Additionally, PingFederate no longer supports authorization details sent as stringified JSON arrays.

Cluster engine nodes starting without replication data

Fixed PF-33881

Resolved a replication issue that, in rare cases, caused an engine node in a cluster to start without replication data from other nodes.

Server error when revoking user sessions

Fixed PF-33920

Resolved an issue that prevented user sessions from being revoked through the session management API when using persistent sessions.

Potential security vulnerability

Fixed PF-33935

We've resolved a potential security vulnerability that is described in security advisory SECADV037.

Fragment mapping validation errors

Fixed PF-33957

When utilizing the PingFederate administrative API to create or update a fragment that includes another fragment, the API will no longer produce a validation error when fragment mapping involves an input source type.

Updated template variable

Fixed PF-34016

The `message-template-end-user-password-change.html` template now contains the *USERNAME* variable.

Potential security vulnerability

Fixed PF-34017

We've resolved a potential security vulnerability that is described in security advisory SECADV037.

Policy evaluation issue

Fixed PF-34051

We fixed a policy evaluation issue that occurred when `ui_locales` was present in an authentication request.

Certificate import improvements

Fixed PF-34074

We updated the administrative UI to include certification serial number in the drop-down, thus preventing import errors for certifications sharing the same Subject DN and expiration date combination.

DynamoDB attribute lookup error

Fixed PF-34099

We fixed an attribute lookup error that occurred when different DynamoDB attributes shared an overlapping path.

Certificate in-use detection slowdown

Fixed PF-34077

We fixed a defect that caused PingFederate to check every certificate when loading certificate-related pages in the administrative interface, which slowed down performance.

Known issues and limitations

PingID password credential validator with integrated RADIUS server

Issue

PingFederate versions 11.1.4, 11.1.5, 11.2.1, and 11.2.2 contain version 3.0.2 of the PingID password credential validator (PCV). That version of the PCV has known issues that you should review before upgrading. For more information, see Known issues in PingID RADIUS PCV 3.0.2.

Administrative console and administrative API

Issue

- Although PingFederate 11.3 and later support DPoP, a known limitation is that the following features don't support DPoP when PingFederate is the RP:
  - The administrative console authentication scheme using OIDC
  - The administrative API authentication scheme using OAuth 2.0
- /bulk: Only resource types currently supported by the administrative API are included in the exported data. We don't intend to introduce administrative API support to the following areas:
  - SAML 2.0 IdP Discovery
  - SAML 2.0 SP Affiliation
  - SMS Provider
- Previously, the administrative API did not accurately reflect a **Persistent Grant Max Lifetime** setting of 29 days (or shorter) with the selection of the **Grants Do Not Timeout Due To Inactivity** option. As a result, if you have configured such OAuth authorization server settings and have generated a bulk export in version 10.0 through 10.0.2, we recommend that you re-generate a new bulk export after upgrading to

version 10.0.3 (or a more recent version). The newly exported data does not contain the aforementioned flaw, and you can safely import it to version 10.0.3 (or a more recent version).

- When enabling mTLS certificate-based authentication, administrators often configure a list of acceptable client certificate issuers. When you use a browser to access the console or the administrative API documentation, PingFederate returns to the browser the list of acceptable issuers as part of the TLS handshake. If the browser's client certificate store contains multiple client certificates, the browser often presents you only the certificates whose issuer matches one of the acceptable issuers. However, when PingFederate runs in a Java 11 environment, Chrome presents you all its configured client certificates, regardless of whether the issuer matches one of the acceptable issuers or not.
- When using mTLS authentication to authenticate to an LDAP server for administrative console or administrative API access, PingFederate doesn't support using a Microsoft Active Directory server.
- Prior to toggling the status of a connection with the administrative API, you must ensure that any expired certificates or no longer available attributes are replaced with valid certificates or attributes; otherwise, the update request fails.
- When creating or updating a child instance of a hierarchical plugin, the administrative API retains objects with an `"inherited": false` name/value pair (or without such name/value pair altogether), ignores those with a value of `true`, and returns a 200 HTTP status code. No error messages are returned for the ignored objects.
- Using the browser's navigation mechanisms (for example, the **Back** button) causes inconsistent behavior in the administrative console. Use the navigation buttons provided at the bottom of windows in the PingFederate console.
- Using the PingFederate console in multiple tabs on one browser might cause inconsistent behavior which could corrupt its configuration.
- If authenticated to the PingFederate administrative console using certificate authentication, a session that has timed out might 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 sign-on page, and then back to the administrative console after authentication is complete. Similar behavior applies for certificate authentication, in principle. However, because

the browser might automatically resubmit the certificate for authentication, the browser might redirect to the administrative console and not the sign on page.

PingOne MFA CIBA Authenticator

Issue PingOne MFA

PingFederate 11.3 is not compatible with the PingOne MFA CIBA Authenticator bundled in PingOne MFA Integration Kit version 2.1 and earlier. This issue was resolved in version 2.2 of that integration kit.

TLSv1.3

Issue

For Java versions that don't support TLSv1.3 (meaning versions earlier than 8u261), PingFederate fails on start up with a `NoSuchAlgorithmException` exception. To resolve this error, remove `TLSv1.3` from the following settings in the `run.properties` file:

- **`pf.tls.client.protocols`**
- **`pf.tls.runtime.server.protocols`**
- **`pf.tls.admin.server.protocols`**

TLS cipher suite customization

Issue

PingFederate's TLS cipher suites can be customized by modifying `com.pingidentity.crypto.SunJCEManager.xml` (or a similarly-named file if BCFIPS or an HSM is configured). After updating the file and replicating, all cluster nodes must be restarted for the change to take effect.

Java

Issue

- CloudHSM is not supported when using Java 17.

- Updating Java version 8 to version 11 results in an error when PingFederate is already installed and running on Windows. To work around this issue, uninstall and reinstall the PingFederate Windows service by running the `UninstallPingFederateService.bat` and `InstallPingFederateService.bat` files located in `<pf_install>/pingfederate/sbin/wrapper`.

HSMs

Issue

AWS CloudHSM

- It is not possible to use an elliptic curve (EC) certificate as an SSL server certificate.
- TLS 1.3 is not currently supported.

Thales HSMs

- JWT token decryption using ECDH-ES may fail. This issue only arises if PingFederate is configured with static OAuth and OpenID Connect keys, a static key is stored on the HSM, and PingFederate is consuming a token encrypted with this key.
- It is not possible to use an EC certificate as an SSL server certificate.
- TLS 1.3 is not currently supported.

Entrust HSMs

- JWT token decryption using ECDH-ES may fail. This issue only arises if PingFederate is configured with static OAuth and OpenID Connect keys, a static key is stored on the HSM, and PingFederate is consuming a token encrypted with this key.
- It is not possible to import a PKCS12- or PEM-formatted EC certificate.
- It is not possible to use an EC certificate as an SSL server certificate.
- TLS 1.3 is not currently supported.

SSO and SLO

Issue

- When consuming SAML metadata, PingFederate does not report an error when neither the `validUntil` nor the `cacheDuration` attribute is included in the metadata. Note that PingFederate does reject expired SAML metadata as indicated by the `validUntil` attribute value, if it is provided.
- The anchored-certificate trust model cannot be used with the Single log off (SLO) redirect binding because the certificate cannot be included with the logout request.
- 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.

Composite Adapter configuration

Issue

SLO is not supported when users are authenticated through a Composite Adapter instance that contains another instance of the Composite Adapter.

Self-service password reset

Issue

Passwords can be reset for Microsoft Active Directory user accounts without the permission to change password.

OAuth

Issue

PingFederate does not support a case-sensitive naming convention for OAuth client ID values when client records are stored in a directory server. For example, after creating a client with an ID value of `sampleClient`, PingFederate does not allow the creation of another client with an ID value of `SampleClient`.

Although it's possible to create clients using the same ID values with different casings when client records are stored in XML files, a database server, or custom storage, we recommend not doing so to avoid potential record migration issues.

Customer identity and access management

Issue

Some browsers display a date-picker user interface for fields that have been designed for date-specific inputs. Some browsers do not. If one or more date-specific fields are defined on the registration page or the profile management page (or both), end users must enter the dates manually if their browsers do not display a date-picker user interface for those fields.

Provisioning

Issue

- 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.
- The `totalResults` value in SCIM responses indicates the number of results returned in the current response, not the total number of estimated results on the LDAP server.

Logging

Issue

- 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, the `USER_KEY` attribute will not be masked in the server logs. Other persistent grant attributes will be masked.
- Even if a source attribute has been configured for masking in an IdP adapter and the source attribute is mapped as the adapter's unique user key, the user key attribute is not masked in the server or audit logs.

Database logging

Issue

- 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, the `USER_KEY` attribute will not be masked in the server logs. Other persistent grant attributes will be masked.

- Even if a source attribute has been configured for masking in an IdP adapter and the source attribute is mapped as the adapter's unique user key, the user key attribute is not masked in the server or audit logs.

RADIUS NAS-IP-Address

Issue

The RADIUS NAS-IP-Address is only included in Access-Request packets when the `pf.bind.engine.address` is set with an IPv4 address. IPv6 is not supported.

Amazon SNS Notification Publisher

Issue

When deploying PingFederate with a forward proxy, plugins based on the AWS SDK, such as the Amazon SNS Notification Publisher, will only honor the `http.proxyHost`, `http.proxyPort`, `http.proxyUser`, and `http.proxyPassword` properties in `run.properties`. The plugin will rely on these properties even if the service URL is `https`.

Deprecated features

SAML IdP Discovery and SAML SP Affiliations

Info

As of PingFederate 12.0, these features have been deprecated, and will be removed in a future release.

Text Message SSPR

Info

Support for text message self-service password reset (SSPR) is deprecated as of PingFederate 12.0 and will be removed in a future release. To ensure continued support,

migrate your SSPR configurations to an authentication policy using the One-Time Passcode Integration Kit.

Upgrade from PingFederate 6.x and 7.x

Info

Starting with version 12.0, PingFederate no longer supports upgrading from PingFederate version 6.x and 7.x.

PingOne Fraud integration kit

Info PingOne Fraud

The PingOne Fraud integration kit is no longer bundled with PingFederate.

Microsoft Internet Explorer 11

Info

Ping Identity commits to deliver the best experience for administrators and users. As we continue to improve our products, we encourage you to migrate off of Microsoft Internet Explorer 11. Starting with PingFederate 11.0, Internet Explorer 11 is no longer included in the PingFederate qualification process for administrators or users. For a list of supported browsers, see System requirements.

Configcopy tool, Connection Management Service, SSO Directory Service

Info

As of PingFederate 10.2, these features have been deprecated and will be removed in a future release.

Oracle Directory Server Enterprise Edition

Info

As Oracle ended its Premier Support for Oracle Directory Server Enterprise Edition (ODSEE 11g) in December 2019, we no longer include ODSEE as part of the PingFederate

qualification process (starting with PingFederate 10.2). We continue to qualify against Oracle Unified Directory and other supported directory servers. For a full list, see System requirements.

SNMP

Info

Starting with PingFederate 10.2, monitoring and reporting through the SNMP has been removed.

Roles and protocols

Info

Starting with PingFederate 10.1, roles and protocols are always enabled and no longer configurable through the administrative console and API.

S3_PING discovery protocol

Info

Starting with PingFederate 10.1, the S3_PING discovery protocol has been deprecated. Customers running on AWS infrastructure should instead use NATIVE_S3_PING.

Red Hat Enterprise Linux install script

Info

Starting with PingFederate 10.0, the Red Hat Enterprise Linux install script is no longer available. To install PingFederate 10.0 for Linux, you must download and extract the product distribution `.zip` file.

PingFederate 11.3.15 (April 2026)

New features and enhancements

Unconnected cluster node startup

Improved PF-38898

We added the `force.require.replication.data.on.startup` parameter to the `cluster-config-replication.conf` file.

This parameter allows you to prevent an engine node from starting up without establishing a connection to the cluster.

Learn more in Cluster management.

Resolved issues

SLO failure

Fixed PF-38442

We fixed a defect where front-channel logouts requests to `/idp/startSLO.ping` failed to send logout requests to relying party URIs.

OGNL code test

Security PF-38742

We improved role-based access control (RBAC) for the administrative expression testing endpoint. Access to expression evaluation is now limited to appropriately privileged roles, ensuring alignment with intended administrative permissions.

Dyanmic JWKS rotation timer

Fixed PF-38903

We fixed a defect that prevented dynamic JWKS rotation timing from resetting after a node joined a cluster.

PingFederate 11.3.14 (October 2025)

Resolved issues

HTML flow login and Authentication API

Fixed PF-38039

We've fixed a defect that could potentially allow a user to access an HTML browser sign-on page when the Authentication API redirectless mode is used.

Learn more in PingFederate unexpected template rendering in redirectless mode in the Ping Identity Support Knowledge Base.

LDAP account lockout

Fixed PF-38043

We've fixed a defect where PingFederate could incorrectly lock user accounts during an LDAP connectivity failure with Active Directory. This fix applies to all LDAP datastore types except for Generic LDAP.

PingFederate 11.3.13 (September 2025)

Resolved issues

Refresh token MySQL deadlocks

Fixed PF-35868

We've fixed a defect that caused multiple refresh token requests in short succession to result in JDBC data source deadlocks and duplicated data entry into the database.

This feature can cause significant performance issues if PingFederate or the JDBC data source has insufficient resources.

Virtual hostname accuracy in email notifications

Fixed PF-37964

We've fixed a defect where a template variable incorrectly used the primary PingFederate base URL instead of the virtual hostname in some email notifications.

Apache Commons BeanUtils and Compress

Fixed PF-38029

PingFederate now uses the Apache Commons BeanUtils library version 1.11.0 and Apache Commons Compress library version 1.26.

PingFederate 11.3.12 (May 2025)

Resolved issues

Unnecessary ID token reissued with secondary client secret

Fixed PF-37450

We've fixed a defect that caused the token endpoint to unnecessarily reissue an ID token when using a secondary client secret and an asymmetric algorithm for token signing and encryption.

PingFederate 11.3.11 (April 2025)

New features and enhancements

NATIVE_S3_PING update

Improved PF-37234

We've updated the behavior of the `NATIVE_S3_PING` discovery protocol when the **`remove_all_data_on_view_change`** parameter is active.

Previously, the protocol would delete all files in the S3 bucket, which could lead to the creation of an unwanted subcluster.

Now the protocol deletes all files except for its own to prevent the S3 bucket from being empty.

Learn more in Dynamic cluster discovery.

Resolved issues

Group membership loss during provisioning

Fixed PF-36874

We've fixed a defect that caused PingFederate to lose user group membership information when it lost contact with the datastore during provisioning operations.

Group membership loss during provisioning

Fixed PF-37279

We've fixed a defect that caused the ID token claim to be omitted when an OAuth client uses the secondary secret.

PingFederate 11.3.10 (December 2024)

Resolved issues

Cross-site scripting

Security PF-36304 PF-36311 PF-36313

We've fixed a security vulnerability where PingFederate accepted cross-site scripting inputs.

Email verification failure after registration workflow

Fixed PF-36574

We've fixed a defect that caused the email verification screen to fail to appear when a user registered through an authentication source.

OAuth Client Set Authentication Selector with DynamoDB

Fixed PF-36662

We've fixed a defect that caused an error in searching for OAuth Client for OAuth Client Set Authentication Selector when DynamoDB is the client storage.

PingFederate 11.3.9 (November 2024)

Resolved issues

Refresh token time zone discrepancies

Fixed PF-35867

We've fixed a defect that caused refresh tokens to roll prematurely when making authorization requests to servers in different time zones.

Provisioning character limit

Fixed PF-36035

We've fixed a defect that caused outbound provisioning to fail and cease if a source user object exceeded a 255-character limit. In the new behavior, PingFederate will skip user objects that exceed 255 characters and log a warning.

PingDirectory password warning

Fixed PF-36232

We've fixed a defect that prevented PingFederate from issuing a password expiration warning when using PingDirectory as a datastore.

Multiple application requests within a browser

Fixed PF-36239

We've fixed a defect that could cause inconsistent sessions or authentication errors when starting multiple applications in different browser tabs at the same time.

Device authorization grant time zone error

Fixed PF-36261

We've fixed a defect that caused device authorization grant flow errors when clustered server nodes are in different time zones.

PingFederate 11.3.8 (July 2024)

Resolved issues

OIDC admin login failure

Fixed PF-34523

We've fixed a defect that caused the OIDC administrative console login to fail when the `node.group.id` didn't match a server's node id.

OGNL `Extended Property` retrieval failure

Fixed PF-35111

We've fixed a defect that caused OGNL to fail to obtain the `Extended Property` value in authorization policies or fragments.

Refresh token rolls when configured not to roll

Fixed PF-35166

We've fixed a defect that caused PingFederate to roll refresh tokens when **Refresh Token Rolling Policy** is disabled but **Refresh Token Rolling Interval** has a value.

OAuth client only validates one access token manager when `aud` parameter included

Fixed PF-35737

We've fixed a defect that caused PingFederate to validate only the first OAuth client access token manager it found when **Validate Against All Eligible Access Token Managers** was checked, and the `aud` parameter was included in the request.

Custom adapter not returning IPv4 addresses

Fixed PF-35783

We've fixed a defect where PingFederate failed to return IPv4 addresses in a custom adapter request using the `request.getRemoteAddr()` method.

Davinci integration kit

Info PF-35838

The Davinci integration kit has been updated to version 1.2.

PingFederate 11.3.7 (May 2024)

New features and enhancements

PingOne admin URL property

New PF-31859

Added support for the Australia region to the `pf.pingone.admin.url.region` property.

