

# PingFederate Express<sup>TM</sup>

Version 1.0

For Apache HTTP Servers

## User Guide

**Ping**Identity<sup>®</sup>

© 2009 Ping Identity® Corporation. All rights reserved.

Version 1.0  
August, 2009

Ping Identity Corporation  
1099 18th Street, Suite 2950  
Denver, CO 80202  
U.S.A.

Phone: 877.898.2905 (+1 303.468.2882 outside North America)  
Fax: 303.468.2909  
Web Site: <http://www.pingidentity.com>

### **Trademarks**

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

### **Disclaimer**

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

# Contents

- Introduction.....4**
  - Intended Audience .....4
  - System Requirements.....4
  - Processing Overview .....5
- Installation and Setup .....7**
  - Testing the PingFederate Express Installation .....8
- Multiple Server Deployment .....8**
  - Deploying PingFederate Express in a Cluster .....9
- Supplemental Information .....10**
  - SAML Profile Support.....10
  - Certificate Maintenance .....11
  - Assertion Replay Prevention.....11

# Introduction

PingFederate Express™ is a lightweight SAML (Security Assertion Markup Language) endpoint providing secure Internet single sign-on (SSO) to Web applications or other resources hosted by Apache HTTP Servers. Based on PingFederate®, Ping Identity's flagship Internet-identity security platform, PingFederate Express provides a quick and easy way for a Service Provider (SP) to process SAML assertions sent from an Identity Provider (IdP) partner who is using PingFederate.

To simplify deployment at your site, the configuration for PingFederate Express is provided by your IdP partner in a separate configuration ZIP file containing information about the partner's PingFederate deployment. The automated installation uses this information to configure PingFederate Express quickly, creating a secure end-to-end connection back to the IdP for SSO.

For information about PingFederate and SAML, refer to the Ping Identity Web site ([www.pingidentity.com](http://www.pingidentity.com)) and the SAML-standards Web site ([www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=security](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security)). Limited information, relevant to PingFederate Express, is also available at the end of this document (see “[Supplemental Information](#)” on page 10).

## Intended Audience

This document is intended for system administrators with experience in the configuration and maintenance of Linux/Unix and Apache Servers. Knowledge of networking and user-management configuration is assumed. Please consult the documentation provided with your server tools if you encounter any difficulties in areas not directly associated with PingFederate Express.

Knowledge of PingFederate or SAML specifications is *not* required.

## System Requirements

PingFederate Express is designed and supported exclusively for Apache 2.2, installed on Red Hat Enterprise Linux (RHEL) 5 via the Red Hat Package Manager (RPM). PingFederate Express supports both 32-bit and 64-bit RHEL 5 operating systems and the pre-fork multi-processing module.

The following system requirements must be satisfied in order to implement PingFederate Express:

- RHEL 5
- Apache HTTP Server 2.2, installed via RPM

---

**Note:** The PingFederate Express RPM assumes the default Apache directory structure set up by the Apache-installation RPM, which also installs the Apache Server proxy and the `openssl` and `zlib` libraries required for this installation.

---

- Sun Java JDK/JRE 1.5 or 1.6 installed on the Apache Web server machine

---

**Important:** The `JAVA_HOME` environment variable must be set to the Sun JDK/JRE directory.

---

## Additional Prerequisites

- A PingFederate Express configuration file (`pf-express-config.zip`) generated by the IdP partner
- A valid PingFederate Express license file (`pf-express.lic`)

