

PingFederate[®]

Upgrade Utility

Version 7.2.1

User Guide



© 2014 Ping Identity® Corporation. All rights reserved.

PingFederate Upgrade Utility *User Guide*
Version 7.2.1
August, 2014

Ping Identity Corporation
1001 17th Street, Suite 100
Denver, CO 80202
U.S.A.

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

Trademarks

Ping Identity, the Ping Identity logo, PingFederate, PingOne, PingConnect, and PingEnable are registered trademarks of Ping Identity Corporation ("Ping Identity"). All other trademarks or registered trademarks are the property of their respective owners.

Disclaimer

The information provided in this document is provided "as is" without warranty of any kind. Ping Identity disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Ping Identity or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Ping Identity or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Document Lifetime

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

From the Web site, you may also download and refresh this PDF if it has been updated, as indicated by a change in this date: **August 28, 2014.**

Contents

Upgrade Introduction	4
Upgrading PingFederate	4
Step One -- Preparation	5
Step Two -- Run the Upgrade Utility	5
Step Three -- Copy Any Customized Files or Settings	8
Known Limitations	9

Upgrade Introduction

This Upgrade Utility is a command-line tool that automatically migrates existing PingFederate 6.x (and higher) configurations to the current version. The tool first installs the new distribution and then copies over files or property values from the previous installation.

As an option, you can run the utility with a *custom* switch that allows you to choose whether to override any new system defaults or to install newer versions of bundled adapters (see [Using Custom Mode](#) on page 7).

Note: The Upgrade Utility does *not* affect the existing installation of PingFederate. After you complete the steps in this Guide and then test and deploy the new PingFederate in production, we recommend that you remove the previous installation.

The Upgrade Utility creates a detailed log showing what files and settings are affected during the upgrade.

Intended Audience

The PingFederate Upgrade Utility and this document are intended for system administrators with significant knowledge of the current PingFederate configuration and enterprise deployment.

Upgrading PingFederate

Fully upgrading your existing PingFederate installation involves initial preparation before running the Upgrade Utility. Then afterward, some manual copying may be needed for customized files or supporting Web-application deployments.

The Upgrade Utility is located in the `/bin` directory of the distribution ZIP as either a batch file (for Windows installations) or a shell script (for Linux/Unix installations).

Note: The Upgrade Utility does not migrate OAuth client configurations created prior to PingFederate version 6.8. Reconfigure clients manually using either the PingFederate Client Management screen or the REST-based Web Service for OAuth client management (see Client Management in the PingFederate *Administrator's Manual*).

If you have a large number of OAuth Clients configured, contact Ping Identity [Support](#) for migration assistance (www.pingidentity.com/support).

Important: As of PingFederate version 6.11, security updates related to XML encryption may affect existing partner connections, requiring manual reconfiguration or partner notification. For more information, see Upgrade Considerations in the PingFederate Release Notes.

Step One -- Preparation

Before running the Upgrade Utility:

1. If you have not already done so, download the current version of PingFederate and obtain a new license key.
2. If you have not recently updated the Java SE Development Kit (JDK) to version 7 or 8 on your PingFederate host machine(s), you must do so.

Note: When you upgrade the JDK, be sure to modify the previously defined paths for the system `JAVA_HOME` and `PATH` environment variables. (For more information, see *Installing the JDK in Getting Started*.)

Important: PingFederate versions prior to 6.7 will not start using Java 7 or 8. If you need to start the previous PingFederate version on the same server after the upgrade, retain the older Java installation and change environment variables back when needed.

3. (Optional) Complete any unfinished connections (“Drafts”) in the existing PingFederate administrative console, *if* you want to include them in the migration.

Because they may cause unpredictable errors in the administrative console, connection drafts cannot be moved from one instance of PingFederate to another.

4. Unzip the Upgrade Utility distribution into a directory on the same machine running PingFederate.
5. If you are upgrading PingFederate in a clustered-server environment, unzip the Upgrade Utility on each PingFederate runtime host.

Note: Start the upgrade on the PingFederate server running the administrative console.

Step Two -- Run the Upgrade Utility

1. Stop the currently installed PingFederate administrative server.
2. From the `pf-upgrade-7.2.1/bin` directory at a system prompt, execute the following command:

On Windows:

```
upgrade <sourcePingfederateRootDir> <outputDir> <pingfederateZip> [-c]
```

On Linux/Unix:

```
./upgrade.sh <sourcePingfederateRootDir> <outputDir> <pingfederateZip> [-c]
```

where:

- `<sourcePingfederateRootDir>` is the full or relative path of the base directory where the existing PingFederate software (`pingfederate/*`) is installed;

Important: The `pingfederate` subdirectory *must* exist by that name for the upgrade utility to function correctly.

