PingFederate®

Integration Kit for RSA SecurID

Version 1.2

User Guide

Ping Identity®

PingFederate Integration Kit for RSA SecurID *User Guide*
Version 1.2
October, 2015

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

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

Trademarks

Disclaimer

Document Lifetime

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

From the Web site, you may also download and refresh this PDF if it has been updated, as indicated by a change in this date: October 27, 2015

Contents

Introduction

The PingFederate Integration Kit for RSA SecurID® for adds an Identity Provider (IdP) integration option to PingFederate by providing an RSA SecurID Adapter, which acts as an RSA® Authentication Agent. The Adapter works in conjunction with RSA Authentication Manager and RSA SecurID Authenticators to allow an IdP enterprise to generate SAML (Security Assertion Markup Language) assertions and provide single sign-on (SSO) to Service Provider (SP) applications.

The PingFederate Integration Kit for RSA SecurID® is certified under the RSA Secured® Partner Program.

Intended Audience

This document is intended for system administrators with experience in the configuration and maintenance of RSA Authentication Manager 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 or the RSA SecurID Adapter.

System Requirements

The PingFederate Integration Kit for RSA SecurID is designed and supported for RSA Authentication Manager 6.1.2, 7.1 SP2, 7.1 SP3, 7.1 SP4 and 8.1.

- PingFederate 7.x (or higher)
- RSA Authentication Agent API 8.1 SP1 (or higher) for Java available through here

  This contains the following RSA jars which need to be deployed in PingFederate.

  1. authapi.jar
  2. crypto.jar

  Tip: There is backward compatibility for RSA Authentication Agent API 8.1 SP1 as existing agent code which uses APIs from version 8.1can be reused.

- RSA Authenticators

  Note: To deploy the RSA SecurID Adapter in a PingFederate server cluster, the load balancer for the server nodes must implement "sticky sessions." (For more information about deploying PingFederate in a cluster, see the PingFederate Server Clustering Guide.)

ZIP Manifest

The distribution ZIP file for the Integration Kit contains the following:

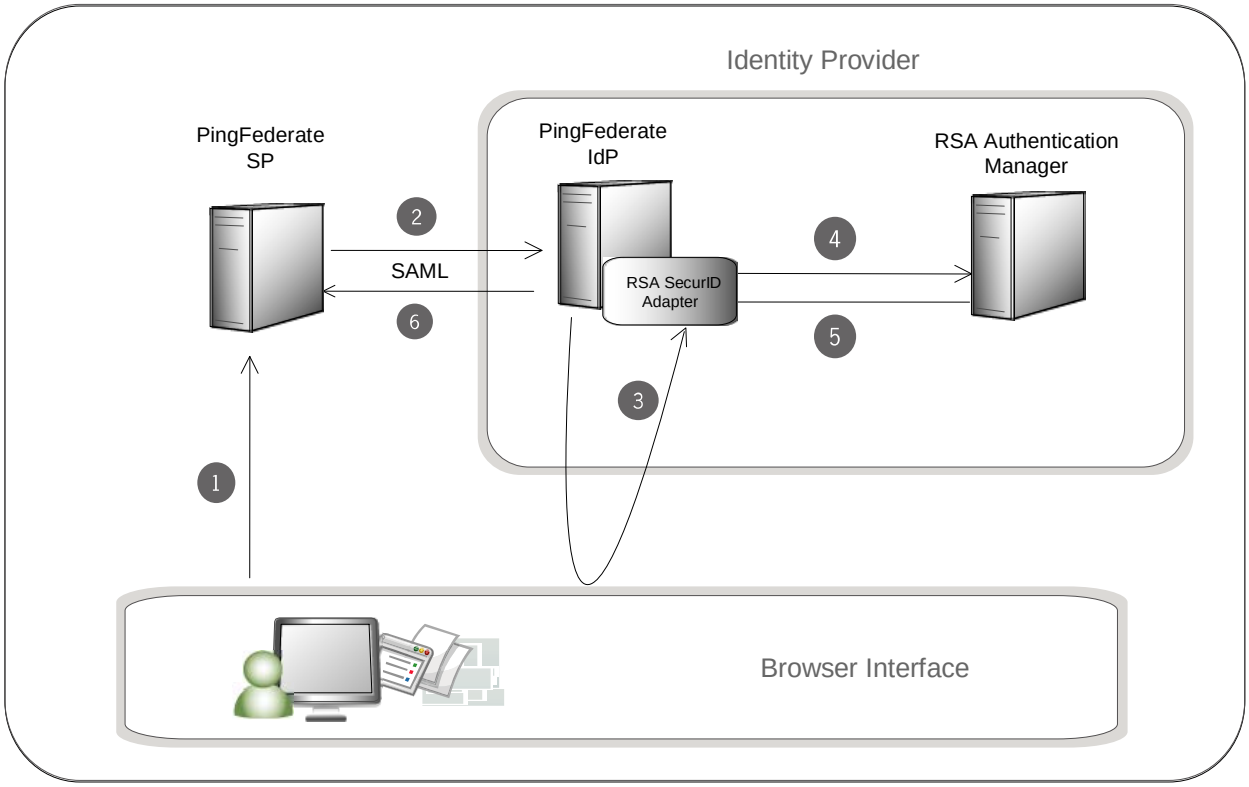
- `ReadMeFirst.pdf` – contains links to this online documentation
- `/dist` – contains libraries needed to run the adapter:
  - `pf-securid-authn-adapter-1.2.x.jar` – the RSA SecurID Adapter JAR file