## Processing Overview

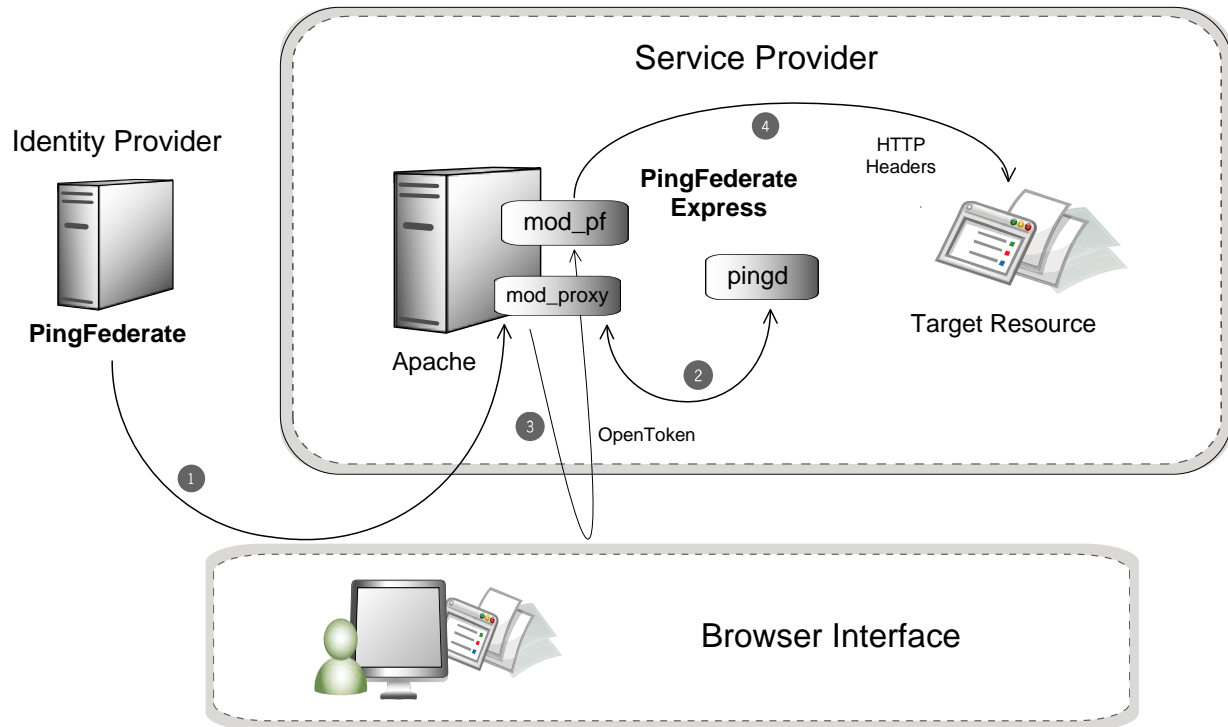
PingFederate Express acts as a SAML Web filter in front of an application (or any externally protected resource) protected by Apache. Operationally, PingFederate Express uses the Apache Server's native proxy module in conjunction with the installed SAML service (`pingd`) which validates and translates a SAML assertion into a secure session token (called `OpenToken`). The token is then verified by a PingFederate Express Apache Agent module (`mod_pf`), which provides access to the requested resource.

The basic responsibility of PingFederate Express is to filter requests to determine whether they are for a protected resource dependent on IdP authentication. If so:

- PingFederate Express checks to see if an `OpenToken` session is already available and if the session parameters meet session policy.
- If an `OpenToken` session exists and the session meets policy for the request, PingFederate Express passes the request through to the application.

If an `OpenToken` session does not exist, or if the existing session does not meet the session policy for the request, PingFederate Express redirects the user's browser to the Identity Provider (IdP) for authentication. After authentication, PingFederate Express validates the SAML assertion, and if valid, redirects the user back to the protected resource with a valid `OpenToken` session.

The following figure illustrates an IdP-initiated SSO scenario, showing the request flow and how PingFederate Express validates the SAML assertion, wraps attributes from the assertion into a secure session token, and passes the token to Apache.



## Processing Steps

1. A user clicks a link that initiates an SSO transaction to the SP partner application. The IdP partner authenticates the user (if not already done), and the PingFederate IdP server redirects the request, containing a SAML 2.0 assertion, back through the user's browser to the SP site.
2. The `mod_proxy` Apache module forwards the request to the `pingd` SAML service, which processes the assertion and creates an `OpenToken` for the user, including any configured attributes. The service then includes the `OpenToken` in a redirect back to `mod_proxy`.
3. The `mod_proxy` module redirects the user's browser to the protected URL with the new `OpenToken`.
4. The `mod_pf` Apache module, configured to protect the URL, verifies the `OpenToken` and grants access to the protected resource. The SAML subject and any attributes from the SAML assertion are exposed to the resource as HTTP request headers.