- `<outputDir>` is the full or relative path of the directory that will contain the new PingFederate base directory;

- <pingfederateZip> is the full or relative path and file name for the current distribution; and
- -c runs the utility in optional custom mode (see [Using Custom Mode](#) on page 7).

Examples:

```
upgrade c:\sso\pingfederate-6.0.0 c:\sso c:\sso\pingfederate-7.2.1.zip
./upgrade.sh /sso/pingfederate-6.0.0 /sso /sso/pingfederate-7.2.1.zip
```

For version 7.2.1, this command would install the new software into:

```
c:\sso\pingfederate-7.2.1 (on Windows)
/sso/pingfederate-7.2.1 (on Linux/Unix)
```

Note: This directory is referred to in this document as <pf_install>, with subdirectory separators standardized as forward slashes (/).

After a moment, the command window displays messages indicating upgrade progress. The process is complete when this message appears:

```
Upgrade completed with [N] errors and [N] warnings
```

If there are errors, scroll up the command window to see them and correct indicated problems. Errors during the upgrade should be rare but may include such input/output problems as missing or malformed configuration files in the source installation.

The messages, including any errors, are also logged to the Upgrade Utility base directory in the file:

```
upgrade.log
```

Tip: Rerun the Upgrade Utility as many times as needed to correct any problems.

3. Copy the new PingFederate license file, `pingfederate.lic`, into the directory:

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

Tip: Alternatively, you can import the new license via the administrative console at the next step (see *Installing a New License Key in the PingFederate Administrator's Manual*).

4. Start the new PingFederate installation and open the administrative console.
5. Verify configuration settings in the administrative console.

Note: Access the connection management screens and ensure that automatic validation is run on each connection.

6. If you are upgrading a server cluster:
 - a. Stop each server node and run the Upgrade Utility for each PingFederate installation in the cluster.
 - b. Start the *new* installation on each node.

- c. In the administrative console, click **Cluster Management** on the Main Menu.
- d. On the Cluster Management screen, ensure all nodes are shown in the list of IP addresses.
- e. Click **Replicate Configuration**.

Important: The Upgrade Utility *does not* migrate the administrative user-interface (UI) configuration to clustered servers. For more information about cluster management, see the *Server Clustering Guide*.

7. If PingFederate is running as a service, stop the existing service and re-install it (for Windows) or reconfigure it (for Linux/Unix) to use the new PingFederate installation.

For more information, see Installation in *Getting Started*.

8. If applicable, repeat the previous step for each server node in a clustered deployment (update each PingFederate service).

Using Custom Mode

The custom-mode feature (invoked with the `-c` option on the command line) allows administrators to override several newer default security settings (new, depending on which PingFederate version is currently running). In addition, if either of the installed OpenToken and LDAP adapters is out of date, running the tool in custom mode allows you to replace the adapter with the latest version, if applicable.

About Security Defaults

In general, using the new security defaults is highly recommended and should not cause significant issues for most PingFederate installations. The newer default security settings include:

- Disabling weaker cipher suites for both the SUN and LUNA Java Cryptography Extension (JCE) in PingFederate version 6.2 and later. If you want to see which cipher suites are commented out, choose yes (y) when prompted on whether to use the new defaults. Then, after the upgrade is complete, refer to either of the following configuration files in the new installation's `<pf_install>pingfederate/server/default/data/config-store` directory:
 - `com.pingidentity.crypto.SunJCEManager.xml`
 - `com.pingidentity.crypto.LunaJCEManager.xml`
- Disabling SQLFilter as of PingFederate version 6.2.
- Disabling the sending of PingFederate session cookies by way of the unsecure hypertext transfer protocol. As of version 6.5, the session cookie is configured to be sent only using HTTPS.

Upgrading Adapters

Upgrading the OpenToken and LDAP adapters from previous versions is also recommended and will not normally require any follow-on configuration changes. For OpenToken, however, if your existing installation uses a version of the adapter prior to 2.3, upgrading requires minor configuration modifications in the PingFederate console as well as redeployment of the agent configuration file (see OpenToken Adapter Configuration in the PingFederate *Administrator's Manual*).

If you are upgrading from an OpenToken version prior to 2.5.1, we recommend that you redeploy agent configuration files, if applicable, as well as any new agent libraries contained in recent versions of PingFederate integration kits and other plug-ins that use OpenToken.

