Ping Identity®

PingFederate® Integration Kit for RSA SecurID®

RSA SecurID Ready Implementation Guide

Last Modified: March 25, 2010

Partner Information

Product Information	
Partner Name	Ping Identity Corporation
Web Site	www.pingidentity.com
Product Name	PingFederate Integration Kit for RSA SecurID
Version & Platform	6.0
Product Description	The PingFederate Integration Kit for RSA SecurID adds an Identity Provider (IdP) option to integrate RSA SecurID with PingFederate, Ping Identity's flagship platform for Internet identity management and security. The Integration Kit provides a PingFederate Adapter that acts as an RSA Authentication Agent. The Adapter works in conjunction with RSA Authentication Manager and RSA SecurID Authenticators to allow an enterprise to generate Security Assertion Markup Language (SAML)) identity assertions, which enable secure Internet single sign-on (SSO) to Service Provider (SP) applications and other protected resources.
Product Category	Enterprise Single Sign-On

Solution Summary

The PingFederate Integration Kit for RSA SecurID adds an Identity Provider (IdP) option to integrate RSA SecurID with PingFederate, Ping Identity's flagship platform for Internet identity management and security. The Integration Kit provides a PingFederate Adapter that acts as an RSA Authentication Agent. The Adapter works in conjunction with RSA Authentication Manager and RSA SecurID Authenticators to allow an enterprise to generate Security Assertion Markup Language (SAML)) identity assertions, which enable secure Internet single sign-on (SSO) to Service Provider (SP) applications and other protected resources.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication
List Library Version Used	RSA Authentication Agent API 5.0.3 for Java
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	No
RSA Authentication Agent Host Type	Communication Server
RSA SecurID User Specification	All Users
RSA SecurID Protection of Administrative Users	No
RSA Software Token and RSA SecurID 800 Automation	No

Product Requirements

Partner Product Requirements: PingFederate
PingFederate 5.x or higher

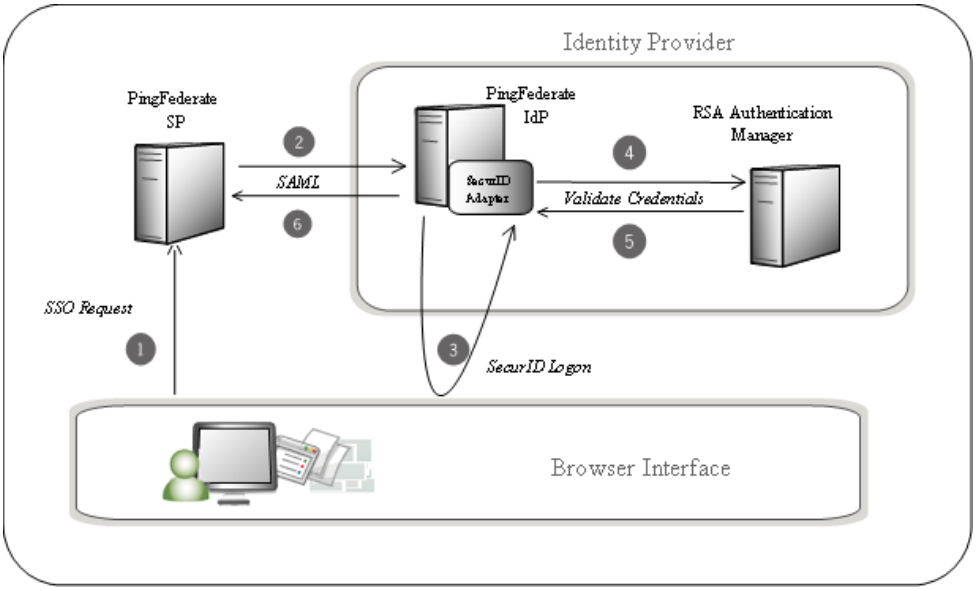
Operating System
Windows 2003 Server – SP2 on x86 32-bit
Red Hat Enterprise Linux 4
Red Hat Enterprise Linux 5
Windows 2003 Server – SP2 on x86 64
Windows 2008 Server – on x86 64
SUSE Linux Enterprise 9 – 64 bit
Solaris 10 for 64 bit

Additional Software Requirements
Application
RSA SecurID API (authapi.jar)[1]
Sun JDK 1.6

[1] Contact RSA Support to obtain a copy of the RSA SecurID API.

Process Diagram

The following figure shows an SP-initiated SSO scenario (one example use case) in which PingFederate authenticates users to an SP application using the RSA SecurID Adapter:



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, 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 steps one or two.**

2. The PingFederate SP server generates a SAML AuthnRequest to the PingFederate IdP server.
3. The PingFederate IdP server requests user authentication using the SecurID Adapter. The Adapter challenges the user for an 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.

Agent Host Configuration

To facilitate communication between the PingFederate Adapter and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies the PingFederate Adapter within its database and contains information about communication and encryption.

To create the Agent Host record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces

When adding the Agent Host Record, you should configure the PingFederate Adapter host as a Communication Server. This setting is used by the RSA Authentication Manager to determine how communication with PingFederate and the RSA SecurID Adapter will occur.

> **Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.**

Please refer to the appropriate RSA Security documentation for additional information about Creating, Modifying and Managing Agent Host records.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	<pf_home>/pingfederate/server/default/data/adapter-config/
securid	<pf_home>/pingfederate/server/default/data/adapter-config/
sdstatus.12	<pf_home>/pingfederate/server/default/data/adapter-config/
sdopts.rec	<pf_home>/pingfederate/server/default/data/adapter-config/

Partner Product Configuration

Before You Begin

This section provides instructions for integrating PingFederate with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved and the ability to perform the tasks outlined in this section. Administrators should have access to documentation for all products in order to install the required components.

