PingFederate®

Atlassian Integration Kit

Version 1.1

User Guide

Ping Identity®

PingFederate Atlassian Integration Kit User Guide
Version 1.1
April, 2016

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: 303.4ste8.2909
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: **April 27, 2016**

Contents

Introduction

The Atlassian Integration Kit (the Kit) enables SSO capabilities for Jira and Confluence. The integration kit requires the use of the Reference ID adapter available as part of the Agentless Integration Kit. The Reference ID adapter is used to pass the user identity information from PingFederate to the specific Atlassian product.

The Kit comes with two components:

1. An Authenticator which utilizes the Atlassian Seraph API to enable SSO for Jira and Confluence.
2. An Atlassian plugin which the administrator uses to configure the Authenticator with the appropriate PingFederate settings.

Intended Audience

This document is intended for system administrators with experience in the configuration and maintenance of IT infrastructure. Knowledge of networking and user-management configuration is assumed. Some exposure to the PingFederate administrative console may be helpful.

Note: If you encounter any difficulties with configuration or use of the Kit, please try reaching the Ping Identity Support Center (`ping.force.com/Support`).

ZIP Manifest

The distribution ZIP file for the Kit contains the following:

- `ReadMeFirst.pdf` – contains links to this online documentation
- `/legal` – contains the legal information:
  - `Legal.pdf` – copyright and license information
- `/dist` – contains libraries needed to run the Kit:
  - `pf-authenticator-1.1.x.jar`
  - `pf-authenticator-plugin-1.1.x.jar`
- `/dist/jira7` – contains library and support file needed to run the Kit within Jira 7:
  - `pf-authenticator-jira7-1.1.x.jar`
  - `login.jsp`
  - `default.jsp`

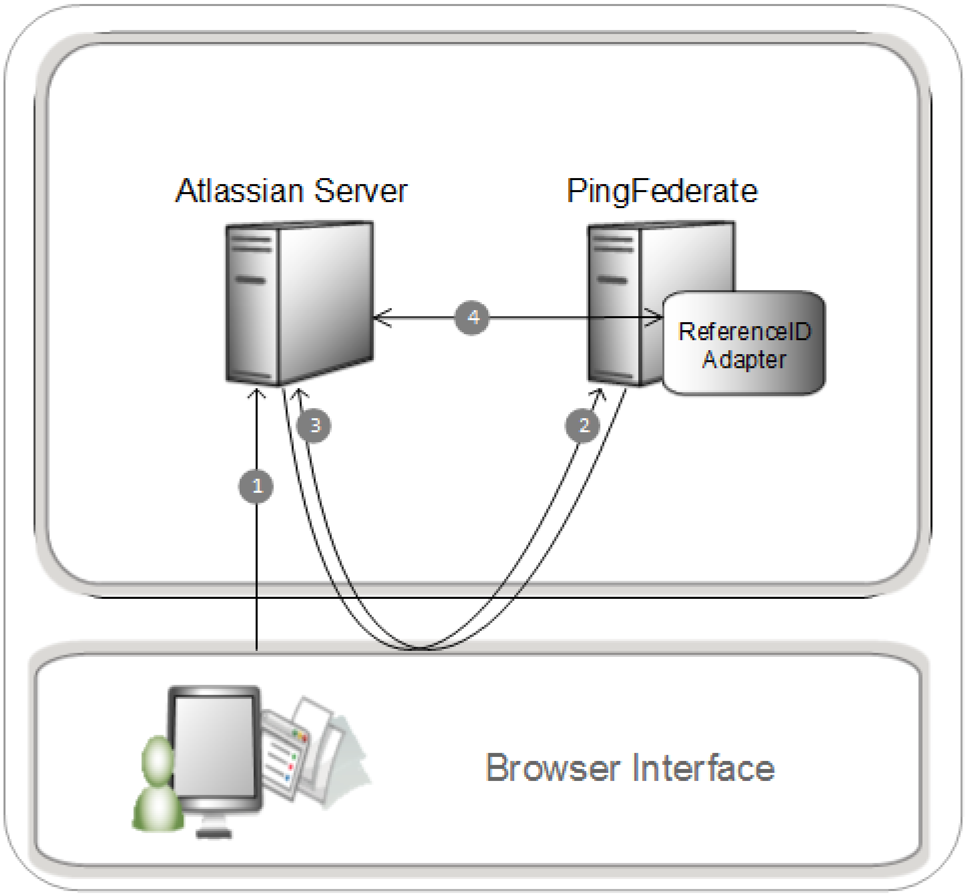
System Requirements

The Kit requires:

- PingFederate 7.3 or higher
- Agentless Integration Kit 1.2 (see Ping Identity Downloads `pingidentity.com/en/products/downloads.html`)

Processing Overview

The following figure illustrates an example SSO process flow.