- `/template` – contains templates of Web forms displayed to end users during authentication
- `pf-securid-images.war` – images used by templates

Note: The templates may be modified and images replaced to meet enterprise branding and other requirements (See Modifying User-Facing Templates on page 10).

Processing Overview

The following figure illustrates an SP-initiated SSO scenario in which PingFederate authenticates users to an SP application using the RSA SecurID Adapter.



Processing Steps

1. The user initiates SSO from an SP application through the PingFederate SP server.

   Note: This SP-initiated scenario represents the optimal use-case, one in which both the IdP and SP are using PingFederate. If your SP partner does not support this scenario, however, PingFederate will accept any valid SAML authentication request. In addition, you can enable IdP-initiated SSO; in this case the processing sequence would not include this step or the next one.

2. The PingFederate SP server generates a SAML `AuthnRequest` to the PingFederate IdP server.
3. The PingFederate IdP server requests user authentication using the RSA SecurID Adapter. The Adapter challenges the user for a RSA SecurID Passcode.
4. The Adapter sends authentication credentials to RSA Authentication Manager.

5. The Authentication Manager validates the credentials sent by the Adapter and returns the status to PingFederate.
6. If the validation fails, user access is denied. If validation succeeds, the PingFederate IdP server generates a SAML assertion with the username as the Subject and passes it to the PingFederate SP server.

Installation and Setup

Setting up the Integration Kit involves:

- Obtain and install the RSA Authentication Agent API jars (`authapi.jar and crypto.jar`)
- Configuring RSA Authentication Manager
- Installing and configuring the RSA SecurID Adapter within PingFederate

Step 1 -- Obtain and Install the Authentication Agent API

The Java Agent API must be loaded into PingFederate during the Adapter installation.

To install the Agent API:

Copy the necessary API library as provided (in this case, `authapi.jar` and `crypto.jar`) into the `<PF_install>/pingfederate/server/default/lib` directory.

Note: The Authentication Agent API can be downloaded from within RSA Support.

Step 2 -- Configure RSA Authentication Manager

To configure RSA Authentication Manager (for version 6.1.2):

1. Access RSA Authentication Manager Host Mode (or Remote Mode if configuring remotely).
2. Add an **Agent Host** with the following settings (at minimum):

Name	Hostname where the PingFederate server is running.
Network Address	IP address where PingFederate is running. (This should be populated automatically as long as the PingFederate hostname can be resolved.)
Agent Type	Choose Communication Server.
Encryption Type	Ensure DES is selected.

3. If PingFederate is running in a cluster, then add all server nodes as **Secondary Nodes** in the Add Agent Host configuration.

Note: Include the server running the PingFederate administrative console.

4. From the **Agent Host** menu, generate and download the Configuration File (`sdconf.rec`) for the new PingFederate Agent.

   This file will be used in configuring the RSA SecurID Adapter.

To configure RSA Authentication Manager (for version 7.x and 8.x):

1. Access RSA Security Console.
2. Add an **Authentication Agent** with the following settings (at minimum):

Hostame	Hostname where the PingFederate server is running.
IP Address	IP address where PingFederate is running. (This should be populated automatically as long as the PingFederate hostname can be resolved.)
Agent Type	Web Agent.

3. If PingFederate is running in a cluster, then add all server nodes as **Alternate IP Addresses** in the Add Authenticate Agent configuration.