The Asia region is deprecated. We recommend using the Australia region instead.

To learn more, see Configuring PingFederate properties.

Resolved issues

Authentication API allows different user for change password flow

Fixed PF-35609

Fixed a defect that caused the authentication API to allow a different user to proceed with the `MUST_CHANGE_PASSWORD` function than the user who initiated the flow.

Note that in all cases, the target user's password was required to complete the change password operation.

Memory heap increase when using admin API on policy tree

Fixed PF-35423

Fixed a defect that caused PingFederate not to release memory when using the admin API on the policy tree.

Authentication API password change flow ignores credentials

Fixed PF-35618

Fixed a defect that caused the authentication API to ignore credentials for password changes provided after user authentication.

Authentication API validation error

Fixed PF-35430

Fixed a defect that caused a validation error in the authentication API when including the `ui_locales` parameter.

Provisioner uses wrong time zone when datasource and PingFederate are in different time zones

Fixed PF-35286

Fixed a defect that caused redundant user provisioner updates when the datasource and PingFederate were in different time zones.

PingFederate 11.3.6 (April 2024)

Resolved issues

Java thread exhaustion in PingOne Advanced Services

Fixed PF-35411

Fixed a defect that caused repeated looping in authentication policy involving a local Identity profile.

OAuth clients in use detection

Fixed PF-35407

Fixed a defect with In Use detection when DynamoDB is used for OAuth client storage.

OIDC policy DELETE request timeout

Fixed PF-35357

Fixed a defect where deleting an OIDC Policy fails when using DynamoDB storage for a large number of OAuth clients.

Active Directory binary attribute caused thread proliferation

Fixed PF-35142

Fixed a defect that caused LDAP data source connection pools to close when still in use after the LDAP data source is modified and replicating under heavy load.

JWKS algorithm parameter not populated after processing shared keys from cluster

Fixed PF-35309

Fixed a defect that caused the `alg` parameter to fail to populate when EC dynamic keys are rotated on a lead cluster node and shared to the cluster.

Upgraded Jetty Library

Improved PF-35184

Upgraded the Jetty library to version 9.4.54.v20240208.

Lightning LDAP library

Improved PF-35310

Upgraded the lightning LDAP library to version 1.5.22.

PingFederate 11.3.5 (February 2024)

Resolved issues

Rest datastore security vulnerability

Security PF-34720

Fixed a JSON injection vulnerability in REST datastores described in security advisory SECADV044.

Runtime nodes security vulnerability

Security PF-34896

Fixed a path traversal vulnerability in Runtime nodes described in security advisory SECADV044.

OpenID Connect policy management editor security vulnerability

Security PF-35081

Fixed a Cross-Site Scripting vulnerability in the OpenID Connect Policy Management Editor described in security advisory SECADV044.

GET SAML request signature processing error

Fixed PF-34641

Fixed a defect where SAML request using HTTP GET method with multiple signature-related parameters encoded in the *RelayState* parameter were causing errors in processing signature validation.

NPE notification error

Fixed PF-34813

Fixed a defect that caused PingFederate to issue null pointer exception (NPE) errors when querying the token endpoint.

Reencyption causes connection or client to fail on engine

Fixed PF-34409

Fixed a defect where changes made on the administrative console were not replicated to the engine during reencryption.

JMX registration failure for imported archives

Fixed PF-34796

Fixed a defect that caused the JMX monitoring to fail to register archive files that are imported to PingFederate.

Content type changes if `well_known` endpoint response is too large

Fixed PF-34865

Fixed a defect that caused the `content-type` of a response from the `well_known` endpoint to change from JSON to HTML if a response is too large.

RHEL 8 using OS-level FIPS causes PingFederate failure

Fixed PF-34879

Fixed a defect that caused PingFederate to fail on startup when installed on a Red Hat Enterprise Linux (RHEL) server with OS-levels FIPS enabled.

Unable to deobfuscate grant attributes

Fixed PF-34839

Fixed a defect where PingFederate was unable to deobfuscate grant attributes of a certain length.

Valid Authorization policy generates "Configuration Error" message

Fixed PF-34853

Fixed a defect that caused PingFederate to incorrectly return an "Invalid Configuration" error for a valid authentication policy.

PingFederate 11.3.4 (December 2023)

Resolved issues

Fixed JDK8 cluster node issue

Fixed PF-34837

Fixed an issue where nodes were not able to join a cluster when running with JDK8.

PingFederate 11.3.3 (November 2023)

Resolved issues

Improved client authentication security

Security PF-34645

Fixed a potential security vulnerability described in security advisory SECADV040.

Added support for partitioned cookies

New PF-34440

PingFederate now supports using the `Partitioned` attribute to address third-party cookie issues with the iframe-based login widgets in Google Chrome.

Fixed `/idp/startSLO.ping` `404` caused by virtual issuer configuration

Fixed PF-34322

Fixed an issue that was returning a `404` error if the `/idp/startSLO.ping` endpoint was hit while a virtual issuer was configured. You can now configure virtual issuers with a context path.

Client JWKS now sets properly when using DynamoDB storage

Fixed PF-34504

Clients that maintain a JWKS endpoint can now use private key JWT based authentication when requesting an access token.

Fixed NPE when checking an existing persistent grant that is expired with DynamoDB

Fixed PF-34606

Checking for existing but expired grants with DynamoDB no longer causes a null pointer exception error (NPE).

Connections close after getting a `401` or `403` from PingOne API

Fixed PF-34545

Fixed an issue preventing PingFederate from closing connections after receiving a `401` or `403` response from PingOne MFA.

Outbound provisioning performance improvement

Fixed PF-33466

You can now turn off server-side sorting for LDAP requests related to outbound provisioning, which can improve performance in some environments.

Configure this option using the `ProvisionWithServerSort` parameter in the `com.pingidentity.common.util.ldap.LDAPUtil.xml` file.

Unable to copy and paste policy contract in specific situations

Fixed PF-34433

You can now copy and paste a policy contract below a selector node.

XML decryption failing with `KeyName` element

Fixed PF-34536

Fixed an issue where decryption of an encrypted SAML element could fail if a `KeyName` was specified.

Resolved a vulnerability in the Initial Setup Wizard

Security PF-34646

Fixed a Server-Side Request Forgery vulnerability in the Initial Setup Wizard described in security advisory SECADV041.

Certificate in-use detection slowdown

Fixed PF-34077

We fixed a defect that caused PingFederate to check every certificate when loading certificate-related pages in the administrative interface, which slowed down performance.

Upgraded third-party libraries

Improved

- Upgraded Jetty to version 9.4.53.v20231009.
- Upgraded JGroups to version 4.2.24.Final.

PingFederate 11.3.2 (September 2023)

New features and enhancements

Authenticating to Azure SQL Managed Instance through Azure Active Directory

Improved

Now PingFederate supports authentication to Azure SQL Managed Instance through Azure Active Directory without a username and password. For more information, see Configuring a JDBC connection.

Jetty library upgrade

Improved

We upgraded the Jetty library to 9.4.52.v20230823.

Resolved issues

One-time link in password-reset email messages

Fixed PF-33983

When using redirectless mode, now the one-time link (OTL) in password-reset email messages returns users to the authentication API application configured for the policy, rather than to PingFederate.

Incorrect error template when using service provider authentication policies

Fixed PF-34111

When a service provider (SP) authentication policy fails, PingFederate now renders the `sp.sso.error.page.template.html` page instead of the `idp.sso.error.page.template.html` page.

Updating OAuth clients with dynamic client registration

Fixed PF-34146

Fixed a defect where an OAuth client created with dynamic client registration (DCR) couldn't be updated with DCR after it was modified with the administrative console.

Idle JDBC datastore connections

Fixed PF-34163

Now PingFederate closes idle JDBC datastore connections until the minimum pool size is reached instead of closing and recreating all of them.

The `id_token_jti` property in token endpoint responses

Fixed PF-34210

The `id_token_jti` property is no longer included in token endpoint responses.

*Administrative API defect when fragment rules have **Default to Success** disabled*

Fixed PF-34216

Fixed an administrative API defect when a fragment rule had **Default to Success** disabled

Email notifications for licensing events even when disabled

Fixed PF-34225

Resolved an issue that caused PingFederate to send email notifications for licensing events even though they were disabled in the **Runtime Notifications** configuration.

PingFederate 11.3.1 (August 2023)

New features and enhancements

Configuration retrieval on engine start up

Improved PF-33667

We introduced new settings in the `cluster-config-replication.conf` file to improve configuration retrieval reliability during engine startup. By setting *publish.replication.data.on.startup* to `true`, the administrative console automatically publishes the last replicated configuration upon startup, eliminating the need to initiate replication through the administrative UI or API after a console restart. Additionally, you can configure engines to fail startup if they cannot retrieve configuration data by setting *require.replication.data.on.startup* to `true`. This setting proves beneficial in DevOps deployments, where fresh engine nodes are frequently created without any initial configuration. For more information, see the *publish.replication.data.on.startup* and *require.replication.data.on.startup* property descriptions in Cluster management.

Resolved issues

Jetty library upgrade

Fixed PF-31865

We upgraded the Jetty library, resolving CVE-2022-2047 and CVE-2022-2048.

OAuth scope names

Fixed PF-33056

Using `submit` and `onSubmit` as OAuth scope names in the administrative UI drop-down no longer causes front-end JavaScript errors.

Policy fragment validation error

Fixed PF-33156

Policy fragments with valid authentication sources no longer fail with an Invalid Configuration error during runtime.

Eliminating redundant group updates

Fixed PF-33441

PingFederate, when configured with PingDirectory as an outbound provisioning data source, no longer sends redundant group updates in each provisioning cycle when the entry remains unchanged.

Potential security vulnerability

Fixed PF-33449

We've resolved a potential security vulnerability that is described in security advisory SECADV037.

PingFederate as a Windows service

Fixed PF-33450

We fixed an issue so that PingFederate as a Windows service now runs on Java 17. When updating to the latest maintenance release using an in-place update method (for example, from 11.3.0 to 11.3.x), in addition to the steps in Updating to the latest maintenance release, you must remove the existing PingFederate Windows service. After removal, re-install the PingFederate Windows Service to apply this fix.

Authentication policy fail path

Fixed PF-33519

When an OIDC identity provider (IdP) connection fails in an authentication policy, PingFederate now continues on to the fail path of the authentication policy.

Fragment mapping validation error

Fixed PF-33722

We resolved an issue that incorrectly produced an administrative API validation error when the fragment mapping references `context.RequestedUser` as the mapping source.

Authorization details within a RAR

Fixed PF-33863

PingFederate now processes authorization details within a rich authorization request (RAR) as a JSON Array in a JWT request. Additionally, PingFederate no longer supports authorization details sent as stringified JSON arrays.

Cluster engine nodes starting without replication data

Fixed PF-33881

Resolved a replication issue that, in rare cases, caused an engine node in a cluster to start without replication data from other nodes.

Server error when revoking user sessions

Fixed PF-33920

Resolved an issue that prevented user sessions from being revoked through the session management API when using persistent sessions.

Potential security vulnerability

Fixed PF-33935

We've resolved a potential security vulnerability that is described in security advisory SECADV037.

Fragment mapping validation errors

Fixed PF-33957

When utilizing the PingFederate administrative API to create or update a fragment that includes another fragment, the API will no longer produce a validation error when fragment mapping involves an input source type.

Updated template variable

Fixed PF-34016

The `message-template-end-user-password-change.html` template now contains the *USERNAME* variable.

Potential security vulnerability

Fixed PF-34017

We've resolved a potential security vulnerability that is described in security advisory SECADV037.

Policy evaluation issue

Fixed PF-34051

We fixed a policy evaluation issue that occurred when `ui_locales` was present in an authentication request.

Certificate import improvements

Fixed PF-34074

We updated the administrative UI to include certification serial number in the drop-down, thus preventing import errors for certifications sharing the same Subject DN and expiration date combination.

DynamoDB attribute lookup error

Fixed PF-34099

We fixed an attribute lookup error that occurred when different DynamoDB attributes shared an overlapping path.

PingFederate 11.3 (June 2023)

New features and improvements in PingFederate 11.3.

New features and enhancements

Support for `nbf` and `iat` claims in JWT access token managers

New

Now you can configure access token managers to include the JSON web token (JWT) `access_token` claims `nbf` (not before) and `iat` (issued at). This enables stronger validations by receiving clients or protected resources that process that access_token. For more information, go to Configuring an access token management instance, and in the *JSON web token data model* section click the *JSON token management* tab.

Retries for client-side LDAP errors

New

To further improve reliability and robustness, now PingFederate executes retries rather than failover only. PingFederate initiates a single retry if a request fails and it appears the connection has become invalid. For more information, see the **Retry Failed Operations** field in Setting advanced LDAP options.

Referencing incoming PAR parameters in authentication policies

New

For authorization requests, parameters can now be referenced for incoming PAR requests (pushed authorization requests) inside authentication policies. This lets PingFederate process incoming requests independently of how it received them. For more information, see Pushed authorization requests endpoint.

Unique identifiers for PingFederate transactions

New

To improve logging, PingFederate now uses a `transactionId`. For each transaction, this value won't change between the initial request and the final response. This is especially useful for troubleshooting. For more information, see the `transactionid` field in Security audit logging.

All user attributes available to HTML and mail templates

New

Now you can configure HTML and mail templates with user details. With these details, you can personalize user facing pages and include messages, such as greetings by name, or email addresses that were used for a password recovery flow. The attributes are documented in the templates.

Logging certificate expiration advance warnings

New

Previously, PingFederate produced notifications to inform administrators about expiring certificates. Now you can configure PingFederate to log upcoming expirations without producing notifications. For more information, see Configuring runtime notifications.

Improved European Union compliance with SAML 2.0

New

Two major SAML 2.0 messaging improvements align PingFederate closer to EU regulations:

- Now PingFederate can decrypt `EncryptedID` elements included as SAML attributes. They no longer must be enclosed as an `EncryptedAttribute`. For more information, see Specifying XML encryption policy (for SAML 2.0).
- To enhance signing capabilities, PingFederate now also supports some of the RSASSA-PSS algorithms. For more information, see Signing algorithms.

Support for credential-protected forward proxy servers

New

Because proxy servers can require credentials for authentication purposes, now you can configure PingFederate with proxy server credentials so that connections can be easily established and secured. For more information, see Configuring forward proxy server settings.

Amazon DynamoDB for attribute source lookups

New

Our continued effort to support Amazon DynamoDB (NoSQL) now lets you use DynamoDB as a source for attribute lookups. The connector supports the DynamoDB query language so you can easily configure it. For more information, see Configuring an AWS DynamoDB datastore.

OAuth 2.0 DPoP

New

As regulations for APIs in the context of financial services tighten, it's important to support highly secure API authentication and authorization methods. OAuth DPoP (Demonstrating Proof-of-Possession) is an extension to the OAuth framework and specifies how OAuth tokens are bound to clients. Clients must digitally prove the ownership of these tokens at runtime, which prevents unauthorized clients from misusing them. This extension is useful for any OAuth scenario, not only in financial environments. For more information, see Configuring authorization server settings.

Logging the TLS version that clients use

New

For TLS connections, PingFederate can now log the TLS version that clients use. This gives you an easy way to identify clients that might need updates to use newer versions. For more information, see the tlsversion field in Security audit logging.

Certificate expiration dates added to certificate menus

New

In the administrative console, now certificate selection menus show the distinguished name (DN) and expiration date for each certificate, rather than a serial number. This gives you easy access to relevant information.

New JWT Token Processor

New

A new JWT token processor enhances the token exchange capabilities so that you can leverage any configured issuer. Now PingFederate can validate and accept incoming tokens that were created by pre-configured issuers. For more information, see Configuring a JWT Token Processor 2.0 instance.

Enhanced authentication policies

New

Complex authentication policies are sometimes challenging to manage. To simplify your work and add flexibility to policies, PingFederate provides several policy enhancements:

- Now the Requested AuthN Context Authentication Selector can determine the authentication context for flows. For more information, see Configuring the Requested AuthN Context Authentication Selector.
- Now you can use Context and Extended Properties for attribute sources when mapping authentication policy contracts and local identity profiles. For more information, see Configuring contract mapping, Configuring local identity mapping, and Defining issuance criteria for contract or local identity mapping.
- Now you can use the Scope and Virtual Server ID attributes for authentication sources in policy rules. For more information, see Scope and Virtual Server ID in Configuring rules in authentication policies.
- Now you can use OGNL expressions to configure more complex policy rules. For more information, see Expression in Configuring rules in authentication policies.

PAR support for OIDC IdP connections and OIDC admin authentication

New

PingFederate now initiates outbound authorization requests using the PAR endpoint of the target authorization server if you expose it. This enhancement lets PingFederate use PAR inbound and outbound, which improves OAuth flow security. For more information, see the **Pushed Authorization Request Endpoint** field in Configuring OpenID Provider information.

Support for OpenID Connect back-channel logout

New

In the context of OpenID session management, PingFederate now supports back-channel logout. PingFederate supports this feature whether it's configured as an OpenID Connect provider (OP) or a relying party (RP). For more information, see the OpenID Connect Back-Channel Logout 1.0 specification.

Ability to include x5t and typ in ID token headers

New

Now PingFederate can include JWT header values `x5t` and `typ` in the ID tokens it issues. You can include the `x5t` header with static keys enabled, whereas you can configure the `typ` header to an appropriate value without a dependency on the types of keys. The `x5t` header adds another mechanism for verifying the validity of a received JWT. For information about the `x5t` and `typ` parameters, see the JSON web key (JWK) and JWT specifications, respectively, and steps 9 and 10 in Configuring policy and ID token settings.