Processing Steps

1. The user navigates to Atlassian (Jira or Confluence).
2. The user is redirected to PingFederate server to perform SSO. After the user logs in PingFederate creates a random identifier and associates it with the user's attributes.
3. PingFederate redirects the user back to Atlassian. The URL contains an identifier (REFID) which is used to request user attributes from PingFederate in the next step.
4. The Authenticator issues a request (which contains the identifier obtained from the previous step) to PingFederate's ReferenceID adapter. After PingFederate ensures the identifier is valid and hasn't timed out, the user's attributes are returned to the Authenticator and the session is created.

Installation and Configuration

The following sections provide instructions for configuring PingFederate to connect to Atlassian for secure Internet single sign-on (SSO). The instructions for configuring the plugin are similar for both Jira and Confluence. Jira will be used for this section of the guide.

Note: Install the Agentless Integration Kit and configure an SP ReferenceID adapter before proceeding. Refer to the Implementing SP Functionality of the Agentless Integration Kit User Guide for more information.

Note: AutoAddGroups (also called Default Group Memberships) is now supported (in both Confluence and Jira) when using Active Directory as the User Directory. This is specific to the LDAP permission set `Read Only, with Local Groups`. Also note that same LDAP must be configured as a password credential validator for the IdP Adapter used for authentication.

Define the Authenticator Configuration Directory

Before using the Plugin to configure the Authenticator, you must define where the Plugin will store the configuration settings. This is achieved using an environment variable:

1. Create a directory of your choosing on the Atlassian server. We suggest creating a subdirectory in your Atlassian instance: e.g. `<Atlassian Installation Directory>/pingfederate-settings`

Note: The user that is running jira must have read/write permissions for the created directory

2. For Linux servers:

   a. Within your Jira root directory, edit `./bin/setenv.sh`

   b. At the top of this file insert the following (modify the actual path to suit your environment):

```
PINGFEDERATE_ATLASSIAN_DATA_PATH=<Atlassian Installation
Directory>/pingfederate-settings; export PINGFEDERATE_ATLASSIAN_DATA_PATH
```

3. For Windows servers:

   c. If JIRA/Confluence is running as a standalone service (started using startup.bat), add the following line in setenv.bat:

   d. If JIRA/Confluence is started using Windows service:

   – Navigate to JIRA's bin directory with a command prompt running as Administrator, where the Tomcat7.exe binary is located

   – Issue the following command below to set the environment variable:

```
tomcat7 //US//JIRA200416102141 --
Environment=PINGFEDERATE_ATLASSIAN_DATA_PATH=C:\<path>\pingfederate-
settings
```

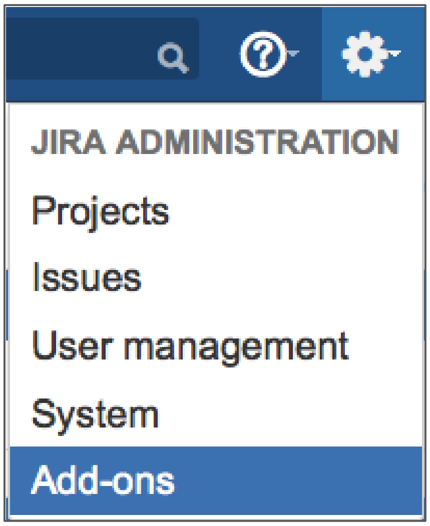
(where `JIRA200416102141` is the installed JIRA service name in services.msc)