   Note: Include the server running the PingFederate administrative console.

4. From the **Authentication Agent** menu, generate and download the Configuration File (`sdconf.rec`) for the new PingFederate Agent. This file will be used in configuring the RSA SecurID Adapter.
5. Access Manage Node Secret and create a new secret. This can be exported to the RSA SecurID Adapter after being converted to 8.1 SP1 format. For information on converting the exported file please refer to **Convert an Existing Node Secret to 8.1 SP1 Format**.

Step 3 – Install the Adapter and Configure PingFederate

To install the RSA SecurID Adapter and configure PingFederate:

1. Stop the PingFederate server if it is running.
2. From the integration-kit `dist` directory, copy the file `pf-securid-authn-adapter-1.2.x.jar` and the folder `pf-securid-images.war` into:
   `<PF-install>/server/default/deploy`
3. From the integration-kit `dist/template` directory, copy all files into:
   `<PF-install>/server/default/conf/template`
4. Start PingFederate.

5. Log on to the PingFederate administrative console and click **Adapters** under My IdP Configuration on the Main Menu.

(For more information about IdP Adapters, see Configuring IdP Adapters in the PingFederate *Administrator's Manual*.)

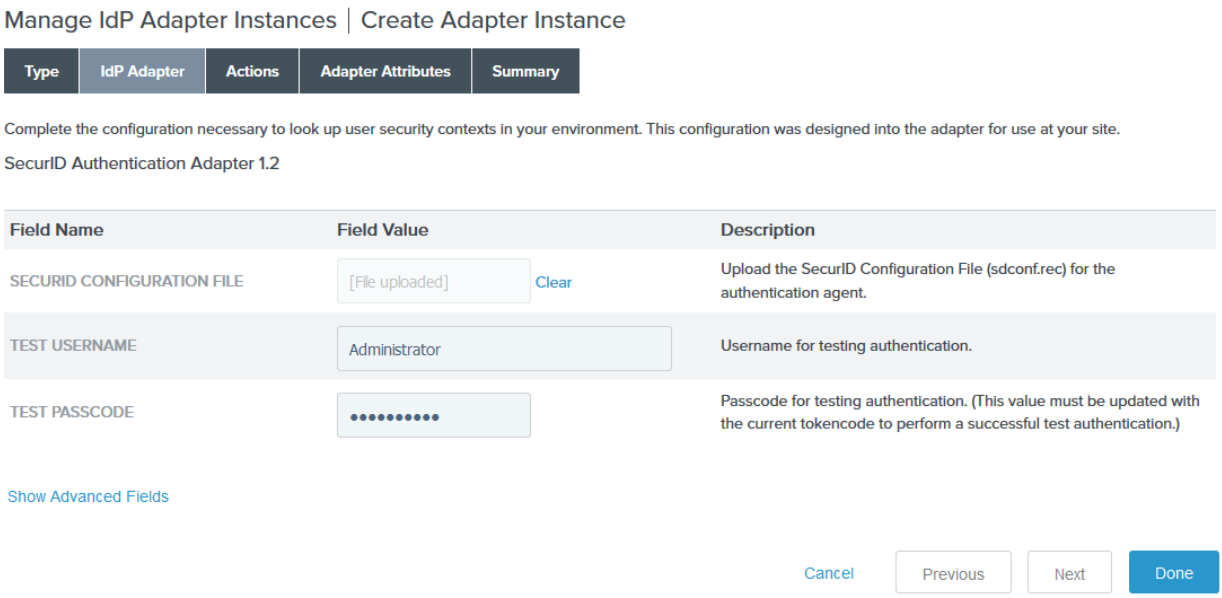
6. On the Manage IdP Adapter Instances screen, click **Create New Instance**.

7. On the Type screen, enter an Instance Name and Instance ID.

The Name is any you choose for identifying this Adapter Instance. The ID is used internally and may not contain spaces or non-alphanumeric characters.

8. Select SecurID Authentication Adapter 1.2.x from the Type dropdown list and click **Next**.

Note: References to screens in these steps conform to the appearance of the PingFederate 8.x administrative console. However, the configuration is the same for 7.x versions; only the screen names have changed.



