

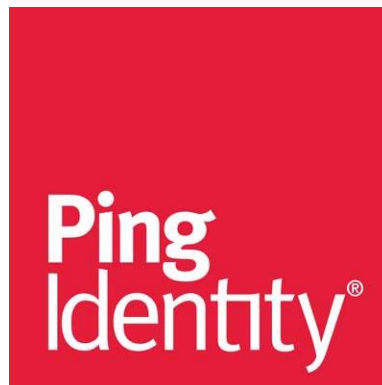


RSA Adaptive Authentication Implementation Guide

Last Modified: May 9, 2013

Partner Information

Product Information	
Partner Name	Ping Identity Corporation
Web Site	www.pingidentity.com
Product Name	PingFederate
Version & Platform	6.7 on Linux and Windows
Product Description	PingFederate is a cross domain Internet single sign-on server, also known as a federated single sign-on server. PingFederate allows for users to authenticate in one security domain and then seamlessly authenticate to, and access, applications in another security domain. The RSA Adaptive Authentication Integration Kit provides a stronger form of authentication before allowing the user to navigate to the target security domain.



Solution Summary

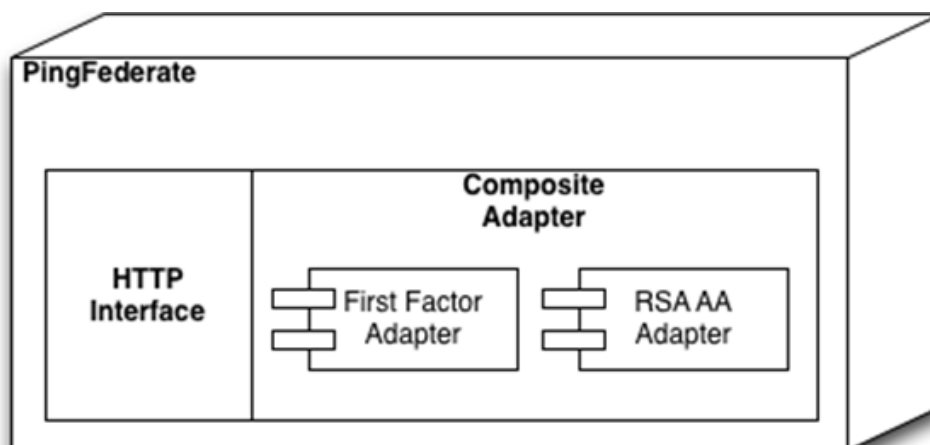
Ping Identity PingFederate integrates with RSA Adaptive Authentication (AA) using the Ping Identity RSA Adaptive Authentication Adapter which is part of the Ping Identity RSA Adaptive Authentication Integration kit.

When a user invokes an SSO transaction with PingFederate, a first-factor IdP Adapter processes it to validate an existing user session or to prompt the user for a first-factor authentication. The result of this step is that PingFederate is now aware of the user's username. Processing is then passed to the RSA Adaptive Authentication Adapter.

The RSA Adaptive Authentication Adapter first gathers device information and the Flash Shared Object (FSO) to perform an analyze call to RSA AA. Depending on the result, the RSA AA Adapter may then create a user account at RSA AA, query for enrollment questions, and prompt the user to enroll, or it may challenge the user to authenticate.

Further, in the event that the user's account is locked out, deleted, or otherwise denied, the RSA AA Adapter will report this account status back to the user.

RSA Adapted Authentication supported features Ping Identity Corporation PingFederate	
RSA Adaptive Authentication Hosted	No
RSA Adaptive Authentication On-Premise	Yes
RSA Adaptive Authentication User Enrollment	Yes
RSA Adaptive Authentication Login Authentication	Yes
RSA Adaptive Authentication Transaction Monitoring	No
RSA Adaptive Authentication Web/Mobile Browser Data Collection	Yes
RSA Adaptive Authentication Mobile Channel Data Collection	No
User Challenge Questions	Yes
Knowledge-based Authentication	No
Site-to-User Authentication	No
Out-of-Band Phone Authentication	No
Out-of-Band Email Authentication	No
Out-of-Band SMS Authentication	No



Partner Product Configuration

Before You Begin

This section provides instructions for installing and configuring PingFederate with RSA Adaptive Authentication.