4. Restart the Jira server

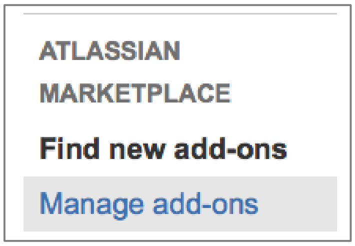
Upload the Plugin

1. Log in to Jira as an administrative user

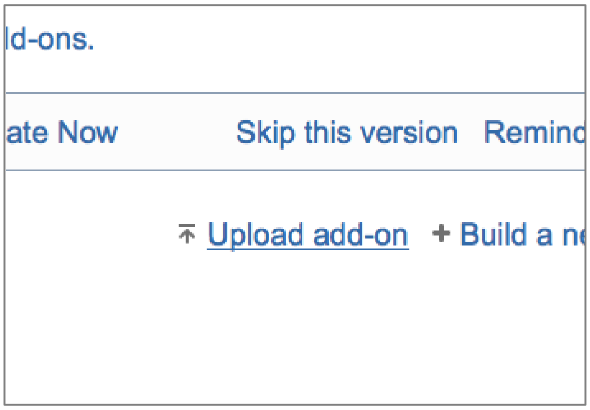
2. Navigate to the `Add-ons` section:



3. Choose `Manage add-ons` from the left side navigiation menu:



4. Choose `Upload add-on` from the right side of the page:



5. Browse to the location of the distribution package, choose: `dist/pf-authenticator-plugin-1.1.x.jar` and click `Upload`
6. Click `Configure`

Configure the Plugin

The url to configure the Authenticator is:

`http://<atlassian_hostname>:<atlassian_port>/plugins/servlet/ping/config`

The configuration page is also accessible from:

`Manage add-ons > Ping Identity SSO Plugin > Configure`.

Available Configuration Options are:

Field	Description
Configuration Directory	Make sure this matches the value you specified in the section Define the Authenticator Configuration Directory
Pickup URL	`https://<pf_host>:<pf_port>/ext/ref/pickup`. Please make note of the following: • Always use https over http • Enable the Require SSL/TLS option within the PingFederate SP ReferenceID adapter configuration
SP Adapter Instance ID	The Instance ID of your PingFederate SP ReferenceID adapter
Authentication	Determines the type of authentication to be performed between the Authenticator and the ReferenceID adapter. `Mutual SSL`: We recommend using this option as it provides the highest level of security. See Mutual SSL Authentication. `Basic`: Uses a username and passphrase to authenticate with PingFederate. See Basic Authentication

The remaining configuration options are explained in the following sections.

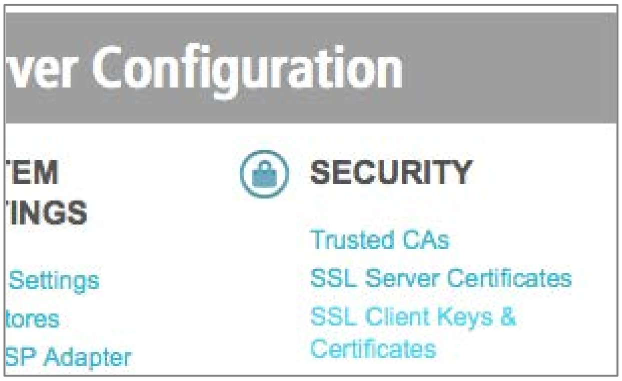
Mutual SSL Authentication

PingFederate Configuration

1. Configure a secondary SSL port. See the property `pf.secondary.https.port` in the table under Changing Configuration Parameters.

2. Import the SSL Certificate of your Atlassian server into PingFederate. See Trusted Certificate Authorities in the PingFederate Adminstrator's Manual. If you do not have an SSL certificate for the Atlassian server you can use PingFederate's Client Key/Certificate Utility to create one:

   e. From PingFederate's Admin Page go to: `Server Configuration > Security > SSL Client Keys & Certificates`