9. On the IdP Adapter screen provide entries for each of the fields shown, as indicated in the table below.

Field	Description
RSA SecurID Configuration File	Click the Browse button to locate this configuration file (**`sdconf.rec`**), which is generated from RSA Authentication Manager. The file is uploaded to PingFederate when you click **Next**.
Test Username	Enter a valid RSA SecurID Username to be used for testing authentication to RSA Authentication Manager when you click **Next**.
Test Passcode	Enter the current Passcode for the Test Username.

Field	Description
Note: The Username and Passcode are used to download the Node Secret from RSA Authentication Manager. The fields are required for initial setup, or to reset the Node Secret if it has been cleared in RSA Authentication Manager (see step 15). Alternatively the node secret can also be exported through RSA Authentication Manager and uploaded through the advanced field ***SecurID Node Secret***. Please note that the node secret needs to be converted to the 8.1 SP1 format before import. Refer to **Convert an Existing Node Secret to 8.1 SP1 Format** for instructions.	

10. (Optional) Click **Show Advanced Fields** to view additional configuration settings.

11. Depending on your RSA SecurID configuration and other requirements at your site, provide entries if needed, as described in the table below and on the screen.

Field Name	Description
SecurID Node Secret	This file is typically generated during test authentication. However, if RSA Authentication Manager is configured to create this file, then it must be uploaded here.
SecurID Optional Configuration	Upload SecurID Optional Configuration File (`sdopts.rec`) if required in your Authentication Manager setup.
Challenge Retries	The maximum number of times a user will be asked to try again when authentication fails.
Logout Path	Any path in the format indicated. Setting a path will invoke adapter logout functionality that is normally invoked during SAML 2.0 single-logout processing. Available primarily for partner SaaS providers who do not support SAML Single Log-out (SLO) but who may want users' IdP SSO sessions to end after logging out of the SaaS services.
Logout Redirect	The landing page at the SP after successful IdP logout (applicable only when Logout Path is set above).
Logout Template	Template on the IdP server to display after successful IdP logout, if Logout Redirect fails or is not provided (applicable only when Logout Path is set above).
Authentication Context value	Additional information provided to the SP to assess the level of confidence in the assertion. This value will override the default authentication context used by the adapter.
Session State	Determines whether a session is maintained within the securid adapter.
Session Timeout	Session Idle Timeout (in minutes). If left blank the timeout will be the Session Max Timeout. Ignored if 'No' is selected for Session State.
Session Max Timeout	Session Max Timeout (in minutes). Leave blank for indefinite sessions. Ignored if 'No' is selected for Session State.

12. Click **Next.**

13. On the Actions screen, click **Next.**

Important: The **Reset Node Secret** action is used only if the Node Secret is cleared at some point from RSA Authentication Manager. In that case, return to this screen and click **Reset Node Secret**. Then go back to the IdP Adapter screen and re-enter the current **Passcode** for the test user in order to download the Node Secret.

14. On the Adapter Attributes screen, select subject as the Pseudonym.

(For more information about this screen, see Setting Pseudonym Values and Masking in the PingFederate *Administrator's Manual* or click **Help**.)

15. On the Summary screen, verify that the information is correct and click **Done**.
16. On the Manage IdP Adapter Instances screen, click **Save** to complete the Adapter configuration.
17. Configure or modify the connection(s) to your SP partner(s) using the RSA SecurID Adapter Instance.

For more information, see Identity Provider SSO Configuration in the PingFederate *Administrator's Manual*.

Modifying User-Facing Templates

The RSA SecurID Adapter uses Velocity HTML templates (contained in the `dist/template` directory) to present end users with authentication challenges and other RSA SecurID messages. The templates reference images and a `styles.css` style sheet (in the `dist/pf-securid-images.war folder`). You can replace the images for branding or other purposes and modify the style sheet to change the look and feel of the Web pages. To a limited extent, you may also modify the templates themselves, if needed.

Caution: Velocity templates contain variables used by the Java-based Velocity rendering engine. Modifying these files directly is not recommended, except for clearly identifiable HTML markup if necessary.

The following table lists the templates and their use (the initial, identical portion of each file name—`SecurIDAuthenticationAdapter`—is omitted in the table). For more information about Velocity templates, see System Administration in the PingFederate *Administrator's Manual*.

Template File	Description
.form.template.html	Main logon form, presented under normal conditions.
.nexttoken.template.html	Form presented when user is required to enter the next token.
.pinreset.template.html	Form presented when user is allowed to choose whether to create a PIN or use a system-generated PIN.
.reauthenticate.template.html	Logon form asking user to authenticate again after resetting

Template File	Description
	PIN.
.systempinreset.template.html	Presents user with a new, system-generated PIN.
.userpinreset.template.html	Presents user with a form to input a new PIN.