Support for the alg parameter response for JWKS keys

New

The `alg` header is now supported in PingFederate's JWKS endpoint. Any elliptic curve keys and all RSA-256 based keys expose this header. This feature lets clients verify that a received JWT has been signed by the advertised algorithm. For information about the `alg` parameter, see the JWK specification and JSON Web Keys endpoint.

Support for client_secret_jwt as client authentication

New

With the client_secret_jwt authentication method, a client can choose to create a signed JWT when authenticating against PingFederate's token endpoint, introspection endpoint, PAR endpoint, or CIBA endpoint instead of providing the client secret. This feature prevents potential client secret leakage because it's not actively exchanged with any party. PingFederate also supports this feature when it acts as an RP. For more information, see client_secret_jwt in the Open ID Connect specification and Client authentication schemes.

Refresh token reuse and revocation best practice

New

PingFederate now revokes a chain of tokens if a refresh token is revoked or if a refresh token is reused. This includes derived authorization codes and access tokens. For more information, see the Refresh Token settings section of Configuring authorization server settings.

Overriding configuration settings using environment variables

New

Now you can configure many properties as environment variables instead of setting them in properties files. This is especially important for container environments, which is common practice.

Auditing enhancements

New

Several enhancements provide more details in PingFederate generated logs. These include the logging of JWT IDs (jti), hashed values of authorization codes, access tokens, and refresh tokens. Also, PingFederate now logs which system has locked out users after multiple, unsuccessful login attempts, so you'll know if it was PingFederate or an LDAP server. PingFederate also adds more details to the administrative API logs, so now there are almost no differences between logs generated when using the administrative console or administrative API. For more information, see Administrator audit logging, Administrative API audit log, and Security audit logging.

Amazon DynamoDB and OAuth client records

New

Now you can manage OAuth clients in Amazon DynamoDB. With this update, you can use DynamoDB to manage OAuth clients, persistent grants, and persistent authorization sessions. Learn more in Configuring an Amazon DynamoDB for client storage.

Upgraded Velocity Engine 2.3

New

PingFederate now supports Apache Velocity Engine 2.3. For more information, see Upgrading in the Apache Velocity Engine documentation.

Support for strict content security policy (CSP) for HTML templates

New

Now you can include CSP policies for HTML templates without having to implement workarounds. For more information, see Customizable user-facing pages.

Ability to use additional Velocity tools

New

Now you can use Velocity templates with more tools, such as cookieTool.

Support for Microsoft Azure SQL Managed Instance

New

PingFederate now supports Microsoft Azure SQL Managed Instance. For more information, see the Datastore integration table in System requirements, and for more information on how to configure a connection to Microsoft Azure SQL Managed Instance, see Configuring a JDBC connection.

mTLS authentication for REST API datastores

New

PingFederate now supports mutual TLS (mTLS) client authentication for REST API datastores.

mTLS authentication for LDAP datastores

New

PingFederate now supports mTLS client authentication for LDAP datastores.

Entrust nShield Connect HSM and Java 11

New

Now when you integrate an Entrust nShield hardware security module (HSM) with PingFederate, you can use Java 11.

Bundled User Count Utility

New

We added the User Count Utility (UCU) as a bundled component. You can use the UCU to produce unique and active user counts in a PingFederate environment.

Upgraded third-party components

New

We upgraded the following third-party components:

- Upgraded Spring Framework to 5.3.27
- Upgraded jose4j to 0.9.3

Resolved issues

SAML login session tracking

Fixed PF-33168

We improved SP-Initiated SAML login session tracking. This security improvement can affect existing SAML SP connections that rely on multiple session states in a single transaction.

For more information about how your configuration can be affected, and the steps to resolve issues, see Solicited SAML Response Validation in the Ping Identity Support Portal.

Log message when multiple entries match the LDAP PCV search filter

Fixed PF-32427

Now when multiple entries match the LDAP PCV search filter, the following message appears in the log at DEBUG level: `error code 4 - This search operation has sent the maximum of 1 entries to the client`

Multivalued authorization request parameters

Fixed PF-32783

Now multivalued request parameters work as expected in authorization requests for OIDC administrative console authentication.

Tracked parameters in the LDAP search filter when using the administrative API

Fixed PF-32914

Now you can use tracked parameters in the Attribute Sources and User Lookup LDAP search filter when using the administrative API.

Showing and hiding passwords being entered

Fixed PF-33059

Now all password entry fields in PingFederate templates have icons that let users show and hide the password they're entering.

Connections and OAuth clients referencing deleted extended properties

Fixed PF-33311

When a connection or OAuth client references a deleted extended property, PingFederate no longer throws a null pointer exception. Instead it ignores the extended property and logs an error.

Slow log consumption affects performance

Fixed PF-33368

We've fixed a defect that caused performance issues for PingFederate when third-party logging services were slow to consume logging events.

Custom error messages from external consent adapters

Fixed PF-33151

Now PingFederate can use customized messages from external consent adapters in error responses.

Restricting password credential validators

Fixed PF-33487

When `restrictToDefaultAccessTokenManager` is enabled on an OAuth client, the client can only get access tokens when being validated by password credential validators that are mapped to the restricted access token manager.

Bypass Authorization Approval and prompt parameters

Fixed PF-33598

When an OAuth client has Bypass Authorization Approval enabled, now that setting takes precedence over the `prompt` parameter in requests.

Document file permissions

Fixed PF-33605

Updated the file permissions of legal documents.

The `memoryoptions` script allocates excessive JVM heap

Fixed PF-33610

The `memoryoptions` script no longer allocates excessive JVM heap on Windows systems.

Authorization Code and Device Authorization grant handling

Fixed PF-33622

For the Device Authorization grant type, if **Check Activation Code** is set to **Before Authentication**, then authorization detail is set in the input parameters map when `IdpAuthenticationAdapterV2` in the SDK is invoked.

Converting the values of binary attributes from PingOne LDAP gateway datastores

Fixed PF-33637

Now when PingFederate retrieves a binary attribute from a PingOne LDAP gateway datastore, it correctly converts the attribute value to the specified format (base64, SID, hex).

Unexpected certificate usage

Fixed PF-33709

When more than one trusted CA matches the issuer DN of an OAuth client, now PingFederate only flags the trusted CA as in use if its certificate hasn't expired and its subject DN matches the client's configured issuer DN.

Potential information disclosure vulnerability

Fixed PF-33867

Removed a potential information disclosure vulnerability.

Jetty unable to serve gzip precompressed resources

Fixed PF-33869

Now PingFederate allows Jetty to precompress resources such as images and CSS.

Returning `400` error instead of a `500` error

Fixed PF-30236

When a system-level issue causes a data source attribute lookup to fail during OAuth flows, if the `<pf_install>/pingfederate/server/default/data/config-store/org.sourceid.saml20.domain.AttributeMapping.xml` file's `AbortOnAttrLookupFailure` attribute is set to `true`, now PingFederate returns a `500` error instead of a `400` error.

Usercount Utility's aggregate command

Fixed PF-32757

When you run the Usercount Utility's aggregate command:

- If all `.ucu` files contain tracking IDs, the utility generates a user count for each event, like before.
- If no `.ucu` files contain tracking IDs, now the utility generates a user count for each application.
- If some `.ucu` files contain tracking ids but others don't:
  - for the files without tracking IDs, now the utility generates a user count for each application.
  - for the files with tracking IDs, now the utility generates a user count for each event.

CPU load displayed as N/A

Fixed PF-32837

Now when the CPU load is 0, heartbeat pages display the value with digits instead of as "N/A".

Unexpected carriage return in audit logs

Fixed PF-32989

We resolved an issue that caused an unexpected carriage return in audit logs during SP-initiated single sign-on (SSO) if an identity provider responded with a non-success status.

Known issues and limitations

PingID password credential validator with integrated RADIUS server

Issue

PingFederate versions 11.1.4, 11.1.5, 11.2.1, and 11.2.2 contain version 3.0.2 of the PingID password credential validator (PCV). That version of the PCV has known issues that you should review before upgrading. For more information, see Known issues in PingID RADIUS PCV 3.0.2.

Administrative console and administrative API

Issue

- Although PingFederate 11.3 and later support DPoP, a known limitation is that the following features don't support DPoP when PingFederate is the RP:
  - The administrative console authentication scheme using OIDC
  - The administrative API authentication scheme using OAuth 2.0
- /bulk: Only resource types currently supported by the administrative API are included in the exported data. We don't intend to introduce administrative API support to the following areas:
  - SAML 2.0 IdP Discovery
  - SAML 2.0 SP Affiliation
  - SMS Provider
- Previously, the administrative API did not accurately reflect a **Persistent Grant Max Lifetime** setting of 29 days (or shorter) with the selection of the **Grants Do Not Timeout Due To Inactivity** option. As a result, if you have configured such OAuth

authorization server settings and have generated a bulk export in version 10.0 through 10.0.2, we recommend that you re-generate a new bulk export after upgrading to version 10.0.3 (or a more recent version). The newly exported data does not contain the aforementioned flaw, and you can safely import it to version 10.0.3 (or a more recent version).

- When enabling mTLS certificate-based authentication, administrators often configure a list of acceptable client certificate issuers. When you use a browser to access the console or the administrative API documentation, PingFederate returns to the browser the list of acceptable issuers as part of the TLS handshake. If the browser's client certificate store contains multiple client certificates, the browser often presents you only the certificates whose issuer matches one of the acceptable issuers. However, when PingFederate runs in a Java 11 environment, Chrome presents you all its configured client certificates, regardless of whether the issuer matches one of the acceptable issuers or not.
- When using mTLS authentication to authenticate to an LDAP server for administrative console or administrative API access, PingFederate doesn't support using a Microsoft Active Directory server.
- Prior to toggling the status of a connection with the administrative API, you must ensure that any expired certificates or no longer available attributes are replaced with valid certificates or attributes; otherwise, the update request fails.
- When creating or updating a child instance of a hierarchical plugin, the administrative API retains objects with an `"inherited": false` name/value pair (or without such name/value pair altogether), ignores those with a value of `true`, and returns a 200 HTTP status code. No error messages are returned for the ignored objects.
- Using the browser's navigation mechanisms (for example, the **Back** button) causes inconsistent behavior in the administrative console. Use the navigation buttons provided at the bottom of windows in the PingFederate console.
- Using the PingFederate console in multiple tabs on one browser might cause inconsistent behavior which could corrupt its configuration.
- If authenticated to the PingFederate administrative console using certificate authentication, a session that has timed out might 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 sign-on page, and then back to the administrative console after authentication is complete.

Similar behavior applies for certificate authentication, in principle. However, because the browser might automatically resubmit the certificate for authentication, the browser might redirect to the administrative console and not the sign on page.

PingOne MFA CIBA Authenticator

Issue PingOne MFA

PingFederate 11.3 is not compatible with the PingOne MFA CIBA Authenticator bundled in PingOne MFA Integration Kit version 2.1 and earlier. This issue was resolved in version 2.2 of that integration kit.

TLSv1.3

Issue

For Java versions that don't support TLSv1.3 (meaning versions earlier than 8u261), PingFederate fails on start up with a `NoSuchAlgorithmException` exception. To resolve this error, remove `TLSv1.3` from the following settings in the `run.properties` file:

- **`pf.tls.client.protocols`**
- **`pf.tls.runtime.server.protocols`**
- **`pf.tls.admin.server.protocols`**

TLS cipher suite customization

Issue

PingFederate's TLS cipher suites can be customized by modifying `com.pingidentity.crypto.SunJCEManager.xml` (or a similarly-named file if BCFIPS or an HSM is configured). After updating the file and replicating, all cluster nodes must be restarted for the change to take effect.

Java

Issue

- As of PingFederate 11.1, BC-FIPS and HSMs are not supported when using Java 17.

- Updating Java version 8 to version 11 results in an error when PingFederate is already installed and running on Windows. To work around this issue, uninstall and reinstall the PingFederate Windows service by running the `UninstallPingFederateService.bat` and `InstallPingFederateService.bat` files located in `<pf_install>/pingfederate/sbin/wrapper`.

HSMs

Issue

AWS CloudHSM

- It is not possible to use an elliptic curve (EC) certificate as an SSL server certificate.
- TLS 1.3 is not currently supported.

Thales HSMs

- JWT token decryption using ECDH-ES may fail. This issue only arises if PingFederate is configured with static OAuth and OpenID Connect keys, a static key is stored on the HSM, and PingFederate is consuming a token encrypted with this key.
- It is not possible to use an EC certificate as an SSL server certificate.
- TLS 1.3 is not currently supported.

Entrust HSMs

- JWT token decryption using ECDH-ES may fail. This issue only arises if PingFederate is configured with static OAuth and OpenID Connect keys, a static key is stored on the HSM, and PingFederate is consuming a token encrypted with this key.
- It is not possible to import a PKCS12- or PEM-formatted EC certificate.
- It is not possible to use an EC certificate as an SSL server certificate.
- TLS 1.3 is not currently supported.

SSO and SLO

Issue

- When consuming SAML metadata, PingFederate does not report an error when neither the `validUntil` nor the `cacheDuration` attribute is included in the metadata. Note that PingFederate does reject expired SAML metadata as indicated by the `validUntil` attribute value, if it is provided.
- The anchored-certificate trust model cannot be used with the Single log off (SLO) redirect binding because the certificate cannot be included with the logout request.
- 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.

Composite Adapter configuration

Issue

SLO is not supported when users are authenticated through a Composite Adapter instance that contains another instance of the Composite Adapter.

Self-service password reset

Issue

Passwords can be reset for Microsoft Active Directory user accounts without the permission to change password.

OAuth

Issue

PingFederate does not support a case-sensitive naming convention for OAuth client ID values when client records are stored in a directory server. For example, after creating a client with an ID value of `sampleClient`, PingFederate does not allow the creation of another client with an ID value of `SampleClient`.

Although it's possible to create clients using the same ID values with different casings when client records are stored in XML files, a database server, or custom storage, we recommend not doing so to avoid potential record migration issues.

Customer identity and access management

Issue

Some browsers display a date-picker user interface for fields that have been designed for date-specific inputs. Some browsers do not. If one or more date-specific fields are defined on the registration page or the profile management page (or both), end users must enter the dates manually if their browsers do not display a date-picker user interface for those fields.

Provisioning

Issue

- 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.
- The `totalResults` value in SCIM responses indicates the number of results returned in the current response, not the total number of estimated results on the LDAP server.

Logging

Issue

- 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, the `USER_KEY` attribute will not be masked in the server logs. Other persistent grant attributes will be masked.
- Even if a source attribute has been configured for masking in an IdP adapter and the source attribute is mapped as the adapter's unique user key, the user key attribute is not masked in the server or audit logs.

Database logging

Issue

- 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, the `USER_KEY` attribute will not be masked in the server logs. Other persistent grant attributes will be masked.

- Even if a source attribute has been configured for masking in an IdP adapter and the source attribute is mapped as the adapter's unique user key, the user key attribute is not masked in the server or audit logs.

RADIUS NAS-IP-Address

Issue

The RADIUS NAS-IP-Address is only included in Access-Request packets when the `pf.bind.engine.address` is set with an IPv4 address. IPv6 is not supported.

Amazon SNS Notification Publisher

Issue

When deploying PingFederate with a forward proxy, plugins based on the AWS SDK, such as the Amazon SNS Notification Publisher, will only honor the `http.proxyHost`, `http.proxyPort`, `http.proxyUser`, and `http.proxyPassword` properties in `run.properties`. The plugin will rely on these properties even if the service URL is `https`.

PingOne Fraud integration kit

Info PingOne Fraud

The PingOne Fraud integration kit is no longer bundled with PingFederate.

Deprecated features

Microsoft Internet Explorer 11

Info

Ping Identity commits to deliver the best experience for administrators and users. As we continue to improve our products, we encourage you to migrate off of Microsoft Internet Explorer 11. Starting with PingFederate 11.0, Internet Explorer 11 is no longer included in

the PingFederate qualification process for administrators or users. For a list of supported browsers, see System requirements.

Configcopy tool, Connection Management Service, SSO Directory Service

Info

As of PingFederate 10.2, these features have been deprecated and will be removed in a future release.

Oracle Directory Server Enterprise Edition

Info

As Oracle ended its Premier Support for Oracle Directory Server Enterprise Edition (ODSEE 11g) in December 2019, we no longer include ODSEE as part of the PingFederate qualification process (starting with PingFederate 10.2). We continue to qualify against Oracle Unified Directory and other supported directory servers. For a full list, see System requirements.

SNMP

Info

Starting with PingFederate 10.2, monitoring and reporting through the SNMP has been removed.

Roles and protocols

Info

Starting with PingFederate 10.1, roles and protocols are always enabled and no longer configurable through the administrative console and API.

S3_PING discovery protocol

Info

Starting with PingFederate 10.1, the S3_PING discovery protocol has been deprecated. Customers running on AWS infrastructure should instead use NATIVE_S3_PING.

Red Hat Enterprise Linux install script

Info

Starting with PingFederate 10.0, the Red Hat Enterprise Linux install script is no longer available. To install PingFederate 10.0 for Linux, you must download and extract the product distribution `.zip` file.

PingFederate 11.2.11 (December 2024)

Resolved issues

Cross-site scripting

Security PF-36304 PF-36311 PF-36313

We've fixed a security vulnerability where PingFederate accepted cross-site scripting inputs.

Email verification failure after registration workflow

Fixed PF-36574

We've fixed a defect that caused the email verification screen to fail to appear when a user registered through an authentication source.

PingFederate 11.2.10 (July 2024)

Resolved issues

OAuth client only validates one access token manager when aud parameter included

Fixed PF-35737

Fixed a defect that caused PingFederate to validate only the first OAuth client access token manager it found when **Validate Against All Eligible Access Token Managers** was checked, and the `aud` parameter was included in the request.