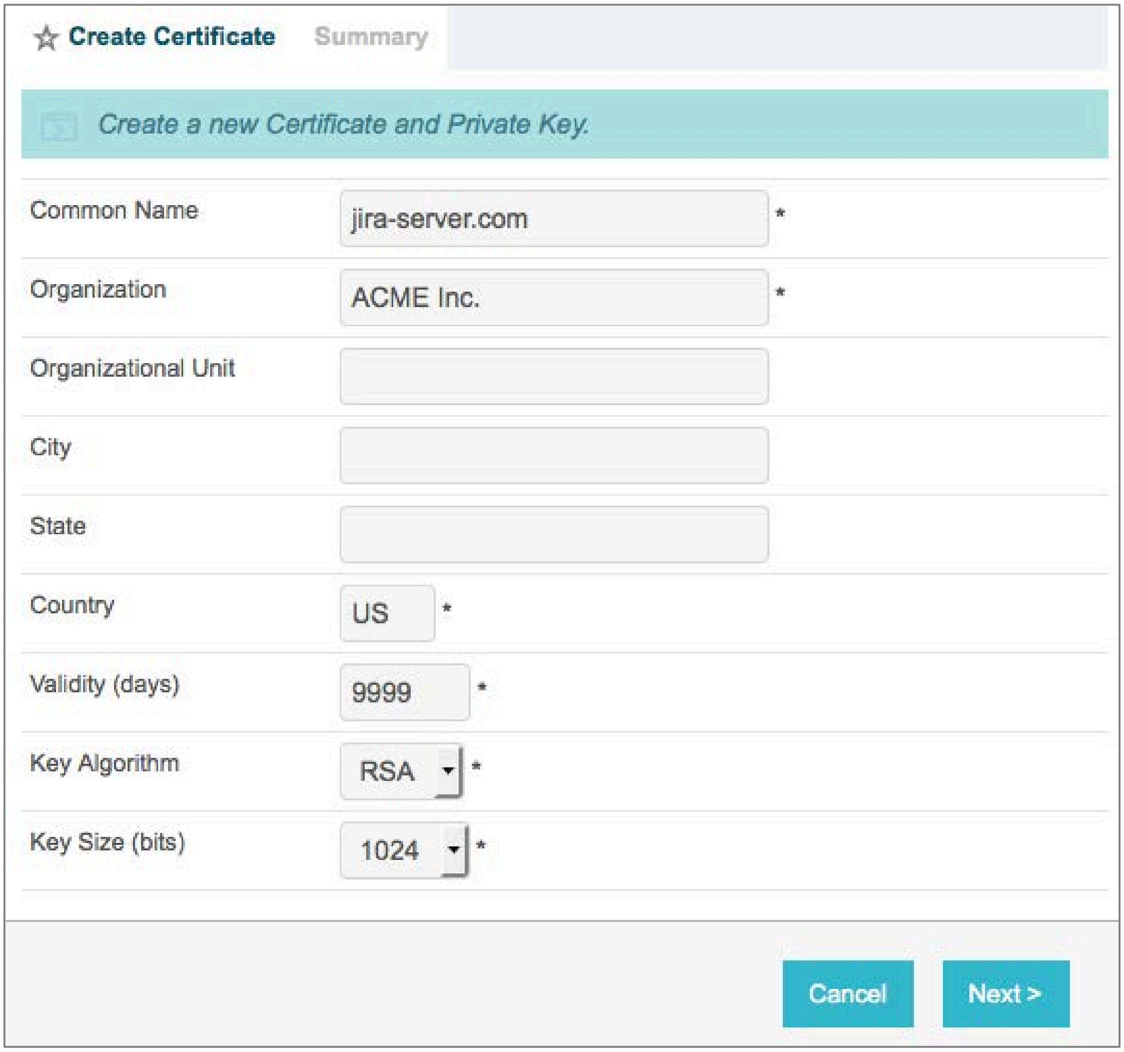


f. Click `Create New`

g. For Common Name enter the domain of your Atlassian server

h. Input a value for Organization

i. Optionally fill out the remaining fields

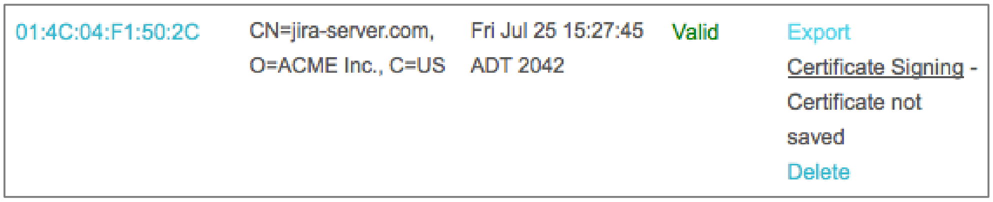


Common Name	jira-server.com *
Organization	ACME Inc. *
Organizational Unit	
City	
State	
Country	US *
Validity (days)	9999 *
Key Algorithm	RSA *
Key Size (bits)	1024 *

j. Click `Next`

k. Click `Done`

l. From the list of certificates click `Export` on your new certificate:



01:4C:04:F1:50:2C	CN=jira-server.com, O=ACME Inc., C=US	Fri Jul 25 15:27:45 ADT 2042	Valid	Export Certificate Signing - Certificate not saved Delete

m. Choose Certificate and private key. This creates a PKCS 12 certificate file (p12 extension), which will be used later in this guide.

n. Click Previous and `Export` once again but this time choose Certificate. This will export the certificate file (crt extension).