Note: Starting with PingFederate version 6.6, the LDAP adapter is no longer provided in the product package. However, if this adapter is configured for existing deployments, its JAR file is copied over and the custom-mode option to upgrade older versions is available.

Alternatively, the functionality of the LDAP adapter for an IdP can be replaced by configuring either of two new adapters: HTTP Basic or HTML Form. For more information, see HTTP Basic Adapter Configuration and HTML Form Adapter Configuration in the *PingFederate Administrator's Manual*.

Step Three -- Copy Any Customized Files or Settings

If you have modified any user-facing Velocity templates, you must copy the HTML files over to the new installation manually for each server node (see Customizing User-Facing Screens in the *PingFederate Administrator's Manual*). The templates are located in the directory:

```
<pf_install>/pingfederate/server/default/conf/template
```

Caution: Supporting CSS and image file names were changed as of PingFederate 7.0. For each modified HTML template copied, add .1 to the base name for each CSS file referenced in the header.

Example: `<link rel="..." href="assets/css/screen.1.css" />`

Likewise, add .1 to any references in the copied templates to the installed image files contained in the `assets/images` directory.

Example: ``

Similarly, if you have modified any Web-container configuration settings that need to be carried forward, you must make corresponding changes manually in the new PingFederate deployment. For upgrading PingFederate version 6.9 and higher, you can simply copy over the relevant files from the Jetty configuration directory `<pf_install>/pingfederate/etc`. For existing versions prior to 6.9, first identify any changes made to the JBoss configuration, then make corresponding changes for the newer Jetty configuration.

For example, a commonly modified file prior to version 6.9 might be `jboss-service.xml` located in the directory `<pf_install>/pingfederate/server/default/deploy/jetty.sar/META-INF`. When changes are identified, make the same modifications at corresponding points in either the `jetty-admin.xml` or `jetty-runtime.xml` files located in the new Jetty configuration directory `<pf_install>/pingfederate/etc`.

Known Limitations

- When Browser SSO Profiles and WS-Trust are both selected in an SP connection, IdP Adapter and Token Processor instances mapped to the connection must not share the same Instance ID. If the Instance IDs overlap, before running the Upgrade Utility, create a new IdP Adapter (or Token Processor) instance with a different Instance ID, remove the currently mapped IdP Adapter (or Token Processor) instance from the connection, map the new IdP Adapter (or Token Processor) instance to the connection, complete the rest of the steps to fulfill the attribute contract, and save the connection.
- As of version 6.5, PingFederate supports Thales nShield Connect HSM configurations. If your PingFederate installation is configured in a clustered environment with nShield Connect, you must copy the `<pf_install>/server/default/data/ncipher-kmdata-local` directory to the new installation manually and update the environmental variable `NFAST_KMLOCAL` to point to the new location. For more information, see Additional Steps for Server Clusters in the *Getting Started* guide.
- To avoid overwriting any PingFederate logging customization that may have occurred at your site, the Upgrade Utility determines whether `log4j.xml` has been modified in the existing installation. If so, new features in `log4j.xml` are *not* installed; the tool does not currently support automatic merging of customizations made to the existing logging configuration. (The XML file is located in the `<pf_install>/pingfederate/server/default/conf` directory.) Instead, if the existing file has changed since it was originally installed, the Upgrade Utility copies it to the new installation intact and renames the new configuration file using the current PingFederate version number.

The new configuration file contains several new logging capabilities added between version 6.0 and the current PingFederate version. (Please refer to product Release Notes for version 6.1+ and Managing Log Files in the PingFederate *Administrator's Manual*.) If the Upgrade Utility renames the new `log4j.xml` file, you must merge the two files if you want to retain previous logging changes and also use the new features. Or manually replicate any logging customizations in the new file and use it to replace the old one.

- As of PingFederate 6.2, TLS renegotiation was disabled by default for all HTTPS listeners/connectors. This security update affects only existing partner connections using WS-Trust STS and those making use of inbound mutual SSL/TLS authentication for the SOAP or artifact SAML bindings. In such cases, administrators must manually reconfigure `run.properties` to enable the secondary HTTPS port (see Changing Configuration Parameters in the PingFederate *Administrator's Manual*). In addition, affected connection partners must update their configurations to use the new endpoint.
- The Upgrade Utility does not migrate any data maintained in the PingFederate internal Hypersonic database or any external database. If, for example, SaaS Provisioning is enabled in the new PingFederate instance using the internal database, it is re-initialized from the provisioning source.
- The OGNL library used by PingFederate was upgraded with version 6.4. If you use OGNL expressions, we recommend retesting the expressions using the PingFederate administrative console.