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

Install the Ping Identity RSA Adaptive Authentication Integration Kit

1. From the /dist directory in the Integration Kit ZIP file, copy the following files to the <pf_install>/pingfederate/server/default/deploy directory:
`pf-rsa-adaptiveauthentication-adapter-1.0.jar`
`pf-rsa-adaptiveauthentication-war-1.0.war`
2. From the /dist directory in the Integration Kit ZIP file, copy the following file to the <pf_install>/pingfederate/server/default/lib directory:
`pf-rsa-adaptiveauthentication-soap-1.0.jar`
3. From the /templates directory in the Integration Kit ZIP file, copy the following files to the <pf_install>/pingfederate/server/default/conf/template directory:
`AdaptiveAuthenticationAdapter.challenge.with.question.template.html`
`AdaptiveAuthenticationAdapter.enroll.question.template.html`
`AdaptiveAuthenticationAdapter.fingerprint.retriever.template.html`
`AdaptiveAuthenticationAdapter.fso.setter.template.html`
`AdaptiveAuthenticationAdapter.status.message.template.html`
4. Start or restart PingFederate.

Configure the Ping Identity RSA Adaptive Authentication Adapter

1. Log on to the PingFederate administrative console and click **Adapters** under My IdP Configuration.
2. On the Type page, enter an **Instance Name**, an **Instance Id**, and select **RSA Adaptive Authentication IdP Adapter 1.0** from the **Type** dropdown, then click **Next**.



- Configure the fields as described on the **IdP Adapter** screen, and click **Next**.

PingFederate®

Configuring IdP Adapter [Help](#) | [Support](#) | [About](#) | [Logout \(Administrator\)](#)

[Main](#) | [Manage IdP Adapter Instances](#) | [Create Adapter Instance](#)

Type | **IdP Adapter** | Adapter Attributes | Summary

Complete the configuration necessary to look up user security contexts in your environment. This configuration was designed into the adapter for use at your site.

Field Name	Field Value	Description
RSA Adaptive Authentication WSDL URL	<input type="text" value="http://172.16.114.65/Adaptive"/>	The URL to your RSA Adaptive Authentication WSDL.
Caller ID	<input type="text" value="callerid"/>	The CallerId used when generating messages for RSA Adaptive Authentication.
Caller Credential	<input type="password" value="....."/>	The CallerCredential used when generating messages for RSA Adaptive Authentication.
Append Caller ID and Credential to WSDL URL?	<input checked="" type="checkbox"/>	Check to append the CallerId and CallerCredential to the WSDL URL in the form of <wsdl_url>&username=callerid&password=Password1!
Default Orgname	<input type="text"/>	This orgname will be used when calling RSA Adaptive Authentication in the event that the first-factor IdP Adapter does not populate an attribute called 'orgname'.
URL to pf-rsa-adaptiveauthentication-war	<input type="text" value="https://pf.efazendin.pingidenti"/>	This is the URL (E.g. https://<host.domain.com>/pf-rsa-adaptiveauthentication-war-0.7) to the pf-rsa-adaptiveauthentication-war web application. This web application provides javascripts and a flash movie, which help with registering the user's device.
Number of Challenge Questions	<input type="text" value="1"/>	This is the number of questions that should be requested from RSA Adaptive Authentication during a challenge and authenticate sequence.
Device Cookie Name	<input type="text" value="PMData"/>	The name of the cookie that will store the device token.
Device Cookie Domain	<input type="text" value=".efazendin.pingidentity.com"/>	The server domain, preceded by a period (e.g. .example.com). If no domain is specified, the value is obtained from the request.
Device Cookie Path	<input type="text" value="/"/>	The path for the cookie that contains the token.
Device Cookie Expires In	<input type="text" value="300"/>	The number of minutes before the RSA Adaptive Authentication device cookie expires. Set to -1 to create a session cookie.
Trusted Reverse Proxy IPs	<input type="text"/>	A comma separated list of IP addresses of trusted reverse proxies. If the source of the request comes from one of these IPs, the adapter will use the x-forwarded-for http header to represent the user's IP address to RSA Adaptive Authentication.