- Import this certificate into PingFederate as a Trusted CA (`Server Configuration > Security > Trusted CAs`). See Trusted Certificate Authorities in the PingFederate Adminstrator's Manual for more information.

3. Configure the SP ReferenceID adapter:

   a. Navigate to the `Instance Configuration`

   b. Clear the `User Name` and `Pass Phrase` fields

   c. Input a value for `Allowed Subject DN`. As an example, for the certificate shown in section 2.h. above, the DN would be: `CN=jira-server.com, O=ACME Inc., C=US`. See the SP Installation and Setup section of the Agentless Integration Kit User Guide for more information on `Allowed Issuer/Subject DN`.

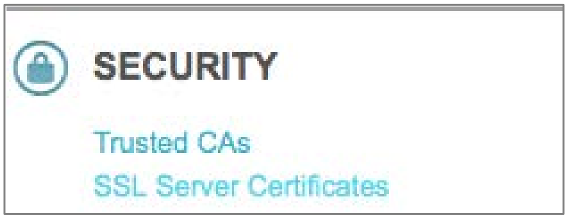
PingFederate is now be configured to accept SSL connections from the Atlassian authenticator.

Atlassian Configuration

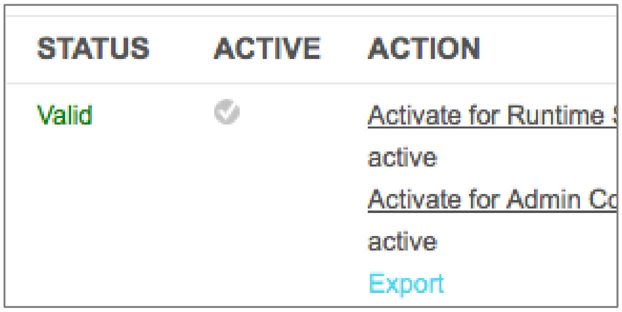
1. Copy the p12 file created in step 2.i from the previous section into the Configuration Directory of your Atlassian Server.

2. Export PingFederate's SSL Server Certificate:

   a. From the Administrator page choose `SSL Server Certificates`



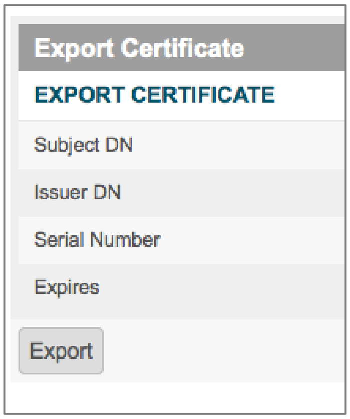
   b. Click `Export` next to your Server Certificate



STATUS	ACTIVE	ACTION
Valid	✓	Activate for Runtime active Activate for Admin Co active Export

   c. Choose `Certificate Only` and click `Next`

   d. Click `Export` to save the certificate



Export Certificate

EXPORT CERTIFICATE

Subject DN

Issuer DN

Serial Number

Expires

3. Copy the Server Certificate that was exported in the previous step info the Configuration Directory of your Atlassian Server.

4. Complete the configuration of the Authenticator Plugin:

Field	Description
Client Keystore File	The full name of the PKCS 12 file from Step 1 (do not include the full path, just the file name)
Client Keystore Password	If there was a password assigned to the client certificate enter that here
PingFederate Certificate	The full name of the certificate from Step 3 (do not include the full path, just the file name)

Note: When the configuration options are saved, the plugin will check to make sure the client and server certificates can be found.

Important: If you are using a self-signed certificate you'll need to import it into the JVM keystore. See the Self-Signed Certificate section for more information.

Basic Authentication

PingFederate Configuration

Configure the SP ReferenceID adapter:

1. Navigate to the `Instance Configuration`
2. Clear the `Allowed Subject/Issuer DN` fields
3. Input values for `User Name` and `Pass Phrase`

PingFederate is now configured for Basic Authentication.

Atlassian Configuration

Complete the configuration of the Authenticator Plugin:

Field	Description

Field	Description
Username	The User Name of the SP ReferenceID Adapter
Pass Phrase	The Pass Phrase of the SP ReferenceID Adapter

Important: If you are using a self-signed certificate you'll need to import it into the JVM keystore. See the Self-Signed Certificate section for more information.

