PingFederate®

Integration Kit For RSA SecurID®

Version 1.0

User Guide

PingIdentity®

© 2010 Ping Identity® Corporation. All rights reserved.

PingFederate Integration Kit for RSA SecurID *User Guide*
Version 1.0
March, 2010

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: www.pingidentity.com

Trademarks

Ping Identity, the Ping Identity logo, PingFederate, and the PingFederate icon are trademarks or registered trademarks of Ping Identity Corporation. RSA, RSA SecurID, RSA SecurCare, and RSA Secured are registered trademarks of RSA Security Inc.

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

The PingFederate Integration Kit for RSA SecurID® 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.

ZIP Manifest

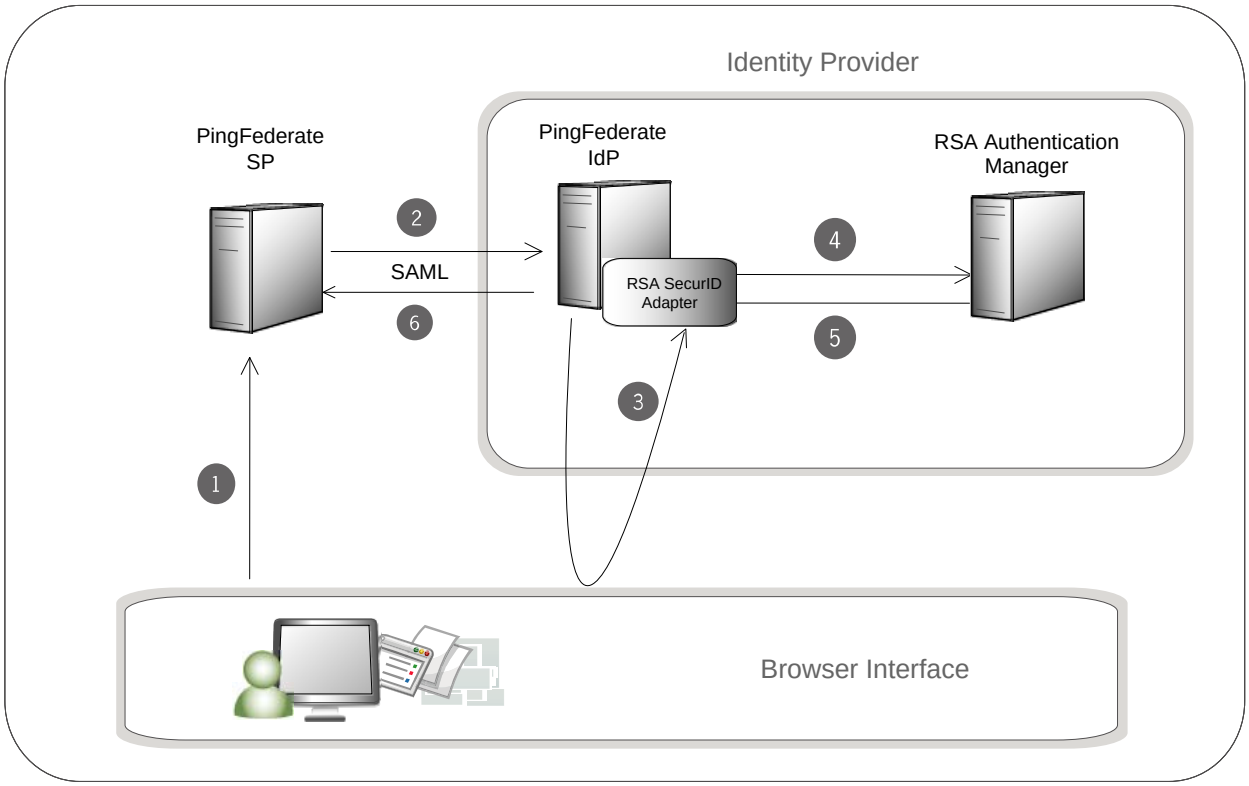
The distribution ZIP file for the Integration Kit contains the following:

- `/docs` – contains this documentation:
  - `RSA_SecurID_Integration_Kit_Qualification_Statement.pdf` – testing and platform information
  - `RSA_SecurID_Integration_Kit_User_Guide.pdf` – this document
- `/dist` – contains libraries needed for the Adapter
  - `pf-securid-adapter-1.0.jar` – 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 9).

Overview

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



Sequence

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. 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.

System Requirements

This Integration Kit for RSA SecurID is designed and supported for RSA Authentication Manager 6.1.

The following additional prerequisites must be satisfied in order to implement the RSA SecurID Adapter:

- PingFederate 5.x (or higher)
- RSA Authentication Agent API 5.0.3.172 (or higher) for Java
- 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*.)