# Installation and Setup

Installation and setup for PingFederate Express involves:

1. Installing the PingFederate Express RPM file.
2. Installing a valid PingFederate Express license file.
3. Executing the configuration script to configure PingFederate Express based upon the IdP-partner configuration file.

---

**Important:** Install, configure, and run PingFederate Express as `root`.

---

## To install and configure PingFederate Express:

1. As `root`, run the following command to install PingFederate Express:

```
rpm -ivh pingfederate-express-1.0.rpm
```

The RPM performs the following steps:

- Installs `pingd` SAML service
- Installs Apache OpenToken Agent (`mod_pf`)
- Installs the OpenToken library (`libopentoken`)
- Checks `OpenSSL` dependencies
- Checks `Apache` dependencies
- Checks `zlib` dependencies

If Security-Enhanced Linux (SELinux) is enabled, the RPM also:

- Sets permissions for `mod_pf` and `libopentoken` to execute in the `httpd` process context
- Allows `mod_proxy_http` to make outbound network connections

2. Copy the license file `pf-express.lic` into the directory:

```
/opt/pingd/resources
```

---

**Note:** The `/opt/pingd/resources` directory does not exist until after the PingFederate Express RPM is installed.

---

3. Ensure the IdP-generated configuration file `pf-express-config.zip` is available on the file system.
4. As `root`, execute the configuration script from the `/opt/pingd/bin` directory to configure PingFederate Express using the following command.

```
./configure.sh <path_to_pf-express-config.zip> [-v]
```

The configuration script prompts for confirmation (or modification) of defaulted entries for required parameters.

---

**Note:** The IdP partner-generated configuration file may contain a CA certificate used for validating the digital signature of inbound identity assertions. You will need to confirm that you trust this certificate to be imported into your root CA store. For more information, see [“Certificate Maintenance”](#) on page 11.

---

The PingFederate Express configuration script performs the following steps:

- Configures the `pingd` SAML service
- Configures the `OpenToken` Apache module
- Generates an `OpenToken` encryption key used for security with `pingd`
- Configures the Apache Proxy Module `httpd-express.conf` file in `/etc/httpd/conf.d`

You can use the optional `-v` switch to see verbose details in the terminal window as the script configures each component.

---

**Note:** The `configure.sh` script can be run again, as needed, at any time (for example, to change parameters or import certificates).

---

5. Start the `pingd` SAML service (as root):

```
service pingd start
```

6. Start (or restart) Apache `httpd` service:

```
service httpd start
```

## Testing the PingFederate Express Installation

PingFederate Express includes a protected start page for testing to verify the installation and configuration. The start page initiates an SSO transaction with the IdP partner, and if successful, displays the HTTP headers that PingFederate Express exposes to an underlying application. These headers correspond to attributes from the SAML assertion.

Access the PingFederate Express protected start page at:

<http://<apache-server>/<protected-path>/?cmd=PingStartPage>

---

**Caution:** This feature is for testing and demonstration only. For security reasons, an administrator should disable the page in a production environment. To disable the page, comment out the `PingFederateStartPageURL` property in the file `<apache_home>/conf/mod_pf.conf`.

---

## Multiple Server Deployment

PingFederate Express supports server clustering. Clustered deployments require the use of at least one load balancer, fronting multiple Apache Servers. When a client accesses the load balancer’s virtual IP, the balancer routes the request to one of the servers in the cluster. User-session states and configuration data are shared among the PingFederate Express instances, or *nodes*, enabling them to process SSO requests as a single entity.

Note that the PingFederate Express software distribution does not contain a load balancer. Numerous hardware or software products are available commercially, including free downloads.

---

**Note:** The `pingd` SAML service is preconfigured to use UDP multicast for the group communication transport protocol. IP multicasting must be enabled in the network environment.

---

## Deploying PingFederate Express in a Cluster

Follow the procedure below to deploy and configure clustered PingFederate Express nodes.

---

**Important:** Each Apache Server must meet installation requirements (see “[System Requirements](#)” on page 4), except for “Additional Prerequisites”—installation of the license key on all nodes is not required, and the IdP configuration file is not used during additional server installations for clustering.

This procedure assumes that PingFederate Express is already installed and has been started initially on one server (see “[Installation and Setup](#)” on page 7).