Install the Authenticator

For Confluence and Jira 6, copy file: dist/pf-authenticator-1.1.x.jar from the distribution package to the Atlassian library directory:

- For Confluence: `<Installation Directory>/confluence/WEB-INF/lib`
- For Jira: `<Installation Directory>/atlassian-jira/WEB-INF/lib`

For Jira 7:

- Copy file: dist/jira7/pf-authenticator-jira7-1.1.x.jar from the distribution package to the Atlassian library directory: `<Jira Installation Directory>/atlassian-jira/WEB-INF/lib`

Jira 7 Configuration

When accessing a direct link to a subpage within Jira 7 (with no user session) the login link does not work correctly. The workaround:

- Copy file: dist/jira7/login.jsp from the distribution package to the Atlassian jsp directory: `< Installation Directory>/atlassian-jira/`
- Edit login.jsp and update the value for the four variables at the top of the file. For information on what these should be refer to the Seraph Configuration section.

Jira 7 will not automatically recompile JSP pages. Perform the following workaround:

- Edit the file: `<Installation Directory>/atlassian-jira/WEB-INF/web.xml`

  Important: Make a backup of this file before proceeding

- Disable the default page by adding comment blocks around the <servlet> and <servlet-mapping>:

```
<!--
    <servlet-mapping>
        <servlet-name>jsp.default_jsp</servlet-name>
        <url-pattern>/default.jsp</url-pattern>
    </servlet-mapping>
-->

<!--
    <servlet>
        <servlet-name>jsp.default_jsp</servlet-name>
        <servlet-class>jsp.default_jsp</servlet-class>
    </servlet>
```

```
-->
```

- Disable the login page by adding comment blocks around the <servlet> and <servlet-mapping>

```
<!--
    <servlet>
        <servlet-name>jsp.login_jsp</servlet-name>
        <servlet-class>jsp.login_jsp</servlet-class>
    </servlet>
-->
<!--
    <servlet-mapping>
        <servlet-name>jsp.login_jsp</servlet-name>
        <url-pattern>/login.jsp</url-pattern>
    </servlet-mapping>
-->
```

- Restart Jira

Note: After the Integration Kit has been configured and SSO works for both the default page and a subpage, the web.xml backup should be restored and Jira restarted.

Configure Seraph

The final step to linking the two systems is to configure the Seraph file within the Atlassian product.

1. Backup the existing seraph-config.xml. It's crucial to perform this step, because if there is an issue with your configuration you may need to restore this file to get back into your Atlassian server. This file can be located at:
   a. For Confluence:

      `<Atlassian Installation Directory>/confluence/WEB-INF/classes`

   b. For Jira:

      `<Atlassian Installation Directory>/atlassian-jira/WEB-INF/classes`

2. Open `seraph-config.xml` in your favorite editor.

3. Change the param-value of **login.url** and **link.login.url** to:

   ```
   https://<pf_host>:<pf_port>/sp/startSSO.ping?PartnerIdpId=
   <idp_connection_entity_id>&amp;SpSessionAuthnAdapterId=
   <sp_refid_adapter_instance_id>&amp;TARGET=${originalurl}
   ```

   pf_host: The PingFederate host

   pf_port: The PingFederate port. This should be the same value that was specified for the secondary SSL port in the Mutual SSL section.

   idp_connection_entity_id: The Partner Entity ID for the IdP connection (found under General Info section of the IdP Connection).

   sp_refid_adapter_instance_id: The Instance ID for the SP ReferenceID adapter.

Note: This value determines where the user is redirected to in step 2 of Processing Overview

4. Change the authenticator class:
    a. For Confluence, remove this line:

       ```
       <authenticator
       class="com.atlassian.confluence.user.ConfluenceAuthenticator"/>
       ```

       Add this line:

       ```
       <authenticator
       class="com.pingidentity.adapters.atlassian.confluence.PFConfluenceAuthen
       ticator"/>
       ```

    b. For Jira, remove this line:

       ```
       <authenticator
       class="com.atlassian.jira.security.login.JiraSeraphAuthenticator"/>
       ```

       Add this line:

       ```
       <authenticator
       class="com.pingidentity.adapters.atlassian.jira.PFJiraAuthenticator"/>
       ```

5. Save the seraph-config.xml
6. For Jira, there are two extra steps:

Disable the default login gadget:

1. Open `<Atlassian Installation Directory>/atlassian-jira/WEB-INF/classes/jira-application.properties`
2. Disable the login gadget:

   ```
   jira.disable.login.gadget=true
   ```

3. Save the File

Change default redirect url:

If you do not perform this step the user will not be automatically redirected to PingFederate for SSO when they land on the Jira Dashboard page. They would have to click the Jira Login link in order to perform SSO.