- On the **Adapter Attributes** screen, check **Pseudonym** for the subject attribute, and click **Next**.
- On the **Summary** screen, click **Done**.
- On the **Manage IdP Adapter Instances** screen, click **Save**.

Configure an SP Connection to use the RSA Adaptive Authentication Adapter

A Composite Adapter is mapped to an SP Connection in the same way that a traditional Adapter is mapped. More information can be found in the PingFederate Admin Manual.

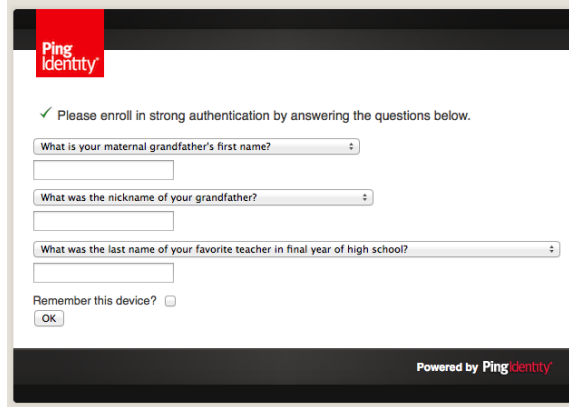
1. From the IdP Adapter Mapping page of an SP Connection, click **Map New Adapter Instance...**



2. On the Adapter Instance screen, select the Composite Adapter, and click **Next**.
3. On the Assertion Mapping screen, decide whether or not to retrieve additional attributes from a data store, and complete that configuration workflow if necessary.
4. On the Attribute Contract Fulfillment screen, map your attributes from your Composite Adapter and data sources into the Attribute Contract for this SP Connection, and click **Next**.
5. From the Summary screen, you can click **Done** and **Save** until you are back to the Main Menu, or complete any additional configuration required for your SP Connection.

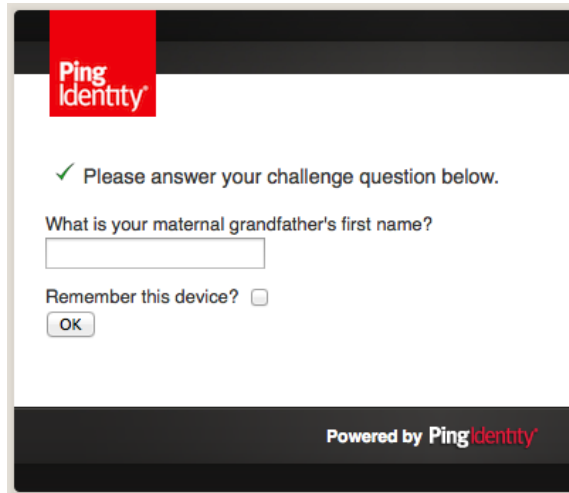
Screens

User Enrollment Screen:



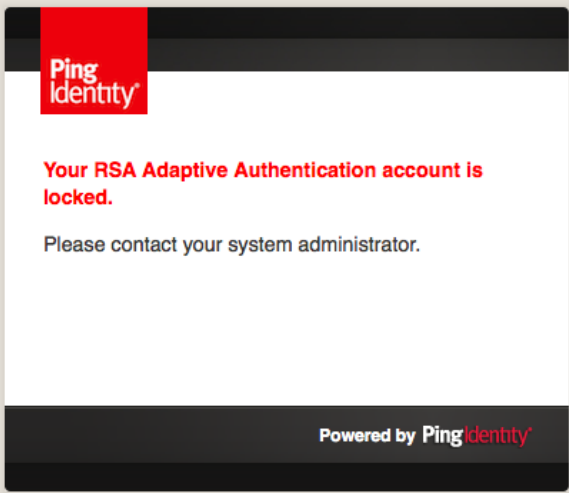
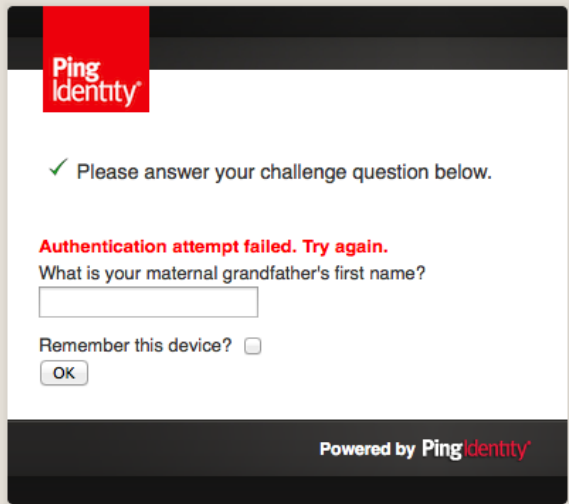
The User Enrollment Screen features the Ping Identity logo in the top left corner. Below the logo, a green checkmark icon is followed by the text "Please enroll in strong authentication by answering the questions below." There are three dropdown menus for selection: "What is your maternal grandfather's first name?", "What was the nickname of your grandfather?", and "What was the last name of your favorite teacher in final year of high school?". Each dropdown menu has a corresponding text input field below it. At the bottom left, there is a checkbox labeled "Remember this device?" and an "OK" button. The bottom right corner of the screen displays "Powered by Ping Identity".