All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Installation and Setup

Setting up the PingFederate Integration Kit involves:

- **Configuring RSA Authentication Manager**
- **Installing and configuring the RSA SecurID Adapter in PingFederate**

Configuring RSA Authentication Manager

To configure RSA Authentication Manager:

1. 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.
2. 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.
3. 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 SecurID Adapter.

Installing the Adapter and Configuring PingFederate

To install the RSA SecurID Adapter[2] 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 RSA SecurID API authapi.jar file into:
   <PF-install>/server/default/lib

[2] (For more information about IdP Adapters, see the PingFederate *Administrator's Manual*.)

5. Copy the RSA SecurID API authapi.jar file into:
   <PF-install>/server/default/lib

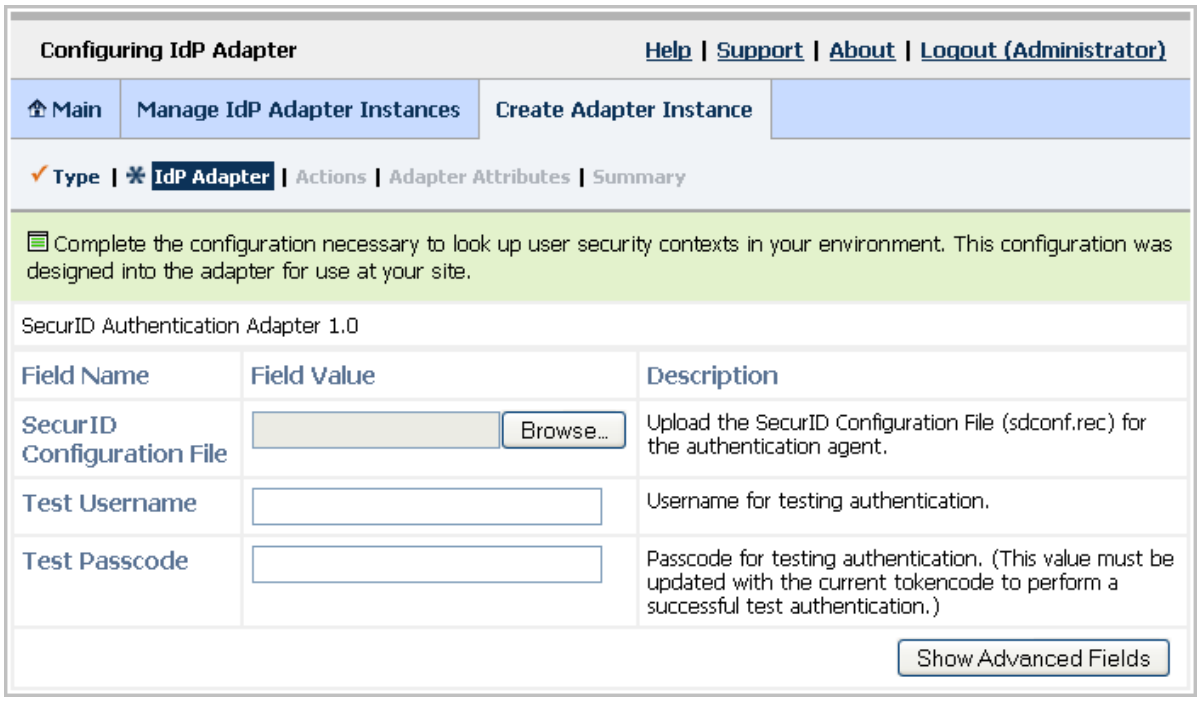
6. Start PingFederate, log on to administrative console and click **Adapters** under My IdP Configuration on the Main Menu.

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: This section references 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
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. (see step 12).	

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 RSA 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** on this screen and again on the Actions screen.

> **Important**: **Never reset the node secret unless it has been cleared on the RSA Authentication Manager server. To do so, click** *Reset Node Secret*, **go to the IdP Adapter screen, enter the test user's** *Passcode* **and download the secret.**

13. 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**.)

14. On the Summary screen, verify that the information is correct and click **Done**.

15. On the Manage IdP Adapter Instances screen, click **Save** to complete the adapter configuration.

16. Configure or modify the connection(s) to your SP partner(s) using the RSA SecurID Adapter Instance.

Certification Checklist For RSA Authentication Manager v6.1

Date Tested: March 24, 2010

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	6.1	Windows 2003
PingFederate	6	Windows 2003

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	✓	Force Authentication After New PIN	N/A
System Generated PIN	✓	System Generated PIN	N/A
User Defined (4-8 Alphanumeric)	✓	User Defined (4-8 Alphanumeric)	N/A
User Defined (5-7 Numeric)	✓	User Defined (5-7 Numeric)	N/A
User Selectable	✓	User Selectable	N/A
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	N/A
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	N/A
Passcode			
16 Digit Passcode	✓	16 Digit Passcode	N/A
4 Digit Password	✓	4 Digit Password	N/A
Next Tokencode Mode			
Next Tokencode Mode	✓	Next Tokencode Mode	N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	N/A
Name Locking Enabled	✓	Name Locking Enabled	
No RSA Authentication Manager	✓	No RSA Authentication Manager	N/A

Additional Functionality			
RSA Software Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
RSA SecurID 800 Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
Credential Functionality			
Determine Cached Credential State	N/A	Determine Cached Credential State	
Set Credential	N/A	Set Credential	
Retrieve Credential	N/A	Retrieve Credential	

Known Issues

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.)*