Wrong content-type for autopost template form

Fixed PF-35784

Fixed a defect that caused PingFederate to send the wrong content-type value for `form.autopost.template.html` requests, which caused the page to render as JSON rather than the formatted form.

PingFederate 11.2.9 (April 2024)

Resolved issues

Rest datastore security vulnerability

Security PF-34720

Fixed a JSON injection vulnerability in REST datastores described in security advisory SECADV044.

Runtime nodes security vulnerability

Security PF-34896

Fixed a path traversal vulnerability in Runtime nodes described in security advisory SECADV044.

OpenID Connect policy management editor security vulnerability

Security PF-35081

Fixed a Cross-Site Scripting vulnerability in the OpenID Connect Policy Management Editor described in security advisory SECADV044.

Slow log consumption affects performance

Fixed PF-33368

Fixed a defect that caused performance issues for PingFederate when third-party logging services were slow to consume logging events.

RHEL 8 using OS-level FIPS causes PingFederate failure

Fixed PF-34879

Fixed a defect that caused PingFederate to fail on startup when installed on a Red Hat Enterprise Linux (RHEL) server with OS-levels FIPS enabled.

PingFederate 11.2.8 (December 2023)

New features and enhancements

Configurable option to turn on/off plugin creation and initialization during PingFederate startup.

New PF-34640

Added the *ConfigurePluginsOnStartup* variable to the `config-store` file.

Default value of `true` creates and initializes plugins during startup. `false` prevents creation and initialization of plugins, which can reduce startup time.

Improved OGNL expression logging

Improved PF-34050

The administrator audit log file (`admin.log`) now logs any OGNL expression tests performed and the expression variables used with an event type of `TEST_EXPRESSION`.

For more information, see Administrator audit logging

Resolved issues

Resolved a vulnerability in the Initial Setup Wizard

Security PF-34646

Fixed a Server-Side Request Forgery vulnerability in the Initial Setup Wizard described in security advisory SECADV041.

PingFederate systematically adds server-side sort control

Fixed PF-33466

You can now turn off server-side sorting using a configuration option.

Updating OAuth clients with dynamic client registration

Fixed PF-34146

Fixed a defect where an OAuth client created with dynamic client registration (DCR) couldn't be updated with DCR after it was modified with the administrative console.

Unable to deobfuscate chunked grant value with character length of 682

Fixed PF-34839

Fixed a defect where PingFederate was unable to deobfuscate grant attributes for a small group of users in OAuth flows.

PingFederate 11.2.7 (August 2023)

Resolved issues

Potential security vulnerability

Fixed PF-33449

We've resolved a potential security vulnerability that is described in security advisory SECADV037.

Potential security vulnerability

Fixed PF-34017

We've resolved a potential security vulnerability that is described in security advisory SECADV037.

Policy evaluation issue

Fixed PF-34051

We fixed a policy evaluation issue that occurred when `ui_locales` was present in an authentication request.

PingFederate 11.2.6 (June 2023)

Resolved issues

Policy fragment validation error

Fixed PF-33156

Policy fragments with valid authentication sources no longer fail with an Invalid Configuration error during runtime.

The `memoryoptions` utility allocates excessive JVM heap

Fixed PF-33610

The `memoryoptions` utility no longer allocates excessive JVM heap on Windows systems.

The device authorization grant type and the Check Activation Code setting

Fixed PF-33622

For the device authorization grant type, if **Check Activation Code** is set to **Before Authentication**, now authorization detail is set in the input parameters map when `IdpAuthenticationAdapterV2` in the SDK is invoked.

Binary attributes handled incorrectly when using PingOne LDAP gateway datastores

Fixed PF-33637

Now when PingFederate retrieves a binary attribute from a PingOne LDAP gateway datastore, it correctly converts the attribute value to the specified format (base64, SID, hex).

Jetty unable to precompress resources

Fixed PF-33869

Now PingFederate allows Jetty to precompress resources such as images and CSS.

Cluster engine nodes starting without replication data

Fixed PF-33881

Resolved a replication issue that, in rare cases, caused an engine node in a cluster to start without replication data from other nodes.

Server error when revoking user sessions

Fixed PF-33920

Resolved an issue that prevented user sessions from being revoked through the session management API when using persistent sessions.

PingFederate 11.2.5 (May 2023)

Resolved issues

Logging validation

Fixed PF-32764

We've improved logging validation.

Multi-value request parameters for OIDC for console login

Fixed PF-32783

We fixed an issue where multi-value request parameters were not working as expected when using OIDC for console login.

Preservation of changes to certain validation rules

Fixed PF-33093

We fixed an issue where PingFederate did not preserve changes to certain validation rules in the `http-request-parameter-validation.xml` file upon upgrade.

SAML login session tracking

Fixed PF-33168

We improved SP-Initiated SAML login session tracking. This security improvement can affect existing SAML SP connections that rely on multiple session states in a single transaction.

For more information about how your configuration can be affected, and the steps to resolve issues, see Solicited SAML Response Validation in the Ping Identity Support Portal.

OTL reset page error messaging

Fixed PF-33307

The one-time link (OTL) reset page now displays an error message when the link is expired.

Access token bug fix

Fixed PF-33342

We resolved an issue where an access token may not include the `pi.sri` claim after refresh. This issue only occurs when reuse of existing access grants is enabled.

Attribute retrieval

Fixed PF-33484

In OAuth and OpenID Connect (OIDC) flows, external consent adapters can now retrieve attributes from the chained attributes map.

LDAP bug fix

Fixed PF-33503

We fixed an LDAP issue where new access grant records were not created with new scopes when **Reuse Existing Persistent Access Grants for Grant Types** was enabled.

ID token ACR claim

Fixed PF-33557

We resolved an issue where an ID token would not include the Authentication Context Class Reference (ACR) claim if an old client secret was used during the retention period.

Redundancies in key algorithm generation

Fixed PF-33607

We fixed an issue that affected cluster replication when PingFederate was deployed with AWS CloudHSM. When replication was initiated, engines generated a number of temporary key pairs, and the increased load on the HSM could trigger SSO errors.

PingFederate 11.2.4 (March 2023)

Resolved issues

Base DN reference attribute

Fixed PF-32971

We've fixed an issue where upstream data stores in the chain could not recognize the reference attribute for base distinguished name (DN) during lookup.

Identity store provisioner validation rules

Fixed PF-33017

We've improved validation rules to ensure that only identity store provisioners that support groups require group attribute contract validation.

DCR with client secret retention

Fixed PF-33035

We've resolved a null pointer exception (NPE) error that occurred when attempting to set up Dynamic Client Registration (DCR) with client secret retention.

Response handling logs

Fixed PF-33131

We've added additional logging to help debug unexpected errors in response handling.

OIDC policies with fragments configured

Fixed PF-33158

We've resolved an issue that occurred when saving OpenID Connect (OIDC) policies with fragments configured.

LDAP filter validation

Fixed PF-33173

We've fixed an issue related to LDAP filter validation that arose when accessing the **IdP Connections** page.

HSM key sessions

Fixed PF-33284

We've improved the process of cluster replication for PingFederate integrated with AWS CloudHSM by purging HSM key pair generation sessions.

PingFederate 11.2.3 (February 2023)

Resolved issues

Potential security vulnerability

Fixed PF-32748

We've resolved a potential security vulnerability that is described in security advisory SECADV035.

Log improvements

Fixed PF-33017

In order to reduce re-encryption and file scanning log verbosity, when a configuration is imported or replicated to a cluster, PingFederate no longer scans files in the `etc` directory.

Other improvements

New

- We also updated the following bundled components and third-party dependencies:

- PingID Integration Kit 2.24
- PingID Adapter 2.13.2
- PingID PCV (with integrated RADIUS server) 3.0.3

PingFederate 11.2.2 (February 2023)

Resolved issues

Server log warnings

Fixed PF-33037

We've added a warning to server logs if the *ds-pwp-state-json* attribute is not present in PingDirectory's LDAP Response. This warning appears in the log every time a user interacts with the profile management page. Please enable this attribute to adhere to PingDirectory's security configuration best practices. PingDirectory version 8.1 and later supports this attribute, and customers running older versions are encouraged to upgrade to a supported version as soon as possible.

PingFederate 11.2.1 (February 2023)

Resolved issues

OAuth client management

Fixed PF-32790

When managing OAuth clients, we've resolved a defect where selecting the **Require JWT Secured Authorization Response Mode** text toggled the incorrect checkbox.

Potential security vulnerability

Fixed PF-32805

We've resolved a potential security vulnerability that is described in security advisory SECADV033.

Informing adapters of end policy result

Fixed PF-32890

When processing policy fragments, all adapters invoked in the fragment now correctly execute their respective post-processing step (if applicable) to inform the adapter of the end policy result.

Managing certificates within Metadata Export

Fixed PF-32965

Managing certificates within the **Metadata Export** flow no longer displays or saves an empty list of certificates, clearing out existing ones in the process. For more information, see Metadata export.

Cluster data replication

Fixed PF-32983

We've resolved a defect where cluster data replication could remove keys from engine node's `pf.jwk` file instead of merging and retaining the keys.

Other improvements

New

- We also updated the following bundled components and third-party dependencies:
  - PingID Integration Kit 2.23
  - PingID Adapter 2.13.2
  - PingID PCV (with integrated RADIUS server) 3.0.2

> **Note**
>
> This version of the PingID PCV has known issues that you should review before upgrading. For more information, see Known issues in PingID RADIUS PCV 3.0.2.

PingFederate 11.2 (December 2022)

New features and improvements in PingFederate 11.2.

New features and enhancements

Support for OAuth 2.0 authorization server metadata

New

PingFederate now supports OAuth 2.0 authorization server metadata. This allows OAuth clients to retrieve relevant endpoints and other details about features that PingFederate supports. The API response is like the OpenID Connect Discovery endpoints response but doesn't include OpenID Connect relevant details. This lets you configure endpoints for your particular use case. See OAuth authorization server metadata endpoint.

Support for nested groups and nested search for PingDirectory

New

For outbound provisioning, PingFederate now supports nested groups and nested search for PingDirectory. This lets you freely choose your favorite directory without needing to choose based on the support for nested groups. See nested group and nested search in Specifying a source location.

Exposed `AccessGrantManagerAccessor` as part of the SDK

New

The `AccessGrantManagerAccessor` is now accessible in the PingFederate SDK. This lets developers query existing persistent grants at run time. See `<pf_install>/pingfederate/sdk/doc/com/pingidentity/access/AccessGrantManagerAccessor.html` in the SDK documentation.

Improved the sign-on experience after users change their password

New

Now you can configure PingFederate to keep users signed in after they change their password. This prevents users from having to sign on again after updating their password, improving the user experience. Learn more in the **Require Re-authentication** settings HTML Form Adapter advanced fields.

Administrative API supports multiple authentication and authorization schemes

New

Now you can configure the PingFederate administrative API to accept either OAuth `access_token` or basic authentication. This is especially useful in cases where applications shouldn't include administrator's credentials in API requests. See `pf.admin.api.authentication` in Configuring PingFederate properties.

Support for Google reCAPTCHA v3 and integration with multiple CAPTCHA providers

New

PingFederate now supports Google reCAPTCHA v3. reCAPTCHA v3 produces a score between 0.0 - 1.0 (risky to safe) that you can use in policies to require step-up authentication or other actions. By default, reCAPTCHA v3 doesn't interrupt user journeys, which are in the control of application developers. Learn more in Managing CAPTCHA and risk providers.

PingFederate also now provides an SDK that allows for integrations with custom CAPTCHA providers, which adds great flexibility to the CAPTCHA feature.

Improved cluster replication notification

New

Instead of showing an active bell icon, the administrative console now displays a banner when cluster replication is required. The banner includes a link to the **Cluster Management** window for easy access. See Cluster management.

The administrative console supports OIDC claims parameter

New

You can configure PingFederate to function as an OpenID Connect client and let administrators sign on to the administrative console using their PingOne credentials. PingFederate initiates an OpenID Connect flow that includes the claims parameter. You can also use this feature outside the PingOne environment, leveraging any authorization server that supports the claims parameter. This allows for a simpler, seamless login flow. See Request Parameters in Enabling OIDC-based authentication.

The administrative console supports third party-initiated login

New

You can configure PingFederate to accept incoming parameters, such as `iss`, that are processed and included in an outgoing authorization request if configured to do so. This feature lets administrators sign on to PingFederate from PingOne. This feature also supports other OpenID Connect authorization servers that support incoming parameters. See Request Parameters in Enabling OIDC-based authentication.

PingOne DaVinci integration kit

New

The PingFederate distribution now includes the PingOne DaVinci integration kit. See PingOne DaVinci Adapter in Bundled adapters and authenticators.

Amazon DynamoDB and persistent authentication sessions

New

PingFederate can now manage persistent user sessions in AWS DynamoDB. Persistent user sessions keep sessions active even after a restart of PingFederate. This feature reduces the interruption of user journeys. See *Configuring an Amazon DynamoDB for persistent authentication sessions* in Defining a datastore for persistent authentication sessions.

Enhanced policy rules

New

When defining policy rules, now attributes that were processed in an earlier step can be accessed further down in the policy tree. This feature enhances the management and usability of policies. See Configuring rules in authentication policies.

The heartbeat endpoint and JMX expose more information

New

The data exposed by the heartbeat endpoint and JMX interface now include more details, such as the number of errors per data store. See Liveliness and responsiveness.

Updated the bundled PingOne MFA Adapter

Improved

Updated the bundled PingOne MFA Adapter to the newest version, 2.0. See PingOne MFA Adapter in Bundled adapters and authenticators.

Toggle log verbosity with ease

New

Gone are the days you had to edit the `log4j2.xml` file on multiple servers to enable or disable DEBUG messages in their server logs. Now you can toggle log settings in the administrative console or with the administrative API.

PingFederate provides a set of message categories, each targeting a specific scenario. For example, the **XML Signatures** category helps you troubleshoot XML signature issues. You

can also add your own categories to suit your unique requirements.

Timestamps for clients and connections

New

When viewing lists of OAuth clients and Browser single sign-on (SSO)/security token service (STS) connections, you can now sort them by modification or creation time. The timestamps can also help you understand the history and the relationship between clients and connections.

AWS CloudHSM and Java 11

New

If you integrate with Amazon Web Services (AWS) CloudHSM, now you can choose between Java 8 and Java 11.

OAuth Rich Authorization Requests

New

OAuth rich authorization requests (RAR) provide a standard way for OAuth client applications to specify fine-grained authorization requirements in their requests. For example, when initiating a money transfer, a personal banking application can pass all relevant information to the authorization server via the new parameter `authorization_details`. The authorization server supporting RAR processes the `authorization_details` parameter value accordingly and ultimately returns tokens to the application if the process completes successfully.

RAR is on track to become a requirement in Financial-grade API (FAPI) 2.0. With this new capability, you can confidently build your open banking solutions with PingFederate.

Other enhancements

New

Now you can optionally define a sender name for each SMTP notification publisher instance.

PingFederate now supports XML Encryption 1.1.

Resolved issues

Sorting LDAP and database-related fields

Fixed PF-29355

For LDAP and database-related fields, PingFederate now sorts values alphabetically and in case-insensitive order.

Detailed comments added to log4j2.xml file

Fixed PF-30514

We've added detailed comments to the `log4j2.xml` file to prevent misconfigurations that could lead to service hangs and production outages. Learn more in Log4j 2 logging service and configuration.

Configuration options added to control SAML error responses

Fixed PF-30514

We've added a configuration option to control whether SAML error responses include `Cause`. The new setting is `IncludeErrorCauseInSamlResponse` in `config-store/org.sourceid.saml20.protocol.StatusResponseTypeUtil.xml`. The default value is *true*.

Improved SP STS message customization

Fixed PF-31149

The *#HttpServletRequest* and *#HttpServletResponse* variables are now available in SP STS message customization. Learn more in Message types and available variables.

Connections with multiple protocol types

Fixed PF-31531

We've resolved an issue where connections with multiple protocol types would only filter on a single protocol type.

OpenID Connect (OIDC) for administrative console authentication

Fixed PF-31717

When using OIDC for administrative console authentication, PingFederate no longer throws an NPE if `private_key_jwt` is used for client authentication method and the `client.secret` property is not set.

Improvements to refresh token rolling criteria

Fixed PF-31761

We've introduced a new separate stored value to track when refresh tokens should be reissued to OAuth clients, resolving a defect where rolling refresh tokens read the incorrect update timestamp to determine refresh token rolling criteria. Learn more in Configuring authorization server settings.

Store clients with special characters

Fixed PF-31786

When adding clients to Active Directory (AD) or other LDAP stores, PingFederate now automatically escapes reserved characters from clientIDs.

Improved detection around invalid Group DN

Fixed PF-31791

We've improved detection around invalid Group distinguished names (DN) and added exceptions in the provisioner log. For more information on Group DN, see Specifying a source location.

Updates to the SameSite=None header attribute supported browsers list

Fixed PF-31806

We've updated the supported browsers list for the `SameSite=None` header attribute to filter out problematic clients with the `SameSite` cookie attribute bug: Safari version 12 and Embedded Apple Webkit Browser Safari 12 on macOS.

Expired user sessions and session log out

Fixed PF-31807

PingFederate's administrative console now identifies expired user sessions on timeout and properly removes the session regardless of user interaction.

Policy and fragment logging

Fixed PF-31862

PingFederate now logs the policy and fragment name before fragment processing.

Bulk import for IdP connections

Fixed PF-31870

Resolved an issue where bulk import fails for identity provider (IdP) connections that fulfill Persistent Grant Extended Attributes.