Challenge Screen(s):



The Challenge Screen features the Ping Identity logo in the top left corner. Below the logo, a green checkmark icon is followed by the text "Please answer your challenge question below." The question "What is your maternal grandfather's first name?" is displayed above a single text input field. At the bottom left, there is a checkbox labeled "Remember this device?" and an "OK" button. The bottom right corner of the screen displays "Powered by Ping Identity".

Denial Screen(s):



Certification Checklist for RSA Adaptive Authentication Login

Date Tested: April 20, 2012

Certification Environment		
Product Name	Version	Operating System
Adaptive Authentication On Premise	6.0.2.1 SP3 P1	Cent OS 6.0

Product Name	Version	Operating System
Ping Identity PingFederate	6.7.0.2	Apple OS X 10.7.3
Ping Identity RSA Adaptive Authentication Integration Kit	1.0	Apple OS X 10.7.3

Login Monitoring			
On Premise		Hosted	
Analysis			
User Status		User Status	
Unknown Bank Users	<input checked="" type="checkbox"/>	Unknown Bank Users	<input type="checkbox"/> N/A
Unenrolled Users	<input checked="" type="checkbox"/>	Unenrolled Users	<input type="checkbox"/> N/A
Unverified Users	<input checked="" type="checkbox"/>	Unverified Users	<input type="checkbox"/> N/A
Deleted Users	<input checked="" type="checkbox"/>	Deleted Users	<input type="checkbox"/> N/A
Locked User Accounts	<input checked="" type="checkbox"/>	Locked User Accounts	<input type="checkbox"/> N/A
Unlocked User Accounts	<input checked="" type="checkbox"/>	Unlocked User Accounts	<input type="checkbox"/> N/A
Verified Users	<input checked="" type="checkbox"/>	Verified Users	<input type="checkbox"/> N/A
Notification		Notification	
Updates Server	<input type="checkbox"/> N/A	Updates Server	<input type="checkbox"/> N/A

Login Authentication			
On Premise		Hosted	
Analysis Response Actions		Analysis Response Actions	
Allow	<input checked="" type="checkbox"/>	Allow	<input type="checkbox"/> N/A
Review	<input checked="" type="checkbox"/>	Review	<input type="checkbox"/> N/A
Challenge	<input checked="" type="checkbox"/>	Challenge	<input type="checkbox"/> N/A
Deny	<input checked="" type="checkbox"/>	Deny	<input type="checkbox"/> N/A
Challenge Events		Challenge Events	
Challenges Unbound Devices	<input checked="" type="checkbox"/>	Challenges Unbound Devices	<input type="checkbox"/> N/A
Challenges High Risk Users	<input checked="" type="checkbox"/>	Challenges High Risk Users	<input type="checkbox"/> N/A

✓ = Pass ✗ = Fail N/A = Not Applicable to Integration

Checklist for RSA Adaptive Authentication Login (Continued)