---

To configure PingFederate Express in a cluster, for each Apache Web server:

1. As `root`, run the following command to install the PingFederate Express RPM on additional servers:

```
rpm -ivh pingfederate-express-1.0.rpm
```

---

**Note:** Do not execute the PingFederate Express configuration script (`configure.sh`), run during the initial server installation, on the additional servers. The PingFederate Express configuration must be replicated manually to each node as specified in the following steps.

---

2. Copy the following files from the original installation’s `/etc/httpd/conf` directory to the corresponding directory on the other nodes:
  - `agent-config.txt`
  - `mod_pf.conf`
3. Copy the file `httpd-express.conf` from the original installation’s `/etc/httpd/conf.d` directory to the corresponding directory on the other nodes.
4. Copy the file `latest.data.zip` from the original installation’s `/opt/pingd/data/archive` to the following directory on the other nodes:

```
/opt/pingd/data/drop-in-deployer
```
5. On the new nodes, rename the file `latest.data.zip` to:

```
data.zip
```

6. Configure each pingd SAML service node to operate in cluster mode:

For each node (including the original), edit the file:

```
/opt/pingd/etc/pingd.xml
```

Change the value of the system property `pf.operational.mode` from `STANDALONE` to `CLUSTERED_ENGINE`, as shown below in **boldface**.

```
<Call class="com.pingd.SysProp"
name="set"><Arg>pf.operational.mode</Arg><Arg>CLUSTERED_ENGINE</Arg>
</Call>
```

7. For each node, start the pingd SAML service (as root):

```
service pingd start
```

---

**Note:** Ensure that you start the server containing the Express license file first, for it to be pushed to other servers.

---

8. For each node, start (or restart) the Apache httpd service:

```
service httpd start
```

## Supplemental Information

The following sections provide specific information about your PingFederate Express configuration and deployment, concerning details related to SAML specifications and security. This information is not required for installation or initial deployment but rather covers inner workings of the product that you may find helpful.

For more information about SAML, refer to:

[www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=security](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security)

## SAML Profile Support

PingFederate Express supports a specific configuration to facilitate a quick and simplified installation and deployment.

### The configuration supports:

- A single IdP-partner connection
- The SAML 2.0 protocol
- SP-initiated SSO using the redirect/POST profile
- IdP-initiated SSO using the POST profile
- Digital signatures on SAML response messages (which contain assertions)

### The configuration *does not* support:

- Digital signatures on SAML Authentication Requests for SP-initiated SSO (not required by specifications)
- User Provisioning

- Security Token Service for Web Services, using WS-Trust specifications
- Single Logout
- Other SAML versions and specifications, including profiles and bindings using the back channel

These and other configuration options are available by converting your deployment to the enterprise version of PingFederate.

## **Certificate Maintenance**

The SAML specification requires that the SAML response sent to the SP partner must be digitally signed, when sent via HTTP POST (the PingFederate Express profile). To enable PingFederate Express to verify digital-signatures, the IdP's signing certificate is included in the configuration file generated by the IdP.

If the IdP signing certificate is issued by a trusted third-party CA, PingFederate Express employs a dynamic trust model to avoid any service interruption when a CA-signed certificate expires. With this trust model, the IdP public certificate is always embedded in incoming SAML messages. PingFederate Express verifies that the certificate's Subject DN matches the previously configured certificate, and then uses the embedded certificate for signature checking. Therefore, no configuration changes are needed at your site when your IdP partner uses a renewed or new CA-signed certificate, as long as the embedded certificate has the same Subject DN as the expired certificate.

For self-signed certificates, PingFederate Express uses the statically configured certificate to validate the digital signature. Certificate maintenance must be coordinated between the IdP and SP to avoid any service interruption when the self-signed certificate expires.

## **Assertion Replay Prevention**

The SAML standards specify that when an SP receives assertions via the POST binding, the SP should keep track of that assertion for the duration of its validity to ensure that it is not replayed (that is, intercepted by a third party and reposted). PingFederate Express provides an Assertion-Replay Prevention Service that is enabled by default in both stand-alone and clustered modes. In clustered mode, SAML assertion tracking is shared among all PingFederate Express nodes, therefore any replay attempt routed to a different PingFederate Express node in the cluster would be thwarted.