Template double-submission

Fixed PF-31957

PingFederate templates no longer allow double-submission.

Connection failures on external LDAP authentication login

Fixed PF-32001

PingFederate now recovers from initial connection failure when logging into the administrative console using external LDAP authentication.

Hiding user information from authentication API responses

Fixed PF-32028

You can now configure the `IncludeUserInfoInResponses` setting in the `<install dir>/server/default/data/config-store/org.sourceid.saml20.domain.mgmt.impl.AuthnApiManagerImpl.xml` file to hide user information from authentication API responses.

Errors on policy fragments configured to handle failures locally

Fixed PF-32073

When an error occurs on policies containing fragments and configured to handle failures locally, PingFederate no longer redirects a user to the service provider (SP) error page on SP-initiated SSO.

Password management

Fixed PF-32081

We've resolved an issue around password requirements messaging during password management.

Updated description text on Import Connections page

Fixed PF-32088

We've updated the description text on the import IdP/SP connection page to indicate that PingFederate only performs minimal validation for imported connections. We suggest using the administrative API for connection migration, which performs thorough validation.

OTL for password reset expiry or reuse error reporting

Fixed PF-32090

In the case where a one-time link (OTL) for password reset expires or is reused, PingFederate now responds with the appropriate error message in the authentication API and logs the error response in the `audit.log`. Learn more about OTL for password reset in Configuring self-service account recovery.

Duplicate scope and scope group name values

Fixed PF-32234

We've resolved a defect that allowed scope and scope group names to be the same when saved through the administrative console. Learn more in Scopes and scope management.

Warning during SQL provisioning table creation

Fixed PF-32254

We've decreased the maximum key length for `saasGroupName`, resolving a warning that occurred when creating SQL provisioning tables.

'Change Password' link accessibility

Fixed PF-32343

On sign-on pages, we've improved the accessibility of the 'Change Password' link, regardless of browser window size.

Notification publisher accessor added to SDK

Fixed PF-32345

We've added a notification publisher accessor to the SDK, addressing an error where plugins utilizing a notification publisher could not invoke one of the notification publishers configured in PingFederate.

Fragment processing now independent of policy processing

Fixed PF-32461

PingFederate now processes policy fragments independently from policies and other fragments.

LIP registration via a third-party service and the authentication API

Fixed PF-32574

We've resolved a defect where Local Identity Profile (LIP) registration via a third-party service and the authentication API would still require a password, despite previously registering with the third party.

Known issues and limitations

PingID password credential validator with integrated RADIUS server

Issue

PingFederate versions 11.1.4, 11.1.5, 11.2.1, and 11.2.2 contain version 3.0.2 of the PingID password credential validator (PCV). That version of the PCV has known issues that you should review before upgrading. For more information, see Known issues in PingID RADIUS PCV 3.0.2.

Administrative console and administrative API

Issue

- /bulk: Only resource types currently supported by the administrative API are included in the exported data. We don't intend to introduce administrative API support to the following areas:
  - SAML 2.0 IdP Discovery
  - SAML 2.0 SP Affiliation
  - SMS Provider
- Previously, the administrative API did not accurately reflect a **Persistent Grant Max Lifetime** setting of 29 days (or shorter) with the selection of the **Grants Do Not Timeout Due To Inactivity** option. As a result, if you have configured such OAuth authorization server settings and have generated a bulk export in version 10.0 through 10.0.2, we recommend that you re-generate a new bulk export after upgrading to version 10.0.3 (or a more recent version). The newly exported data does not contain the aforementioned flaw, and you can safely import it to version 10.0.3 (or a more recent version).

- When enabling mutual TLS certificate-based authentication, administrators often configure a list of acceptable client certificate issuers. When you use a browser to access the console or the administrative API documentation, PingFederate returns to the browser the list of acceptable issuers as part of the TLS handshake. If the browser's client certificate store contains multiple client certificates, the browser often presents you only the certificates whose issuer matches one of the acceptable issuers. However, when PingFederate runs in a Java 11 environment, Chrome presents you all its configured client certificates, regardless of whether the issuer matches one of the acceptable issuers or not.
- Prior to toggling the status of a connection with the administrative API, you must ensure that any expired certificates or no longer available attributes are replaced with valid certificates or attributes; otherwise, the update request fails.
- When creating or updating a child instance of a hierarchical plugin, the administrative API retains objects with an `"inherited": false` name/value pair (or without such name/value pair altogether), ignores those with a value of `true`, and returns a 200 HTTP status code. No error messages are returned for the ignored objects.
- Using the browser's navigation mechanisms (for example, the **Back** button) causes inconsistent behavior in the administrative console. Use the navigation buttons provided at the bottom of windows in the PingFederate console.
- Using the PingFederate console in multiple tabs on one browser might cause inconsistent behavior which could corrupt its configuration.
- If authenticated to the PingFederate administrative console using certificate authentication, a session that has timed out might 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 sign-on page, and then back to the administrative console after authentication is complete. Similar behavior applies for certificate authentication, in principle. However, because the browser might automatically resubmit the certificate for authentication, the browser might redirect to the administrative console and not the sign on page.

TLSv1.3

Issue

For Java versions that don't support TLSv1.3 (meaning versions earlier than 8u261), PingFederate fails on start up with a `NoSuchAlgorithmException` exception. To resolve this error, remove `TLSv1.3` from the following settings in the `run.properties` file:

- **`pf.tls.client.protocols`**
- **`pf.tls.runtime.server.protocols`**
- **`pf.tls.admin.server.protocols`**

TLS cipher suite customization

Issue

PingFederate's TLS cipher suites can be customized by modifying `com.pingidentity.crypto.SunJCEManager.xml` (or a similarly-named file if BCFIPS or a hardware security module (HSM) is configured). After updating the file and replicating, all cluster nodes must be restarted for the change to take effect.

Java

Issue

- As of PingFederate 11.1, BC-FIPS and HSMs are not supported when using Java 17.
- Updating Java version 8 to version 11 results in an error when PingFederate is already installed and running. To work around this issue, uninstall and reinstall the PingFederate Windows service by running the `UninstallPingFederateService.bat` and `InstallPingFederateService.bat` files located in `<pf_install>/pingfederate/sbin/wrapper`.

Hardware security modules (HSMs)

Issue

AWS CloudHSM

- It is not possible to use an elliptic curve (EC) certificate as an SSL server certificate.
- TLS 1.3 is not currently supported.

Thales HSMs

- JWT token decryption using ECDH-ES may fail. This issue only arises if PingFederate is configured with static OAuth and OpenID Connect keys, a static key is stored on the HSM, and PingFederate is consuming a token encrypted with this key.
- It is not possible to use an elliptic curve (EC) certificate as an SSL server certificate.
- TLS 1.3 is not currently supported.

Entrust HSMs

- PingFederate must be deployed with Oracle Server Java Runtime Environment (JRE) 8 or Amazon Corretto 8.
- JWT token decryption using ECDH-ES or RSAES OAEP may fail. This issue only arises if PingFederate is configured with static OAuth and OpenID Connect keys, a static key is stored on the HSM, and PingFederate is consuming a token encrypted with this key.
- SAML assertion decryption using RSA OAEP may fail when the decryption key is stored on the HSM.
- It is not possible to use an elliptic curve (EC) certificate as an SSL server certificate.
- TLS 1.3 is not currently supported.

SSO and SLO

Issue

- When consuming SAML metadata, PingFederate does not report an error when neither the `validUntil` nor the `cacheDuration` attribute is included in the metadata. Note that PingFederate does reject expired SAML metadata as indicated by the `validUntil` attribute value, if it is provided.
- The anchored-certificate trust model cannot be used with the Single log off (SLO) redirect binding because the certificate cannot be included with the logout request.
- 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.

Composite Adapter configuration

Issue

SLO is not supported when users are authenticated through a Composite Adapter instance that contains another instance of the Composite Adapter.

Self-service password reset

Issue

Passwords can be reset for Microsoft Active Directory user accounts without the permission to change password.

OAuth

Issue

PingFederate does not support a case-sensitive naming convention for OAuth client ID values when client records are stored in a directory server. For example, after creating a client with an ID value of `sampleClient`, PingFederate does not allow the creation of another client with an ID value of `SampleClient`.

Although it's possible to create clients using the same ID values with different casings when client records are stored in XML files, a database server, or custom storage, we recommend not doing so to avoid potential record migration issues.

Customer identity and access management

Issue

Some browsers display a date-picker user interface for fields that have been designed for date-specific inputs. Some browsers do not. If one or more date-specific fields are defined on the registration page or the profile management page (or both), end users must enter the dates manually if their browsers do not display a date-picker user interface for those fields.

Provisioning

Issue

- 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.
- The `totalResults` value in SCIM responses indicates the number of results returned in the current response, not the total number of estimated results on the LDAP server.

Logging

Issue

- 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, the `USER_KEY` attribute will not be masked in the server logs. Other persistent grant attributes will be masked.
- Even if a source attribute has been configured for masking in an IdP adapter and the source attribute is mapped as the adapter's unique user key, the user key attribute is not masked in the server or audit logs.

Database logging

Issue

- 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, the `USER_KEY` attribute will not be masked in the server logs. Other persistent grant attributes will be masked.
- Even if a source attribute has been configured for masking in an IdP adapter and the source attribute is mapped as the adapter's unique user key, the user key attribute is not masked in the server or audit logs.

RADIUS NAS-IP-Address

Issue

The RADIUS NAS-IP-Address is only included in Access-Request packets when the `pf.bind.engine.address` is set with an IPv4 address. IPv6 is not supported.

PingOne Fraud integration kit

Info PingOne Fraud

The PingOne Fraud integration kit is no longer bundled with PingFederate.

Deprecated features

Microsoft Internet Explorer 11

Info

Ping Identity commits to deliver the best experience for administrators and users. As we continue to improve our products, we encourage you to migrate off of Microsoft Internet Explorer 11. Starting with PingFederate 11.0, Internet Explorer 11 is no longer included in the PingFederate qualification process for administrators or users. For a list of supported browsers, see System requirements.

Configcopy tool, Connection Management Service, SSO Directory Service

Info

As of PingFederate 10.2, these features have been deprecated and will be removed in a future release.

Oracle Directory Server Enterprise Edition

Info

As Oracle ended its Premier Support for Oracle Directory Server Enterprise Edition (ODSEE 11g) in December 2019, we no longer include ODSEE as part of the PingFederate qualification process (starting with PingFederate 10.2). We continue to qualify against Oracle Unified Directory and other supported directory servers. For a full list, see System requirements.

SNMP

Info

Starting with PingFederate 10.2, monitoring and reporting through the Simple Network Management Protocol (SNMP) has been removed.

Roles and protocols

Info

Starting with PingFederate 10.1, roles and protocols are always enabled and no longer configurable through the administrative console and API.

S3_PING discovery protocol

Info

Starting with PingFederate 10.1, the S3_PING discovery protocol has been deprecated. Customers running on AWS infrastructure should instead use NATIVE_S3_PING.

Red Hat Enterprise Linux install script

Info

Starting with PingFederate 10.0, the Red Hat Enterprise Linux install script is no longer available. To install PingFederate 10.0 for Linux, you must download and extract the product distribution `.zip` file.

PingFederate 11.1.11 (January 2025)

Resolved issues

Eliminating redundant group updates

Fixed PF-33441

We've fixed a defect that caused PingFederate, when configured with PingDirectory as an outbound provisioning data source, to send redundant group updates in each provisioning cycle when the entry remains unchanged.

Provisioner uses the wrong time zone when data source and PingFederate are in different time zones

Fixed PF-35286

We've fixed a defect that caused redundant user provisioner updates when the data source and PingFederate were in different time zones.

Group membership loss during provisioning

Fixed PF-36874

We've fixed a defect that caused PingFederate to lose user group membership information when it lost contact with the data store during provisioning operations.

PingFederate 11.1.10 (April 2024)

Resolved issues

Rest datastore security vulnerability

Security PF-34720

Fixed a JSON injection vulnerability in REST datastores described in security advisory SECADV044.

Runtime nodes security vulnerability

Security PF-34896

Fixed a path traversal vulnerability in Runtime nodes described in security advisory SECADV044.

OpenID Connect policy management editor security vulnerability

Security PF-35081

Fixed a Cross-Site Scripting vulnerability in the OpenID Connect Policy Management Editor described in security advisory SECADV044.

Slow log consumption affects performance

Fixed PF-33368

Fixed a defect that caused performance issues for PingFederate when third-party logging services were slow to consume logging events.

PingFederate 11.1.9 (November 30)

Resolved issues

Outbound provisioning performance improvement

Fixed PF-33466

You can now turn off server-side sorting for LDAP requests related to outbound provisioning, which can improve performance in some environments.

Configure this option using the `ProvisionWithServerSort` parameter in the `com.pingidentity.common.util.ldap.LDAPUtil.xml` file.

Updating OAuth clients with dynamic client registration

Fixed PF-34146

Fixed a defect where an OAuth client created with dynamic client registration (DCR) couldn't be updated with DCR after it was modified with the administrative console.

Resolved a vulnerability in the Initial Setup Wizard

Security PF-34646

Fixed a Server-Side Request Forgery vulnerability in the Initial Setup Wizard described in security advisory SECADV041.

PingFederate 11.1.8 (August 2023)

Resolved issues

Potential security vulnerability

Fixed PF-33449

We've resolved a potential security vulnerability that is described in security advisory SECADV037.

Binary attributes handled incorrectly when using PingOne LDAP gateway datastores

Fixed PF-33637

Now when PingFederate retrieves a binary attribute from a PingOne LDAP gateway datastore, it correctly converts the attribute value to the specified format (base64, SID, hex).

Potential security vulnerability

Fixed PF-34017

We've resolved a potential security vulnerability that is described in security advisory SECADV037.

PingFederate 11.1.7 (May 2023)

Resolved issues

Logging validation

Fixed PF-32764

We've improved logging validation.

Resource Owner (RO) Password Credentials flow

Fixed PF-33359

We've improved the error messaging around the Resource Owner (RO) Password Credentials flow.

Requested Authentication Context Selector

Fixed PF-33549

The Requested Authentication Context Selector no longer throws a Null Pointer Exception (NPE) during callback.

PingFederate 11.1.6 (February 2023)

Resolved issues

Log improvements

Fixed PF-33017

In order to reduce re-encryption and file scanning log verbosity, when a configuration is imported or replicated to a cluster, PingFederate no longer scans files in the `etc` directory.

Other improvements

Info

- We also updated the following bundled components and third-party dependencies:
  - PingID Integration Kit 2.24
  - PingID Adapter 2.13.2
  - PingID PCV (with integrated RADIUS server) 3.0.3

PingFederate 11.1.5 (February 2023)

Resolved issues

Server log warnings

Fixed PF-33037

We've added a warning to server logs if the *ds-pwp-state-json* attribute is not present in PingDirectory's LDAP Response. This warning appears in the log every time a user interacts with the profile management page. Please enable this attribute to adhere to PingDirectory's security configuration best practices. PingDirectory version 8.1 and later supports this attribute, and customers running older versions are encouraged to upgrade to a supported version as soon as possible.

PingFederate 11.1.4 (February 2023)

Resolved issues

OAuth client management

Fixed PF-32790

When managing OAuth clients, we've resolved a defect where selecting the **Require JWT Secured Authorization Response Mode** text toggled the incorrect checkbox.

Potential security vulnerability

Fixed PF-32805

We've resolved a potential security vulnerability that is described in security advisory SECADV033.

Informing adapters of end policy result

Fixed PF-32890

When processing policy fragments, all adapters invoked in the fragment now correctly execute their respective post-processing step (if applicable) to inform the adapter of the end policy result.

Managing certificates within Metadata Export

Fixed PF-32965

Managing certificates within the **Metadata Export** flow no longer displays or saves an empty list of certificates, clearing out existing ones in the process. For more information, see Metadata export.

Cluster data replication

Fixed PF-32983

We've resolved a defect where cluster data replication could remove keys from engine node's `pf.jwk` file instead of merging and retaining the keys.

PingFederate 11.1.3 (December 2022)

Resolved issues

Improvements to custom revocation checker

Fixed PF-32395

We've improved PingFederate's custom revocation checker, ensuring that when the server returns stapled Online Certificate Status Protocol (OCSP) responses, PingFederate invokes the checker. Previously, PingFederate used the default revocation checker to validate these responses, which could cause single sign-on (SSO) failures with BCFIPS mode enabled. For more information, see Configuring certificate revocation.

Cluster replication notifications

Fixed PF-32398

We've improved notifications to signal to administrators that in the event of a replication failure or any changes to cluster configuration require replication. For more information, see Cluster management.

Null pointer exception during dependency error detection

Fixed PF-32553

During PingFederate dependency error detection, OGNL expressions in adapter-to-adapter mappings no longer raise a null pointer exception (NPE).

PingFederate updates to HSM ordering

Fixed PF-32556

We've updated the recommended security provider ordering for the Thales Luna Network hardware security module (HSM) to address an issue where temporary keys and sessions could accumulate on the HSM, eventually resulting in resource exhaustion. A limitation of the new ordering is that EC certificates can no longer operate as SSL server certificates. For details on the new order, see Integrating with Thales Luna Network HSM.

PingFederate 11.1.2 (October 2022)

Resolved issues

Bulk import for IdP connections

Fixed PF-31870

Resolved an issue where bulk import fails for identity provider (IdP) connections that fulfill Persistent Grant Extended Attributes.

Connection failures on external LDAP authentication login

Fixed PF-32001

PingFederate now recovers from initial connection failure when logging into the administrative console using external LDAP authentication.