Upgrading from a previous version

For upgrading from an existing version follow the steps below,

1. Stop the PingFederate server if it is running.
2. Delete the following file/folder from `<PF-install>/server/default/deploy`

- `pf-securid-authn-adapter-1.x.jar`
- `pf-securid-images.war`

3. From the integration-kit `dist` directory, copy the file `pf-securid-authn-adapter-1.2.x.jar` and the folder `pf-securid-images.war` into: `<PF-install>/server/default/deploy`
4. From the integration-kit `dist/template` directory, copy the following files into: `<PF-install>/server/default/conf/template`
    - `SecurIDAuthenticationAdapter.form.template.html`
    - `SecurIDAuthenticationAdapter.nexttoken.template.html`
    - `SecurIDAuthenticationAdapter.pinreset.template.html`
    - `SecurIDAuthenticationAdapter.reauthenticate.template.html`
    - `SecurIDAuthenticationAdapter.systempinreset.template.html`
    - `SecurIDAuthenticationAdapter.userpinreset.template.html`

Note: These template files have been modified to support 2nd factor authentication and CSRF protection. If these were modified in an earlier version, those updates would need to be reapplied to the new templates.

---

5. Start PingFederate.
6. Log on to the PingFederate administrative console and update existing adapter configurations to configure session state (if required). If this step is not performed the following default values for session state will be used at runtime.

- Session State (Yes)
- Session Timeout (60 minutes)
- Session Max Timeout (480 minutes)

Convert an Existing Node Secret to 8.1 SP1 Format

You can convert the existing node secret to the new format by running the agent_nsload utility that comes from RSA Security. You would need to contact RSA security to get this utility if it did not come with your RSA Authentication Manager software.

To run the agent_nsload utility for conversion of the node secret:

1. Change to the util directory.
2. Change to the required platform-specific folder.

3. Run the agent_nsload utility as below, and give the path to the existing SecurID file location in the machine as the first parameter and the new destination location of the SecurID file as the second parameter.

agent_nsload -c <Existing_Securid_file_path> <New_Securid_dir_path>

where:

- Existing_Securid_file_path is the path where the SecurID file exists.
- New_Securid_dir_path is the directory where the newly generated SecurID file should be stored.

For example:

On Windows:

agent_nsload -c C:\RSA\securid C:\My_Dir

On UNIX:

agent_nsload -c /tmp/RSA/securid /var/ace/

Troubleshooting

The following table lists potential problems administrators might encounter during the setup or deployment of the SecurId Adapter, along with possible solutions.

Note: You can enable additional debug logs from RSA by modifying the file `<PF-install>/server/default/data/adapter-config/securid.properties` You will also need to configure log4j within PingFederate to allow logs from ***com.rsa*** to appear within server.log. For more information please refer to PingFederate *Administrator's Manual*.

Problem	Possible Solution
The RSA SecurID authentication adapter does not appear in the drop-down list when creating a new Adapter Instance.	Ensure the RSA SecurID Agent API (`authapi.jar` and `crypto.jar`) is deployed in the directory: `<pf_install>server/default/lib`
Setup error: "No server available."	Ensure you are using a valid configuration file (`sdconf.rec`) generated from RSA Authentication Manager. Ensure that no firewalls are blocking ports between RSA Authentication Manager and the PingFederate administrative server. The default port is 5500 for both TCP and UDP. For more information refer to RSA documentation.

Problem	Possible Solution
Setup error: “Test Authentication failed. Please make sure you enter the correct values in 'Test Username’ and 'Test Passcode'.”	Ensure that the Username and/or Passcode are valid. Check for a network communication problem between PingFederate and the RSA Authentication Manager.
End-user runtime error: “'Access denied.”	If this error occurs repeatedly without obvious cause: Check the PingFederate server log to see if an exception is logged. Run RSA Authentication Manager Log Monitor and perform a test SSO to check events. Reset the Node Secret both on the Agent Host and in the PingFederate administrative console. (See step 15.) Ensure the Username is not locked out in RSA Authentication Manager Ensure the Username has access to the Agent Host in RSA Authentication Manager. If using an exported node secret, please ensure the file is in the correct format (8.1 SP1). For more information please refer to **Convert an Existing Node Secret to 8.1 SP1 Format**.