For Jira 6:

1. Open `your_jira_home/atlassian-jira/default.jsp`
2. Delete this line: `response.sendRedirect(…….);`
3. Add this line (where the previous line was deleted), replacing the values enclosed in “<>” with values appropriate to your environment:

   ```
   response.sendRedirect("https://<pf_host>:<pf_port>/sp/startSSO.ping?Partner
   IdpId=<idp_connection_entity_id>&amp;SpSessionAuthnAdapterId=<sp_refid_adap
   ter_instance_id>&amp;TARGET=
   http%3A%2F%2F<atlassian_hostname>%3A<atlassian_port>%2Fsecure%2FDashboard.j
   spa");
   ```

4. Save the file

For Jira 7:

Note: This step is optional due to the fact that anonymous access to the home page will no longer be possible once implemented.

1. Copy file: dist/jira7/default.jsp from the distribution package to the Atlassian jsp directory: `<Installation Directory>/atlassian-jira/`
2. Edit default.jsp and update the value for the four variables at the top of the file. For information on what these should be refer to the Seraph Configuration section.

Self-Signed Certificate

If you are using a self-signed certificate for the PingFederate Server, it must be imported into the JVM of the Atlassian server. This is required whether the Authentication Type is Mutual SSL or Basic Authentication. To import the certificate into the JVM keystore, run the following command as an administrative user (or sudo):

```
keytool -importcert -alias PingFederate -file /<full-path-to-cert>/14B181B1359.crt -keystore /<full-path-to-jre>/lib/security/cacerts
```

The default keystore password is either `changeit` or `changeme`.

`full-path-to-jre`: The JRE being used by Atlassian is usually listed when you startup Jira or Confluence.

`full-path-to-cert`: If you are following along up to this point, this value should be `$PINGFEDERATE_ATLASSIAN_DATA_PATH`

Logging

To enable logging for the Authenticator add the following to `WEB-INF/classes/log4j.properties`. Replace `INFO` with `DEBUG` to turn on debug logging:

```
log4j.appender.PingFederateLog=org.apache.log4j.FileAppender
log4j.appender.PingFederateLog.File=${catalina.home}/logs/pingfederate.log
log4j.appender.PingFederateLog.MaxFileSize=20480KB
log4j.appender.PingFederateLog.MaxBackupIndex=5
log4j.appender.PingFederateLog.layout=org.apache.log4j.PatternLayout
log4j.appender.PingFederateLog.layout.ConversionPattern=%d %t %p [%c{4}] %m%n
log4j.appender.PingFederateLog.Threshold=INFO
log4j.logger.com.pingidentity.adapters.atlassian=INFO, PingFederateLog
log4j.additivity.com.pingidentity.adapters.atlassian=false
```

Troubleshooting

The following table lists potential problems administrators might encounter during the setup or deployment of the Atlassian Integration Kit, along with possible solutions:

Problem	Possible Solution
(SSO Failure) An SSO attempt results in a continuous loop between PingFederate and the Atlassian product.	1. Ensure that the IdP User exists in the Atlassian Product. 2. Ensure that the PingFederate ReferenceID Adapter settings match your Authenticator Plugin configuration in the Atlassian Product. 3. If using a self-signed certificate, refer to the following instructions (Self-Signed Certificate). 4. If using Mutual SSL Authentication, ensure the following: a. Import the SSL Certificate of your Atlassian server into PingFederate (Import Certificate into PingFederate). b. Ensure the Atlassian and PingFederate server certificates are in the Configuration Directory. c. Ensure the ReferenceID Adapter contains the correct Issuer or Subject DN values.
Sessions clash when Jira and Confluence services are running on the same host, resulting in the user being logged out at inappropriate times	A possible fix is to use multiple hostname aliases and changing the Base URL of Jira and Confluence respectively to use different hostnames. For example: Base URL for Jira: `http://jira:8080` Base URL for Confluence: `http://confluence:8090` For more information, see: https://confluence.atlassian.com/jirakb/user-is-constantly-logged-out-of-jira-192872663.html