Hiding user information from authentication API responses

Fixed PF-32028

You can now configure the setting `IncludeUserInfoInResponses` in the `<install dir>/server/default/data/config-store/org.sourceid.saml20.domain.mgmt.impl.AuthnApiManagerImpl.xml` file to hide user information from authentication API responses.

Errors on policy fragments configured to handle failures locally

Fixed PF-32073

When an error occurs on policies containing fragments and configured to handle failures locally, PingFederate no longer redirects a user to the service provider (SP) error page on SP-initiated single sign-on (SSO).

Outbound TLS connection failures

Fixed PF-32199

The certificate path-building algorithm now uses PingFederate's custom revocation checker. This fix resolves a bug where outbound TLS connections failed for servers that presented out-of-order certificate chains.

PingDirectory user registration

Fixed PF-32241

During user registration, PingFederate now sends all passwords to PingDirectory, resolving an issue where passwords consisting of only spaces would not properly register a PingDirectory password.

Configurations with no connection type in Kerberos realm

Fixed PF-32274

When reading the `pingfederate-kerberos-realms.xml` file, PingFederate no longer raises an error for configurations with no connection type in the Kerberos realm.

PingFederate 11.1.1 (July 2022)

Resolved issues

Security around password expiration

Fixed PF-29706 PingDirectory

Improved the security around password expiration when using PingDirectory as a user store.

Issuance criteria in authentication policy contracts

Fixed PF-31485

Issuance criteria in authentication policy contracts no longer cause the logs to indicate invalid XML errors. This issue did not cause runtime errors.

HTTP header for client IP addresses

Fixed PF-31735

Resolved an issue that sometimes occurred when IPV6 addresses were specified in the **HTTP Header for Client IP Addresses** field on the **Incoming Proxy Settings** window.

Error descriptions

Fixed PF-31753

PingFederate error descriptions no longer disclose details of java classes.

MasterKeyEncryptor failure during cluster replication

Fixed PF-31795

When PingFederate is using a custom MasterKeyEncryptor that relies on an SSL call to an external service, cluster replication no longer causes cascading failures because PingFederate is unable to open Java key store files.

Updating the client secret with the OAuth client management service

Fixed PF-31851

When updating the client secret with the OAuth client management service, PingFederate now correctly creates the secondary secrets.

OAuth authorization requests with `response_mode=pi.flow`

Fixed PF-31942

Now when PingFederate receives an OAuth authorization request with `response_mode=pi.flow`, password change and account recovery flows using an authentication policy work correctly.

Administrative API enhancement

Info

Improved the administrative API to manage the System for Cross-domain Identity Management (SCIM) inbound provisioning settings in identity provider (IdP) connections.

Message customization enhancement

Info

Enhanced PingFederate message customization by adding the following FedHub-specific context variables:

- `FedHubSpConnApplicationName`
- `FedHubSpConnName`
- `FedHubOAuthClientId`

- `FedHubOAuthClientName`

Cluster management enhancement

Info

Revised the **Cluster Management** window to make it more obvious when changes to the configuration on the administrative node have not been replicated to the engine nodes.

PingFederate 11.1 (June 2022)

New features and improvements in PingFederate 11.1.

New features and enhancements

PingOne integration

New PingOne

We've added Kerberos authentication via PingOne and the PingOne LDAP Gateway Data Store. This new capability allows PingFederate in the cloud, without a direct connection to Active Directory, to complete Kerberos authentication for browser-based SSO requests and STS transactions through PingOne.

JWT Secured Authorization Response Mode (JARM)

New

We're proud to support JWT Secured Authorization Response Mode (JARM) in version 11.1. JARM allows authorization servers to transmit authorization responses in JSON web tokens (JWTs), providing digital signature and encryption, sender authentication, and audience restriction. As JARM becomes a requirement in FAPI 2, you can deploy open banking solutions confidently.

JWT Response for OAuth Token Introspection

New

We're also introducing support for JWT Response for OAuth Token Introspection, a draft specification on track to become one of the authorization server requirements in the FAPI 2 Advanced Profile. JWT-secured introspection responses provide stronger assurance to the introspection requesters, most relevant when the requester, such as a resource server, expects to receive verified claims from the authorization server.

Client secret management

New

Seamless client secret rotation no longer requires real-time coordination between PingFederate administrators and the application development teams. You can now configure PingFederate to retain previous secrets for a configurable period, during which the application teams can work on updating the client secrets in their apps. This enhancement drastically lowers the costs of securing applications that use client secrets for authentication. For more information, see "Client Secret Retention Period" in the topic Managing client configuration defaults.

API support for Device Authorization Grant

New

In addition to template-driven user experience, the user authorization step from Device Authorization Grant supports API now. You can also decide whether PingFederate should check the device activation code before or after authentication. These new capabilities enable you to build applications with the desired user experience for input-constrained devices, such as smart TVs or telepresence equipment.

Amazon DynamoDB for grants

New

You can store OAuth persistent grants in Amazon DynamoDB, which allows you to take advantage of a NoSQL database where it matters most: delivering responsive experiences to globally distributed users and offering high availability at ease.

Revocation of self-contained access tokens

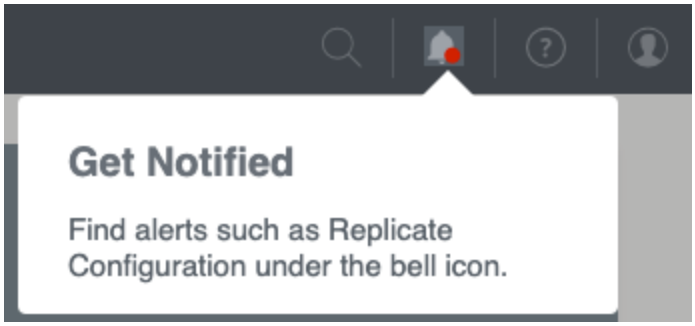
New

You can optionally enable direct revocation for self-contained access tokens (JWT access tokens). This flexibility provides a secure way to invalidate access tokens without revoking the underlying refresh tokens or persistent grants. For more information, see Configuring an access token management instance and its description of the **Enable Token Revocation** checkbox.

A new alert system

New

PingFederate 11.1 centralizes alerts, such as the reminder to replicate configuration, under the new **bell** icon in the top menu. You can review important alerts from any configuration window.



Copy-and-paste authentication policies and fragments

New

Previously, if you wanted to update an authentication policy or a reusable policy fragment midstream, they had to reconfigure all downstream paths, which can take some effort. With PingFederate 11.1, you can copy a subtree of policy paths before removing a step (such as an IdP adapter), adding a new step (such as a selector or another IdP adapter), and then pasting the subtree back to the policy. This new capability applies to reusable policy fragments and between authentication policies and reusable policy fragments.

Administrative API to move individual policies

New

You can use the administrative API to move an individual policy to a specific location. This enhancement makes re-organizing policies by API requests easier and safer.

Cluster configuration management

New

PingFederate engine nodes now capture common configuration replication issues in their server logs and send replication status back to the console node. The **Cluster Management** window provides live updates when you select **Replicate Configuration** in the **Cluster Management** window. If an error occurs, you can act on it immediately and recover from potential outages faster.

Passthrough IdP Adapter

New

You can now associate authentication sessions with user identities passed through the new Passthrough Identity Provider (IdP) Adapter. By placing the Passthrough IdP Adapter downstream from an IdP connection in a policy tree, you can take advantage of additional capabilities associated with defining a user key. For example, you can use the user key to query or revoke a user's authentication sessions.

Kerberos authentication and ObjectSID

New

The Kerberos Adapter and the Kerberos Token Processor now return the `ObjectSID` attribute value. Because `ObjectSID` uniquely identifies the user in Active Directory, leveraging it helps streamline the **Attribute Source & Lookup** configuration.

Kerberos authentication and re-authentication

New

You can configure the Kerberos Adapter to fail when the service provider asks for re-authentication by including `ForceAuthn=true` (SAML 2.0) or `prompt=login` (OpenID Connect) in their authentication requests. For example, suppose user interactions are

required when the partners ask for re-authentication. In that case, you can add the HTML Form Adapter to the **Fail** policy path of the Kerberos Adapter.

More error handling options

New

- You now can configure individual authentication policies to handle authentication failures locally without redirecting to the service providers or returning error messages to the OAuth clients. This flexibility addresses the scenario where an IdP-oriented end-user experience is desirable.
- PingFederate now includes error results from issuance criteria in error responses. Partners can use the error results to resolve issues as needed. If the invoked policy is configured to handle failures locally, you can do the same to improve the end-user experience.
- You can now optionally configure the HTML Form Adapter not to return control to PingFederate when an account lockout occurs. Instead, PingFederate returns a “please try again later” message to the browser or the authentication API application.

Extended properties for end-user interactions

New

You can now leverage extended properties in Velocity templates when customizing template-driven end-user interactions. You can reference extended properties in the templates instead of creating multiple `If` / `ElseIf` / `Else` directives, significantly reducing the initial effort. New and updated experiences can be inherited from extended property values from the OAuth client records and Browser SSO connections, eliminating most of the maintenance costs. PingFederate also passes extended property values to authentication API applications. As a result, application developers who create and maintain end-user UX for customer identities will benefit from this new enhancement.

Better documentation in Velocity templates

New

We've also improved inline documentation in our Velocity templates. Moving forward, we will maintain variable names and their definitions consistently to communicate changes, such as introducing new variables.

Enhancements in Thales HSM integration

New

Both Java 11 and 8 environments are supported when integrating with Thales Luna Cloud Hardware Security Module (HSM) Services or Luna Network HSMs. For more information about Thales Luna HSM Client, see the Luna Cloud HSM Service Client Guide and Luna Network HSM Documentation Archive.

Secondary signing certificate

New

You can now add a secondary signing certificate to your connections. If configured, PingFederate includes it in both the metadata exports and the metadata URL responses. This flexibility allows you to notify your partners about upcoming changes more easily through metadata.

Administrative API improvements

New

We improved the PingFederate administrative API to manage the following configurations:

- JIT provisioning settings in IdP connections
- **System > Data & Credential Stores > Identity Store Provisioners**
- **System > Server > General Settings**
- **System > Server > WS-Trust Settings**

Other improvements

New

- We significantly improved our metrics exposed through HTTP (at the heartbeat endpoint) and JMX to help you detect and diagnose performance issues. Both channels include HTTP response code counts, data source response time statistics, and Jetty queue size information; these metrics help troubleshoot latency issues associated with datastores or traffic volume.
- PingFederate now uses OCSP to obtain certificate revocation status by default on new installations. As part of this enhancement, PingFederate uses the OCSP responder URL provided in the certificate first, followed by the now optional Default OCSP Responder URL, and lastly, CRL, making the certificate validation process more efficient.
- The administrative console now provides guidance when you attempt to import a configuration archive obtained from a different version of PingFederate.
- PingFederate 11.1 supports Amazon IAM roles for service accounts, which increases security posture with credential isolation and auditability.
- PingOne Verify is now part of the PingFederate distribution `.zip` file and Windows installer.
- We also updated the following bundled components and third-party dependencies:
  - PingID Integration Kit 2.17
  - PingOne Fraud Integration Kit 1.0
  - PingOne Protect Integration Kit 1.2
  - Jackson-Databind 2.12.7
  - Log4j2 2.17.2
  - Spring Framework 5.3.20

Resolved Issues

H2 database engine upgrade

Fixed PF-21198

Upgraded the H2 database engine to version 2.1.210.

A username in the URL during change password flows

Fixed PF-24501

The username no longer appears in the URL during change password flows.

Guava upgrade

Fixed PF-28932

Upgraded the Guava dependency to version 30.1.1.

OAuth client Issuer DN

Fixed PF-29368

If the administrative API was used to create an OAuth client that has the Client Certificate authentication type, and the client's Issuer DN does not have a normalized DN value, the administrative console's **Client** window no longer fails to show the Issuer DN as the default value. This issue didn't affect runtime behavior.

Time stamp for last update

Fixed PF-29761

When a user record in a datastore mistakenly has a future date for the last update time, PingFederate no longer uses that date as the value of `attrib_last_timestamp` in the `channel_variable` table. Instead, PingFederate sets the value to the maximum time stamp that is not in the future.

Number and Boolean data types in JSON responses from REST API data source lookups

Fixed PF-29835

The JSON response from REST API data source lookups now retains number and Boolean data types instead of converting them to strings.

`NotYetConnectedException` warning messages from JGroup in the `server.log`

Fixed PF-30075

Resolved an issue that caused the `NotYetConnectedException` warning message to repeatedly appear in the `server.log` when using AWS_PING for dynamic cluster discovery.

Matching OAuth client's redirection URIs

Fixed PF-30146

If the OAuth client's redirection URI contains a wild card in the authority part of the URI, and the `redirect_uri` parameter of the token request contains userinfo in the authority part, then PingFederate will no longer consider the redirection URI a match.

Potential security vulnerability

Fixed PF-30255

Resolved a potential security vulnerability.

Logging invalid assertion errors

Fixed PF-30495

In a specific case, when PingFederate logs an invalid assertion error, the error message no longer fails to include a remark about why the assertion or response is invalid.

Null pointer exception in authentication API password reset flow

Fixed PF-30558

When an OAuth client is performing a password reset through the authentication API, if PingFederate does not find any session attributes, now PingFederate logs an error state instead of a null pointer exception.

Determining authentication instants for flows

Fixed PF-30770

Resolved an issue that prevented PingFederate from correctly determining the authentication instant for the flow when the initial OIDC authorization request specifies a max_age, the flow falls through to legacy authentication source selection (policies are disabled or no policy applies), and the user chooses an upstream OIDC IdP connection.

Templates for PingOne MFA 1.6.1

Fixed PF-30806 PingOne MFA

PingFederate now includes all the templates for PingOne MFA 1.6.1.

Dependency errors for SAML token processors and generators

Fixed PF-31054

When saving SAML token processors or generators, PingFederate now correctly handles dependency errors caused by misconfigured settings on the **Protocol Settings** window's **Federation Info** tab.

Preserving the order of map type configurations

Fixed PF-31145

Now PingFederate preserves the order of map type configurations under `<pf_install>/pingfederate/server/default/data/config-store` when performing a bulk export or a GET operation at the `/configStore` administrative API endpoint.

Warning about using the administrative console in multiple tabs

Fixed PF-31280

Now if you use the PingFederate administrative console in multiple tabs on one browser, it warns you that doing so might cause inconsistent behavior which could corrupt its configuration.

Saving authorization server settings overwrites scope.whitelist

Fixed PF-31304

Resolved an issue that caused PingFederate to overwrite the `scope.whitelist` in the `\data\config-store\org.sourceid.oauth20.domain.AuthzServerManagerImpl.xml` file when you save the authorization server settings.

OAuth client IDs added to admin.log entries

Fixed PF-31561

Now OAuth client MODIFY, CREATE, and DELETE event log entries in the `admin.log` include the client ID.

Honoring the property for maximum HTTP request body size

Fixed PF-31575

Now PingFederate honors the value of `http.maxRequestBodySize` in the `run.properties` file, which specifies the maximum HTTP request body size of any incoming request to PingFederate's web services and administrative API.

Known issues and limitations

Administrative console and administrative API

Issue

- /bulk: Only resource types currently supported by the administrative API are included in the exported data. We don't intend to introduce administrative API support to the following areas:
  - SAML 2.0 IdP Discovery
  - SAML 2.0 SP Affiliation
  - SMS Provider
- Previously, the administrative API did not accurately reflect a **Persistent Grant Max Lifetime** setting of 29 days (or shorter) with the selection of the **Grants Do Not Timeout Due To Inactivity** option. As a result, if you have configured such OAuth authorization server settings and have generated a bulk export in version 10.0 through 10.0.2, we recommend that you re-generate a new bulk export after upgrading to

version 10.0.3 (or a more recent version). The newly exported data does not contain the aforementioned flaw, and you can safely import it to version 10.0.3 (or a more recent version).

- When enabling mutual TLS certificate-based authentication, administrators often configure a list of acceptable client certificate issuers. When you use a browser to access the console or the administrative API documentation, PingFederate returns to the browser the list of acceptable issuers as part of the TLS handshake. If the browser's client certificate store contains multiple client certificates, the browser often presents you only the certificates whose issuer matches one of the acceptable issuers. However, when PingFederate runs in a Java 11 environment, Chrome presents you all its configured client certificates, regardless of whether the issuer matches one of the acceptable issuers or not.
- Prior to toggling the status of a connection with the administrative API, you must ensure that any expired certificates or no longer available attributes are replaced with valid certificates or attributes; otherwise, the update request fails.
- When creating or updating a child instance of a hierarchical plugin, the administrative API retains objects with an `"inherited": false` name/value pair (or without such name/value pair altogether), ignores those with a value of `true`, and returns a 200 HTTP status code. No error messages are returned for the ignored objects.
- Using the browser's navigation mechanisms (for example, the **Back** button) causes inconsistent behavior in the administrative console. Use the navigation buttons provided at the bottom of windows in the PingFederate console.
- Using the PingFederate console in multiple tabs on one browser might cause inconsistent behavior which could corrupt its configuration.
- If authenticated to the PingFederate administrative console using certificate authentication, a session that has timed out might 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 sign-on page, and then back to the administrative console after authentication is complete. Similar behavior applies for certificate authentication, in principle. However, because the browser might automatically resubmit the certificate for authentication, the browser might redirect to the administrative console and not the sign on page.