Login Authentication (Continued)			
On Premise		Hosted	
Authentication Methods		Authentication Methods	
User Challenge Questions	<input checked="" type="checkbox"/>	User Challenge Questions	<input type="checkbox"/> N/A
Knowledge-based	<input type="checkbox"/> N/A	Knowledge-based	<input type="checkbox"/> N/A
Site-to-User	<input type="checkbox"/> N/A	Site-to-User	<input type="checkbox"/> N/A
Out of Band Phone	<input type="checkbox"/> N/A		
Out of Band Email	<input type="checkbox"/> N/A		
Out of Band SMS	<input type="checkbox"/> N/A		
External Authentication ¹	<input type="checkbox"/> N/A		
Authentication Policy		Authentication Policy	
Locks Account On Failed Attempts	<input checked="" type="checkbox"/>	Locks Account On Failed Attempts	<input type="checkbox"/> N/A
Credential Maintenance		Credential Maintenance	
Supports User Credential Maintenance	<input type="checkbox"/> N/A	Supports User Credential Maintenance	<input type="checkbox"/> N/A

✓ = Pass ✗ = Fail N/A = Not Applicable to Integration

Checklist for RSA Adaptive Authentication Device Data Collection

Web/Mobile Browser			
On Premise		Hosted	
Device Data		Device Data	
Device Fingerprint	<input checked="" type="checkbox"/>	Device Fingerprint	<input type="checkbox"/> N/A
Device Token Cookie	<input checked="" type="checkbox"/>	Device Token Cookie	<input type="checkbox"/> N/A
Device Token FSO	<input checked="" type="checkbox"/>	Device Token FSO	<input type="checkbox"/> N/A
HTTP Accept	<input checked="" type="checkbox"/>	HTTP Accept	<input type="checkbox"/> N/A
HTTP Accept Character Set	<input checked="" type="checkbox"/>	HTTP Accept Character Set	<input type="checkbox"/> N/A
HTTP Accept Encoding	<input checked="" type="checkbox"/>	HTTP Accept Encoding	<input type="checkbox"/> N/A
HTTP Accept Language	<input checked="" type="checkbox"/>	HTTP Accept Language	<input type="checkbox"/> N/A
HTTP Referrer	<input checked="" type="checkbox"/>	HTTP Referrer	<input type="checkbox"/> N/A
IP Address	<input checked="" type="checkbox"/>	IP Address	<input type="checkbox"/> N/A
User Identification Data		User Identification Data	
Username	<input checked="" type="checkbox"/>	Username	<input type="checkbox"/> N/A
User Logon Name	<input checked="" type="checkbox"/>	User Logon Name	<input type="checkbox"/> N/A
Org Name	<input checked="" type="checkbox"/>	Org Name	<input type="checkbox"/> N/A

✓ = Pass ✗ = Fail N/A = Not Applicable to Integration

¹ External authentication support implies that the implementation notifies the RSA Adaptive Authentication server of the authentication method's result each time it is called.

Checklist for RSA Adaptive Authentication Login Data Collection

Login Monitoring			
On Premise		Hosted	
Failed Login Notification Data		Failed Login Notification Data	
User Login ID	<input checked="" type="checkbox"/>	User Login ID	<input type="checkbox"/> N/A
User Type	<input checked="" type="checkbox"/>	User Type	<input type="checkbox"/> N/A
Login Authentication			
On Premise		Hosted	
Enrollment Data		Enrollment Data	
Run Risk Action Flag	<input checked="" type="checkbox"/>	Run Risk Action Flag	<input type="checkbox"/> N/A
Device Data	<input checked="" type="checkbox"/>	Device Data	<input type="checkbox"/> N/A
Device Action Type List	<input checked="" type="checkbox"/>	Device Action Type List	<input type="checkbox"/> N/A
Site-to-User Authentication Data		Site-to-User Authentication Data	
User Image	<input type="checkbox"/> N/A	User Image	<input type="checkbox"/> N/A
User Phrase	<input type="checkbox"/> N/A	User Phrase	<input type="checkbox"/> N/A
Notification Data		Notification Data	
Auto Create User Flag	<input type="checkbox"/> N/A	Auto Create User Flag	<input type="checkbox"/> N/A

PEW

✓ = Pass ✗ = Fail N/A = Not Applicable to Integration