Installation and Setup

Setting up the Integration Kit involves:

- Downloading the Authentication Agent API (`authapi.jar`) from RSA
- Configuring RSA Authentication Manager
- Installing and configuring the RSA SecurID Adapter within PingFederate

Step 1: Download the Authentication Agent API

The Java Agent API must be loaded into PingFederate during the Adapter installation. Before you begin, if you have not done so already, obtain the `authapi.jar` file from RSA.

To download the Agent API:

- If you have Internet access to RSA SecurCare® Support, log on and search for the API, or find it on the download page.

  If you do not have an RSA support agreement, contact your RSA representative.

Be sure to save the file in a location accessible from the machine running PingFederate.

Step 2: Configure RSA Authentication Manager

To configure RSA Authentication Manager (for version 6.1):

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.

Step 3: Install the Adapter and Configure PingFederate

To install the RSA SecurID Adapter and configure PingFederate:

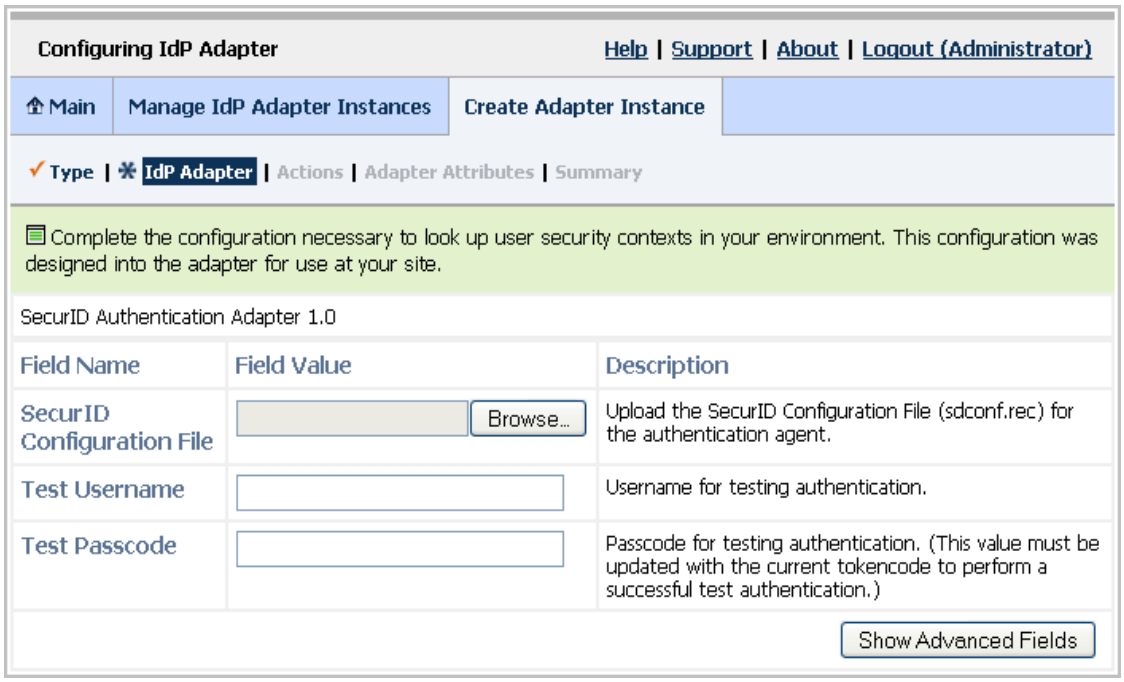
1. Stop the PingFederate server if it is running.
2. From the integration-kit `dist` directory, copy the file pf-`securid-adapter-1.0.jar` and the folder `pf-securid-images.war` into:
   `<PF-install>/server/default/deploy`
3. From the integration-kit `dist/template` directory, copy all files into:
   `<PF-install>/server/default/conf/template`
4. Copy the Authentication Agent API `authapi.jar` file into:
   `<PF-install>/server/default/lib`

   If you do not yet have the API, see Step 1: Download the Authentication Agent API on page 6.
5. Start PingFederate.
6. 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 the PingFederate *Administrator's Manual*.)
7. On the Manage IdP Adapter Instances screen, click **Create New Instance**.
8. 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.
9. Select SecurID Authentication Adapter 1.0 from the Type dropdown list and click **Next**.

Note: References to screens in these steps conform to the appearance of the PingFederate 6.x administrative console. However, the configuration is the same for 5.x versions; only the screen names have changed.



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

Field Name	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.
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 13).	

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

    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).

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 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 the "Identity Provider SSO Configuration" chapter 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 the "System Administration" chapter 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 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.

Troubleshooting

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

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`) 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.
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.

Problem	Possible Solution
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 13 on page 9.) • Ensure the Username is not locked out in RSA Authentication Manager • Ensure the Username has access to the Agent Host in RSA Authentication Manager.