TLSv1.3

Issue

For Java versions that don't support TLSv1.3 (meaning versions earlier than 8u261), PingFederate fails on start up with a `NoSuchAlgorithmException` exception. To resolve this error, remove `TLSv1.3` from the following settings in the `run.properties` file:

- **`pf.tls.client.protocols`**
- **`pf.tls.runtime.server.protocols`**
- **`pf.tls.admin.server.protocols`**

TLS cipher suite customization

Issue

PingFederate's TLS cipher suites can be customized by modifying `com.pingidentity.crypto.SunJCEManager.xml` (or a similarly-named file if BCFIPS or a hardware security module (HSM) is configured). After updating the file and replicating, all cluster nodes must be restarted for the change to take effect.

Java

Issue

- As of PingFederate 11.1, BC-FIPS and HSMs are not supported when using Java 17.
- Updating Java version 8 to version 11 results in an error when PingFederate is already installed and running. To work around this issue, uninstall and reinstall the PingFederate Windows service by running the `UninstallPingFederateService.bat` and `InstallPingFederateService.bat` files located in `<pf_install>/pingfederate/sbin/wrapper`.

Hardware security modules (HSM)

Issue

- For Entrust HSMs, it is not possible to use an elliptic curve (EC) certificate as an SSL server certificate.

- For Entrust HSMs, PingFederate must be deployed with Oracle Server JRE 8 or Amazon Corretto 8.
- For keys stored in AWS CloudHSMs, JWT token signing fails when using RSASSA-PSS SHA-512.
- For keys stored in Thales HSMs, JWT token decryption fails when using RSAES OAEP with AES-CBC-192 or AES-CBC-256. This issue only arises if PingFederate is configured with static OAuth and OpenID Connect keys and is consuming a token encrypted with one of these keys.
- When PingFederate is configured in hybrid mode with a Thales HSM, it is not possible to export a locally-stored EC key pair.
- When PingFederate is configured in hybrid mode with a Thales HSM, JWT token decryption using ECDH-ES may fail. This issue only arises if PingFederate is configured with static OAuth and OpenID Connect keys, a static key is stored locally, and PingFederate is consuming a token encrypted with this key.
- TLS 1.3 is not currently supported with any HSM.

SSO and SLO

Issue

- When consuming SAML metadata, PingFederate does not report an error when neither the `validUntil` nor the `cacheDuration` attribute is included in the metadata. Note that PingFederate does reject expired SAML metadata as indicated by the `validUntil` attribute value, if it is provided.
- The anchored-certificate trust model cannot be used with the Single log off (SLO) redirect binding because the certificate cannot be included with the logout request.
- 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.

Composite Adapter configuration

Issue

SLO is not supported when users are authenticated through a Composite Adapter instance that contains another instance of the Composite Adapter.

Self-service password reset

Issue

Passwords can be reset for Microsoft Active Directory user accounts without the permission to change password.

OAuth

Issue

PingFederate does not support a case-sensitive naming convention for OAuth client ID values when client records are stored in a directory server. For example, after creating a client with an ID value of `sampleClient`, PingFederate does not allow the creation of another client with an ID value of `SampleClient`.

Although it's possible to create clients using the same ID values with different casings when client records are stored in XML files, a database server, or custom storage, we recommend not doing so to avoid potential record migration issues.

Customer identity and access management

Issue

Some browsers display a date-picker user interface for fields that have been designed for date-specific inputs. Some browsers do not. If one or more date-specific fields are defined on the registration page or the profile management page (or both), end users must enter the dates manually if their browsers do not display a date-picker user interface for those fields.

Provisioning

Issue

- 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.
- The `totalResults` value in SCIM responses indicates the number of results returned in the current response, not the total number of estimated results on the LDAP server.

Logging

Issue

- 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, the `USER_KEY` attribute will not be masked in the server logs. Other persistent grant attributes will be masked.
- Even if a source attribute has been configured for masking in an IdP adapter and the source attribute is mapped as the adapter's unique user key, the user key attribute is not masked in the server or audit logs.

Database logging

Issue

- 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, the `USER_KEY` attribute will not be masked in the server logs. Other persistent grant attributes will be masked.
- Even if a source attribute has been configured for masking in an IdP adapter and the source attribute is mapped as the adapter's unique user key, the user key attribute is not masked in the server or audit logs.

RADIUS NAS-IP-Address

Issue

The RADIUS NAS-IP-Address is only included in Access-Request packets when the `pf.bind.engine.address` is set with an IPv4 address. IPv6 is not supported.

Deprecated features

Microsoft Internet Explorer 11

Info

Ping Identity commits to deliver the best experience for administrators and users. As we continue to improve our products, we encourage you to migrate off of Microsoft Internet Explorer 11. Starting with PingFederate 11.0, Internet Explorer 11 is no longer included in the PingFederate qualification process for administrators or users. For a list of supported browsers, see System requirements.

Configcopy tool, Connection Management Service, SSO Directory Service

Info

As of PingFederate 10.2, these features have been deprecated and will be removed in a future release.

Oracle Directory Server Enterprise Edition

Info

As Oracle ended its Premier Support for Oracle Directory Server Enterprise Edition (ODSEE 11g) in December 2019, we no longer include ODSEE as part of the PingFederate qualification process (starting with PingFederate 10.2). We continue to qualify against Oracle Unified Directory and other supported directory servers. For a full list, see System requirements.

SNMP

Info

Starting with PingFederate 10.2, monitoring and reporting through the Simple Network Management Protocol (SNMP) has been removed.

Roles and protocols

Info

Starting with PingFederate 10.1, roles and protocols are always enabled and no longer configurable through the administrative console and API.

S3_PING discovery protocol

Info

Starting with PingFederate 10.1, the S3_PING discovery protocol has been deprecated. Customers running on AWS infrastructure should instead use NATIVE_S3_PING.

Red Hat Enterprise Linux install script

Info

Starting with PingFederate 10.0, the Red Hat Enterprise Linux install script is no longer available. To install PingFederate 10.0 for Linux, you must download and extract the product distribution `.zip` file.

PingFederate 11.0.10 - April 2024

Resolved issues

Rest datastore security vulnerability

Security PF-34720

Fixed a JSON injection vulnerability in REST datastores described in security advisory SECADV044.

Runtime nodes security vulnerability

Security PF-34896

Fixed a path traversal vulnerability in Runtime nodes described in security advisory SECADV044.

OpenID Connect policy management editor security vulnerability

Security PF-35081

Fixed a Cross-Site Scripting vulnerability in the OpenID Connect Policy Management Editor described in security advisory SECADV044.

Slow log consumption affects performance

Fixed PF-33368

Fixed a defect that caused performance issues for PingFederate when third-party logging services were slow to consume logging events.

PingFederate 11.0.9 (December 2023)

Resolved issues

PF-29706 Fixed

Fixed a Server-Side Request Forgery vulnerability in the Initial Setup Wizard described in security advisory SECADV041.

PingFederate 11.0.8 (August 2023)

Resolved issues

Logging validation

Fixed PF-34017

We've improved logging validation.

Potential security vulnerability

Fixed PF-33449

We've resolved a potential security vulnerability that is described in security advisory SECADV037.

Potential security vulnerability

Fixed PF-34017

We've resolved a potential security vulnerability that is described in security advisory SECADV037.

PingFederate 11.0.7 (February 2023)

Resolved issues

Server log warnings

Fixed PF-33037

We've added a warning to server logs if the *ds-pwp-state-json* attribute is not present in PingDirectory's LDAP Response. This warning appears in the log every time a user interacts with the profile management page. Please enable this attribute to adhere to PingDirectory's security configuration best practices. PingDirectory version 8.1 and later supports this attribute, and customers running older versions are encouraged to upgrade to a supported version as soon as possible.

PingFederate 11.0.6 (February 2023)

Resolved issues

Potential security vulnerability

Fixed PF-32805

We've resolved a potential security vulnerability that is described in security advisory SECADV033.

PingFederate 11.0.5 (October 2022)

Resolved issues

IPV6 address issue

Fixed PF-31735

Resolved an issue that sometimes occurred when IPV6 addresses were specified in the **HTTP Header for Client IP Addresses** field on the **Incoming Proxy Settings** window.

Administrative console login

Fixed PF-32001

PingFederate now recovers from initial connection failure when logging into the administrative console using external LDAP authentication.

User registration defect resolution

Fixed PF-32241

During user registration, PingFederate now sends all passwords to PingDirectory, resolving an issue where passwords consisting of only spaces would not properly register a PingDirectory password.

PingFederate 11.0.4 (August 2022)

Resolved issues

MasterKeyEncryptor and cluster replication

Fixed PF-31795

When PingFederate uses a custom MasterKeyEncryptor that relies on an SSL call to an external service, cluster replication no longer causes cascading failures because PingFederate cannot open Java key store files.

Rule matching for fragment nodes and NullPointerException

Fixed PF-31929

When using rule matching for fragment nodes, PingFederate no longer raises a NullPointerException (NPE) if a fragment fails.

Zero byte archives

Fixed PF-31966

Resolved an issue that caused PingFederate to generate a zero byte archive when it couldn't read a file in the `<pf_install>/pingfederate/server/default/data` directory.

JWT access token lifetimes

Fixed PF-31989

When using centralized and dynamically rotating keys for OAuth and OpenID Connect, PingFederate now prevents you from setting the JWT access token lifetime to be longer than the `dynamic-rotation-period-in-days` specified in `<pf_install>/pingfederate/server/default/data/config-store/jwks-endpoint-configuration.xml`.

PingFederate 11.0.3 (May 2022)

Resolved issues

Intermittent failure to respond after restart caused by LDAP SDK

Fixed PF30776

To resolve an issue in which PingFederate occasionally stopped responding after a restart, the UnboundID LDAP SDK for Java was updated to version 6.0.4.

TLS 1.3 for outbound connections

Fixed PF-31303

PingFederate now supports TLS 1.3 for outbound connections when running on Java 8 versions 8u261 and newer.

Updated Spring Framework

Info PF-31169

Updated Spring Framework to version 5.3.18.

PingFederate 11.0.2 (March 2022)

New features and enhancements

Updated PingOne MFA adapter

Info PingOne MFA

Updated the bundled PingOne MFA adapter to version 1.6.

Resolved issues

LDAP connections

Fixed PF-30804

Resolved an issue that caused LDAP connections to periodically fail during provisioning.

Bulk export

Fixed PF-30863

Bulk export no longer fails to include all XML OAuth clients in the response payload.

Single sign-on from browsers on iOS

Fixed PF-31057

Resolved an issue that caused single sign-on from browsers on iOS to fail when an authentication policy terminates on Kerberos Adapter fallback that has an existing session.

nCipher mode

Fixed PF-31064

When running PingFederate in nCipher mode, now the administrative API successfully generates elliptic curve (EC) keys when the optional signatureAlgorithm field is not provided.

TLS 1.3 for inbound connections

Fixed PF-31112

PingFederate now supports TLS 1.3 for inbound connections when running on Java 8 versions 8u261 and newer.

Symantec VIP Adapter

Fixed PF-31123

Resolved an issue that prevented PingFederate from using the Symantec VIP Adapter.

LDAP-related performance

Fixed PF-31146

Resolved an LDAP-related performance issue.

Signature verification for certificate revocation lists

Fixed PF-31159

Resolved an issue where signature verification for certificate revocation lists could take more than 10 seconds on Windows. When LDAP-based authentication was enabled in the administrative console, this could prevent administrative users from signing on.

PingFederate 11.0.1 (January 2022)

New features and enhancements

Rolling grace period for refresh tokens

Improved

When PingFederate rotates a refresh token, if the client fails to get the new token, now PingFederate can accept the previous token for the short period that you specify with the **Refresh Token Rolling Grace Period** setting.

Performance improvement

Info

Improved performance of the administrative console when a large number of OAuth clients are stored in LDAP or JDBC datastores.

URL region of the PingOne home button

Info PingOne

When configuring the URL of the PingOne home button in the PingFederate administrative console, now `pf.pingone.admin.url.region` in `run.properties` supports `Canada` as a region.

AWS CloudHSM client

Info

PingFederate can be successfully integrated with AWS CloudHSM client version 3.4.4.

Resolved issues

Resolved a potential security vulnerability

Security PF-30450

Resolved a potential security vulnerability that is described in security bulletin SECBL021.

Updated Apache Log4j2

Security PF-30536

Resolved a potential security vulnerability by updating Apache Log4j2 to version 2.17.1.

Authenticating PingDirectory users

Fixed PF-30557 PingDirectory

Resolved an issue that allowed PingDirectory users to authenticate with expired passwords.

Certificate revocation list checks

Fixed PF-30637

Resolved an issue that caused certificate revocation list (CRL) checks to return "`issuer not found in trusted CAs store`" even though the issuer certificate is present.

PingFederate 11.0 (December 2021)

New features and improvements in PingFederate 11.0.

New features and enhancements

PingOne LDAP Gateway datastore

New PingOne

PingFederate in the cloud can now connect to on-premise directory servers through the PingOne LDAP gateway. This new capability reduces the complexity of moving to the cloud, while maintaining connectivity to on-premise end-user data.

PingOne unified admin integration

New PingOne

Administrators can now open the PingOne unified admin from any configuration window in the PingFederate administrative console. To activate the new Home icon, enter the PingOne region and the environment ID in the `run.properties` file.

Management of configuration encryption keys

New

PingFederate maintains a set of configuration encryption keys to encrypt sensitive configuration information provided by the administrators and decrypt them later as needed. While we continue recommending customers to protect their configuration encryption keys by AWS KMS or custom solutions based on the PingFederate SDK (the `MasterKeyEncryptor` interface), we are introducing two enhancements in this area.

- Key rotatation: Administrators or key-management processes can now insert a new configuration encryption key into the system with one click in the administrative console or a single administrative API request. Once rotated, PingFederate starts using this new encryption key when it needs to encrypt sensitive configuration data.
- Re-encryption of configuration data: Version 11 also comes with a new `configkeymgr` command-line utility. Administrators can optionally scan, review, re-encrypt, and delete older configuration encryption keys in their systems. Furthermore, administrators can now choose to re-encrypt sensitive information when importing an archive from a different environment; this is most useful when administrators do not want to share configuration encryption keys between the two environments.

Secret Managers

New

The new Secret Managers support allows customers to store certain credentials, such as data store credentials, in external secret management systems and have PingFederate retrieve them as needed. It helps customers comply with internal IT policies or meet and exceed their industry standards. Version 11 integrates out-of-the-box with CyberArk Credential Provider. Customers can also develop custom solutions based on the PingFederate SDK (the `SecretManager` interface), to connect to other secret management systems.

FAPI 1 Advanced Final certifications

New

Ping Identity remains a solid contributor to the financial-grade API initiatives from the OpenID Foundation. We're proud that PingFederate is a certified implementation of various FAPI 1 Advanced Final profiles, including all profiles under Australia CDR and UK Open Banking and four profiles under Brazil Open Banking. Deploy Open Banking solutions with confidence and rest assured that we will continue to invest in OAuth, OpenID Connect, and FAPI specifications. For more information about OpenID certifications, visit https://openid.net/certification/#FAPI_OPs.

Flexibility in ID token issuance

New

When processing an OpenID Connect hybrid flow, in addition to issuing an ID token from the token endpoint, PingFederate may also return an ID token from the authorization endpoint, depending on the requested response type. Administrators now have the flexibility to separate these two ID token issuances and configure their fulfillment differently. These enhancements allow our customers to comply with the regulatory requirements and open standards set by the Australian CDR and FAPI specifications.

Encrypted request objects

New

PingFederate now supports encrypted request objects that OAuth clients send to its Authorization endpoint and the Pushed authorization requests endpoint. As needed,

administrators can make encrypted request objects mandatory. This new capability further secures the confidentiality of authentication request parameters.

Authorization server issuer identification

New

The OAuth 2.0 Authorization Server Issuer Identification draft specification intends to mitigate the scenario where mix-up attacks are a potential threat to all OAuth clients interacting with multiple authorization servers. As needed, administrators can enable this optional capability.

Better private key JWT validation

New

In the context of OAuth client authentication, when processing private key JWTs from applications, PingFederate now ensures that the issuer (`iss`) claim value matches the client ID. This enhancement removes the need to use issuance criteria to enforce this validation requirement.

Message customization in OIDC IdP connection

New

PingFederate 11 can now take the request parameters from the SAML 2.0 SP or the OpenID Connect relying party (OIDC RP) into account when building its OIDC authentication request to the third-party OpenID Provider (OP). This capability allows administrators to selectively configure the values in the outbound OIDC authentication requests if their use cases or the third-party OPs have the need to gather more information from the originating SP or RP.

Multi-valued attribute format

New

Administrators can optionally indicate that PingFederate should always return an array for an attribute value regardless of whether the attribute contains one or multiple values. This

flexibility simplifies the logic required to consume attribute values from access tokens or ID tokens.

Streamlined initial setup experience

New

We're pleased to introduce a brand new initial setup experience, where administrators can finish their initial setup in as little as four steps, rapidly making our rock-solid capabilities available after starting PingFederate for the first time.

Individual policy management by API

New

Administrators can now focus solely on one policy without including other policies as part of the API request when managing an individual authentication policy through the administrative API. This simplification improves the API experience and eliminates the risk of making unexpected changes in other authentication policies.

Console heartbeat

New

Monitoring the status of the console node is now more straightforward with the addition of the `/pf/heartbeat.ping` heartbeat endpoint to the administrative port. Like its runtime counterpart, the administrative heartbeat endpoint is also capable of returning additional information. If administrators want detailed information in the responses, set the **`pf.heartbeat.system.monitoring`** property to `true` in the `run.properties` file.

Datastore enhancements

New

- We expanded the REST API datastore with HTTP POST support. Administrators can connect to data repositories that prefer or require the HTTP POST method.
- Administrators can add attribute options in their LDAP directory searches. This enhancement expands what PingFederate can retrieve from the directory servers that

support attribute options, PingDirectory being one of them.

- When configuring an LDAP search filter that uses one or more variables, an administrator can optionally specify default values for them, most useful in the scenarios where these variables may not contain any values at runtime.

Migration of templates

New

Our upgrade tools now copy customized default templates from the previous installation to the new one. This improvement preserves the end-user experience and branding, making it easier to verify and move forward with version 11 and beyond.

New configuration for dynamic discovery settings

New

Previously, administrators could only define dynamic discovery settings to discover cluster membership in the `server/default/conf/tcp.xml` file. Version 11 provides a new configuration file for these settings, `jgroups.properties` in the `bin` directory. This new approach streamlines future upgrade experiences. For new installations, we recommend defining dynamic discovery settings in the `jgroups.properties` file. While upgraded environments will continue to look for dynamic discovery settings from the `tcp.xml` file, we recommend performing a one-time migration to ease the upgrade experiences in the future.

Email ownership verification by OTP

New

For customer identities, in addition to email ownership verification by one-time link, administrators can now enable email ownership verification by one-time passcode (OTP). This new option offers a modern verification experience. It also helps customers who prefer not to send hyperlinks via email to their consumers.

Request context to authentication API applications

New

Administrators can optionally configure PingFederate to pass contextual information, such as the OAuth client ID or tracked HTTP parameters, from the sign-on requests to the authentication API applications. This allows developers to build applications that offer tailored experiences and satisfy branding requirements from their organizations based on contextual information from the sign-on requests.

Kerberos authentication improvement

New

Administrators can now ensure Kerberos authentication remains functional for service tickets associated with older Kerberos service account passwords after updating the **Domain/Realm Password** field with a new password in PingFederate. This optional capability increases productivity because workforce identities are no longer required to restart their Windows sessions in order to authenticate via Kerberos.

Contextual information in Session Management API responses

New

The Session Management API now includes IP address and User-Agent information in its responses. Clients with access to this API can learn more about their users and provide suitable offerings based on this new insight.

Security enhancements

New

- PingFederate now supports Amazon EC2 Instance Metadata Service version 2 (IMDSv2) when AWS_PING is the chosen dynamic discovery method. No PingFederate configuration changes are required, and IMDSv1 remains supported.
- PingFederate now records administrative timed-out events in the administrator audit log (`admin.log`).
- The **Change Password** and **Password Reset** end user-facing pages now time out after 30 minutes. This is the new default behavior for new and upgraded installations. As

needed, administrators can configure a different **Password Update Timeout** value per HTML Form Adapter instance to suit the needs of their organizations.

Other improvements

New

- PingFederate now includes HTTP/2 support for inbound requests for better performance.
- Administrators can optionally configure PingFederate to mask values obtained from tracked parameters in the server log. Look for the `MaskTrackedParams` setting in the `org.sourceid.saml20.domain.mgmt.impl.TrackedHttpParamManagerImpl.xml` file.
- Administrators are free to enable the refresh token grant type independently on a per-client basis regardless of whether session validation is enabled in any Access Token Managers.
- Administrators can optionally configure PingFederate to redirect end-users back to the **Sign On** page after successfully updating their soon-to-expire password as part of their SSO requests.
- The **Reuse Existing Persistent Access Grants for Grant Types** authorization server setting is now overridable per client.
- PingFederate now supports RSAES OAEP using SHA-256 and MGF1 with SHA-256 (RSA-OAEP-256) when minting outbound ID tokens or processing inbound encrypted request objects
- Administrators can optionally restrict access to the redirectless mode per authentication API application. Additionally, administrators can further limit each application to an OAuth client to improve security around the redirectless mode of the authentication API.
- We upgraded the framework of our administrative API documentation to Swagger 2.0.
- PingFederate now preserves line breaks and indentations of OGNL expressions.
- The following templates now share the following Velocity template variables, which makes branding end-user experiences easier.

Templates	Variables
◦ `identifier.first.template.html` ◦ `html.form.login.challenge.template.html` ◦ `html.form.login.template.html` ◦ `html.form.message.template.html` ◦ `html.form.password.expiring.notification.template.html`	◦ `$client_id` - The ID of the OAuth client used by the request ◦ `$entityId` - The entity ID of the SP connection used by the request ◦ `$connectionName` - The name of the SP connection used by the request ◦ `$baseUrl` - The base URL of PingFederate instance ◦ `$adapterId` - The IdP adapter ID used by the request ◦ `$spAdapterId` - The SP adapter ID used by the request

- Updated the following bundled components and third-party dependencies:
  - Jetty 9.4.44
  - JGroups 4.2.16
  - jose4j 0.7.9
  - Log4j 2.16.0
  - PingFederate Agentless Integration Kit 2.0.4
  - PingID Integration Kit 2.15.0
  - PingOne Integration Kit 2.4.1
  - Spring Framework 5.3.5

Resolved issues

Cluster dynamic OAuth/OpenID Connect keys

Fixed PF-20709

Resolved an issue that sometimes caused a cluster's dynamic OAuth/OpenID Connect keys to fail to synchronize when a node restarts.

Provisioning

Fixed PF-27519

Resolved an issue that prevented a PingFederate provisioner from using a group of GUIDs as the source to detect new and removed records.

Configuring the `favicon.ico` URL

Fixed PF-28074

Now PingFederate correctly applies customizations of `response-header-runtime-config.xml` to the `favicon.ico` URL.

Retrieving OAuth clients from Oracle databases

Fixed PF-28842

Reduced the time it takes for PingFederate to retrieve OAuth clients from Oracle databases.

Unnecessary dependency error banners

Fixed PF-29189

Unnecessary dependency error banners no longer appear in the administrative console when you use the administrative API to modify selectors or service provider adapters.

Localizing end user messages from the authentication API

Fixed PF-29202

Now you can localize end user messages from the authentication API for registration failure scenarios.

Device authorization flow using IdP connection OAuth attribute mapping

Fixed PF-29294

Resolved an issue that stopped PingFederate from completing a device authorization flow when using IdP connection OAuth attribute mapping.

Multiple Sign-On Delay template redirects

Fixed PF-29318

When a proxy is in front of PingFederate, the Multiple Sign-On Delay template now redirects to the correct port.

Logging `XMLCipher::decryptElement` called without a key and unable to resolve

Fixed PF-29352

As a service provider (SP), when PingFederate can't decrypt an assertion using the primary encryption certificate, it now logs the following message at the WARN level instead of the ERROR level: "`XMLCipher::decryptElement called without a key and unable to resolve`".

Security vulnerability

Fixed PF-29381

Resolved a potential security vulnerability caused by web server URI mishandling.

Response headers for `/pf-ws` and `/pf-scim` endpoints

Fixed PF-29392

Introduced the ability to add response headers to the `/pf-ws` and `/pf-scim` endpoints.

Upgrade utility

Fixed PF-29470

Fixed the upgrade utility so that, in non-interactive mode, it retains cipher related settings that are different from the default settings in the source version. PingFederate changes to new default settings on upgrade only if the settings have not been changed from the defaults in the source install.

Custom template specified for the HTML Form Adapter

Fixed PF-29509

Resolved an issue that caused PingFederate to render the default `forgot-password-error.html` template instead of the custom template specified in the **Password Reset Error Template** field for the HTML Form Adapter.

Partial matches for resource URIs with OAuth 2.0 Token Exchange

Fixed PF-29668

Resolved an issue that prevented the use of partial matches for resource URIs with OAuth 2.0 Token Exchange and produced the error message: "`Unable to find a token generation policy instance to issue a token`".

Adding attributes to data source lookups

Fixed PF-29795

Now, when administrators add an attribute to a data source lookup but do not use the attribute anywhere, such as for contract mapping or issuance criteria, the attribute persists in the administrative console and API.

Microsoft Active Directory LDIF script for persistent grant storage

Fixed PF-29847

The Microsoft Active Directory LDIF script for persistent grant storage now creates an index for the `accessGrantGuid` attribute.

Notification publisher

Fixed PF-29870

Resolved the following notification publisher issues:

- When the SMTP server queues a message but has not sent it yet, the log now indicates that the message was queued, not that it was sent.
- PingFederate now respects the **Connection Timeout** setting for the notification publisher's SMTP server.
- Deprecated the **Retry Attempt** and **Retry Delay** fields for the notification publisher's SMTP server and removed them from the administrative console. PingFederate can still handle API configurations with those fields but they do nothing.

Target resources that don't start with `http://` or `https://`

Fixed PF-30002

Now target resources that don't start with `http://` or `https://` are also available for mapping and issuance criteria.

Response code for an invalid transport method

Fixed PF-30039

Now various endpoints return `400 Bad Request` instead of `500 Internal Server Error` when they receive requests with an invalid transport method. For example, calling the ACS endpoint with a `GET` instead of a `POST` now returns `400 Bad Request`.

Custom IDP adapters that use the class for filterable dropdown controls

Fixed PF-30232

The administrative console no longer shows an error message when you try to create an instance of a custom IDP adapter that uses the class for filterable dropdown controls, `ConnectionSelectionFieldDescriptor`.

Memory usage during certificate revocation list (CRL) parsing

Fixed PF-30272

Reduced memory usage during certificate revocation list (CRL) parsing, which speeds up CRL retrieval and avoids memory exhaustion in the case of very large CRLs.

Known issues and limitations

Administrative console and administrative API

Issue

- /sp/idpConnections: For identity provider (IdP) connections, the administrative API connection support is limited to Browser SSO, WS-Trust STS, and OAuth Assertion Grant connections. As a result, when updating an IdP connection using the administrative API, it is possible to lose inbound provisioning settings previously configured using the administrative console.
- /bulk: Only resource types currently supported by the administrative API are included in the exported data. Resources not yet supported include:
  - Identity Store Provisioners
  - Inbound provisioning settings from IdP connections
  - SMS Provider settings
- Previously, the administrative API did not accurately reflect a **Persistent Grant Max Lifetime** setting of 29 days (or shorter) with the selection of the **Grants Do Not Timeout Due To Inactivity** option. As a result, if you have configured such OAuth authorization server settings and have generated a bulk export in version 10.0 through 10.0.2, we recommend that you re-generate a new bulk export after upgrading to version 10.0.3 (or a more recent version). The newly exported data does not contain the aforementioned flaw, and you can safely import it to version 10.0.3 (or a more recent version).
- When enabling mutual TLS certificate-based authentication, administrators often configure a list of acceptable client certificate issuers. When an administrator uses a browser to access the console or the administrative API documentation, PingFederate returns to the browser the list of acceptable issuers as part of the TLS handshake. If the browser's client certificate store contains multiple client certificates, the browser often presents to the user only the certificates whose issuer matches one of the acceptable issuers. However, when PingFederate runs in a Java 11 environment,

Chrome presents to the administrator all its configured client certificates, regardless of whether the issuer matches one of the acceptable issuers or not.

- Prior to toggling the status of a connection with the administrative API, an administrator must ensure that any expired certificates or no longer available attributes are replaced with valid certificates or attributes; otherwise, the update request fails.
- When creating or updating a child instance of a hierarchical plugin, the administrative API retains objects with an `"inherited": false` name/value pair (or without such name/value pair altogether), ignores those with a value of `true`, and returns a 200 HTTP status code. No error messages are returned for the ignored objects.
- Using the browser's navigation mechanisms (for example, the **Back** button) causes inconsistent behavior in the administrative console. Use the navigation buttons provided at the bottom of windows in the PingFederate console.
- Using the PingFederate console in multiple tabs on one browser might cause inconsistent behavior which could corrupt its configuration.
- If authenticated to the PingFederate administrative console using certificate authentication, a session that has timed out might 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 back to the administrative console after authentication is complete. Similar behavior applies for certificate authentication, in principle. However, because the browser might automatically resubmit the certificate for authentication, the browser might redirect to the administrative console and not the login page.

TLSv1.3

Issue

For Java versions that don't support TLSv1.3 (meaning versions earlier than 8u261), PingFederate fails on start up with a `NoSuchAlgorithmException` exception. To resolve this error, remove `TLSv1.3` from the following settings in the `run.properties` file:

- **`pf.tls.client.protocols`**
- **`pf.tls.runtime.server.protocols`**
- **`pf.tls.admin.server.protocols`**

TLS cipher suite customization

Issue

PingFederate's TLS cipher suites can be customized by modifying `com.pingidentity.crypto.SunJCEManager.xml` (or a similarly-named file if BCFIPS or a hardware security module (HSM) is configured). After updating the file and replicating, all cluster nodes must be restarted for the change to take effect.

Updating Java 8 to Java 11

Issue

Updating Java version 8 to version 11 results in an error when PingFederate is already installed and running. To work around this issue, uninstall and reinstall the PingFederate Windows service by running the `UninstallPingFederateService.bat` and `InstallPingFederateService.bat` files located in `<pf_install>/pingfederate/sbin/wrapper`.

Hardware security modules (HSM)

Issue

- For Entrust HSMs or AWS CloudHSM, PingFederate must be deployed with Oracle Server JRE 8 or Amazon Corretto 8.
- For Entrust HSMs, it is not possible to use an elliptic curve (EC) certificate as an SSL server certificate.
- For keys stored in Thales HSMs, JWT token decryption fails when using RSAES OAEP with AES-CBC-192 or AES-CBC-256. This issue only arises if PingFederate is configured with static OAuth and OpenID Connect keys and is consuming a token encrypted with one of these keys.
- When PingFederate is configured in hybrid mode with a Thales HSM, it is not possible to export a locally-stored EC key pair.
- When PingFederate is configured in hybrid mode with a Thales HSM, JWT token decryption using ECDH-ES may fail. This issue only arises if PingFederate is configured

with static OAuth and OpenID Connect keys, a static key is stored locally, and PingFederate is consuming a token encrypted with this key.

- TLS 1.3 is not currently supported with any HSM.

SSO and SLO

Issue

- When consuming SAML metadata, PingFederate does not report an error when neither the `validUntil` nor the `cacheDuration` attribute is included in the metadata. Note that PingFederate does reject expired SAML metadata as indicated by the `validUntil` attribute value, if it is provided.
- The anchored-certificate trust model cannot be used with the SLO redirect binding because the certificate cannot be included with the logout request.
- 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.

Composite Adapter configuration

Issue

SLO is not supported when users are authenticated through a Composite Adapter instance that contains another instance of the Composite Adapter.

Self-service password reset

Issue

Passwords can be reset for Microsoft Active Directory user accounts without the permission to change password.

OAuth

Issue

PingFederate does not support a case-sensitive naming convention for OAuth client ID values when client records are stored in a directory server. For example, after creating a client with an ID value of `sampleClient`, PingFederate does not allow the creation of another client with an ID value of `SampleClient`.

Although it's possible to create clients using the same ID values with different casings when client records are stored in XML files, a database server, or custom storage, we recommend not doing so to avoid potential record migration issues.

Customer identity and access management

Issue

Some browsers display a date-picker user interface for fields that have been designed for date-specific inputs. Some browsers do not. If one or more date-specific fields are defined on the registration page or the profile management page (or both), end users must enter the dates manually if their browsers do not display a date-picker user interface for those fields.

Provisioning

Issue

- 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.
- The **`totalResults`** value in SCIM responses indicates the number of results returned in the current response, not the total number of estimated results on the LDAP server.

Logging

Issue

- 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, the **`USER_KEY`** attribute will not be masked in the server logs. Other persistent grant attributes will be masked.

- Even if a source attribute has been configured for masking in an IdP adapter and the source attribute is mapped as the adapter's unique user key, the user key attribute is not masked in the server or audit logs.

Database logging

Issue

- 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, the `USER_KEY` attribute will not be masked in the server logs. Other persistent grant attributes will be masked.
- Even if a source attribute has been configured for masking in an IdP adapter and the source attribute is mapped as the adapter's unique user key, the user key attribute is not masked in the server or audit logs.

RADIUS NAS-IP-Address

Issue

The RADIUS NAS-IP-Address is only included in Access-Request packets when the `pf.bind.engine.address` is set with an IPv4 address. IPv6 is not supported.

Deprecated features

Microsoft Internet Explorer 11

Info

Ping Identity commits to deliver the best experience for administrators and users. As we continue to improve our products, we encourage our customers to migrate off of Microsoft Internet Explorer 11. Starting with PingFederate 11.0, Internet Explorer 11 is no longer included in the PingFederate qualification process for administrators or users. For a list of supported browsers, see System requirements.

Configcopy tool, Connection Management Service, SSO Directory Service

Info

As of PingFederate 10.2, these features have been deprecated and will be removed in a future release.

Oracle Directory Server Enterprise Edition

Info

As Oracle ended its Premier Support for Oracle Directory Server Enterprise Edition (ODSEE 11g) in December 2019, we no longer include ODSEE as part of the PingFederate qualification process (starting with PingFederate 10.2). We continue to qualify against Oracle Unified Directory and other supported directory servers. For a full list, see System requirements.

SNMP

Info

Starting with PingFederate 10.2, monitoring and reporting through the Simple Network Management Protocol (SNMP) has been removed.

Roles and protocols

Info

Starting with PingFederate 10.1, roles and protocols are always enabled and no longer configurable through the administrative console and API.

S3_PING discovery protocol

Info

Starting with PingFederate 10.1, the S3_PING discovery protocol has been deprecated. Customers running on AWS infrastructure should instead use NATIVE_S3_PING.

Red Hat Enterprise Linux install script

Info

Starting with PingFederate 10.0, the Red Hat Enterprise Linux install script is no longer available. To install PingFederate 10.0 for Linux, you must download and extract the product distribution `.zip` file.

Previous releases

Find information about enhancements and issues resolved in previous releases of PingFederate in the Ping Documentation Archive.