IBM
Security Access Manager 7.0

RSA SecurID Ready Implementation Guide

Last Modified: July 8, 2013

Partner Information

Product Information	
Partner Name	IBM
Web Site	www.IBM.net
Product Name	IBM Security Access Manager
Version & Platform	7.0
Product Description	IBM Security Access Manager for Web, formerly called IBM Tivoli Access Manager for e-business, is a user authentication, authorization and web single sign-on solution for enforcing security policies over a wide range of web and application resources.

Solution Summary

IBM Security Access Manager (formally IBM Tivoli Access Manager for e-business) is an authentication and authorization solution for corporate web, client/server and existing applications. By providing a centralized, flexible, and scalable access control solution, Security Access Manager builds secure and easy-to-manage network-based applications and infrastructure.

IBM WebSEAL can be configured to support RSA SecurID two-factor authentication over the RSA Authentication Manager native protocol. The IBM Security Access Manager (ISAM) Security Runtime Environment for LINUX includes a custom library (*libxtokenauthn.so*) that was written against the RSA Authentication Agent API. You must install and configure an RSA PAM agent on your WebSEAL server machine so that the custom library can use it to communicate with RSA Authentication Manager.

IBM WebSEAL can also be configured to support RSA Risk-Based Authentication. When configured, users accessing resources protected by WebSEAL must authenticate using their username and either their static password or SecurID Passcode. If Authentication Manager determines the access attempt to be high-risk, the user must perform step authentication, providing either on On-Demand Tokencode delivered to an out-of-band device, or answers to life questions to complete authentication. Once authenticated, the user is granted access to the protected resource.

Supported RSA Features	
IBM Security Access Manager 7.0	
RSA SecurID Authentication via Native RSA SecurID Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	No
On-Demand Authentication via Native SecurID Protocol	Yes
On-Demand Authentication via RADIUS Protocol	No
Risk-Based Authentication	Yes
Risk-Based Authentication with Single Sign-On	No
RSA Authentication Manager Replica Support	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No

Authentication Agent Configuration

Authentication Agents are records that are stored in an RSA Authentication Manager server's database; they contain information that allows the server to locate its clients and establish secure communication channels with them. Use the RSA Security Console to create an agent record for each IBM WebSEAL server in your environment.

You will need the following information in order to do so:

- the hostname of each WebSEAL server in your environment
- IP address for all of the network interfaces on each WebSEAL sever host

Set each of your Authentication Agent's **Agent Type** to *Standard Agent*.

Note: Each agent hostname must resolve to one or more valid IP addresses on the local network.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	/var/ace/ or user defined
Node Secret	/var/ace/ or user defined
sdstatus.12	/var/ace/ or user defined
sdopts.rec	/var/ace/ or user defined

Note: The appendix of this document contains more detailed information regarding these files.

Risk-Based Authentication Integration Script

To protect a web-based application with Risk-Based Authentication (RBA), you must generate an integration script using the RSA Security Console, and deploy it to the applications default logon page. The script redirects the user from the web-based application's default logon page to a customized logon page that allows RSA Authentication Manager to authenticate the user with RBA.

The following steps should be taken prior to generating the integration script.

- Download the integration script template for IBM Security Access Manager from the following link: **https://sftp.rsa.com/human.aspx?Username=partner&password=rsasecured&arg01=915558427&arg12=downloaddirect&transaction=signon&quiet=true**
- Verify that the most recent RBA integration script template is installed on your Authentication Manager system by comparing the header of the installed integration script template to the header of the downloaded integration script template.
- Install the downloaded integration script template if it is newer than the installed script template, or if the script template for your agent is not installed.

Please refer to RSA documentation for more information on RBA integration scripts.

Configuration

Before You Begin

This section provides instructions for enabling RSA SecurID two-factor authentication for IBM Security Access Manager users. You should have working knowledge of IBM Security Access Manager and RSA Authentication Manager, as well as access to the appropriate end-user and administrative documentation. Ensure that that both products are running properly prior to configuring the integration. Note that this document is not intended to suggest optimum installations or configurations.

Enable Access to the RSA Authentication Agent Library

1. Install the RSA Authentication Agent 7.0 for PAM on each IBM WebSEAL server machine in your environment. Consult the *RSA Authentication Agent 7.0 for PAM—Installation and Configuration Guide for LINUX* for more information.
2. When you install the PAM agent, you will decide where to store the Authentication Manager *sdconf.rec* and node secret (*securid*) files. By default, WebSEAL searches for these files in a directory named */var/ace*. If you decide to store them in another directory, you must set the *VAR_ACE* environment to the correct path.
3. Perform a RSA Authentication Manager test authentication using the PAM agent's *acetest* utility. Consult the *RSA Authentication Agent 7.0 for PAM—Installation and Configuration Guide* for *LINUX* for instructions. This test will create an RSA node secret file the first time you complete a successful authentication.
4. Navigate to the *sdconf.rec*/node secret directory and run the following commands to set the proper permissions on the files:

```
chmod 444 sdconf.rec
chmod 444 securid
```

Configure RSA SecurID Token Authentication for IBM Secure Access Manager

To configure RSA SecurID token authentication:

1. Stop the WebSEAL server.
2. Open the WebSEAL configuration file (*webseald-<server_name>.conf*), find the *token* stanza and set its *token-auth* variable as follows:
   - If you wish to restrict RSA SecurID authentication to HTTP traffic: *token-auth = http*
   - If you wish to restrict RSA SecurID authentication to HTTPS traffic: *token-auth = https*
   - If you wish to enable RSA SecurID authentication for all traffic: t*oken-auth = both*

Note: If you wish to disable RSA SecurID authentication, set the variable's value to *none (token-auth = none*) and restart the WebSEAL server.

3. WebSEAL's LINUX runtime environment contains a custom library (*libxtokenauthn.so*) that uses the RSA Authentication API to communicate with RSA Authentication Manager. To enable this library, find the *[authentication-mechanisms]* stanza in the WebSEAL configuration file and set the *token-cdas* variable to the library's absolute path as follows:

   token-cdas = /opt/pdwebrte/lib/libxtokenauthn.so

4. Find the *[authentication-levels]* stanza and specify an authentication level for RSA SecurID authentication by setting a *level* variable as follows:

   level = token-card

Note: Refer to the *WebSEAL Administration* Guide for more information about configuring authentication levels.

5. Start the WebSEAL server.

Configure Risk-Based Authentication

1. Download the *am_integration.js* integration script file from the RSA Security Console.
2. Stop the WebSEAL server.
3. Locate the *tokenlogin.html* HTML response page for the WebSEAL instance for which you want to enable Risk-Based Authentication. The location of the HTML response pages can be found in the WebSEAL configuration file (*webseald-<server_name>.conf*). This location is defined by *mgt-pages-root* under the *[acnt-mgt]* stanza, and is relative to the *server-root* setting under the *[server]* stanza.
4. Paste the contents of *am_integration.js* into the *tokenlogin.html* response page as follows. You should create a <script> HTML tag and insert the code after the closing HTML </body> tag. Additions are shown below in red:

```
</BODY>
        <script type="text/javascript" language="Javascript">

        ***Paste contents of am_integration.js here

        </script>
        <script> window.onload=redirectToIdP(); </script>
</HTML>
```

5. Start the WebSEAL server. Users accessing resources protected by this WebSEAL instance are now redirected to the RSA Secure Logon page to complete Risk-Based Authentication before being granted access to resources. This page replaces the standard SecurID challenge page.

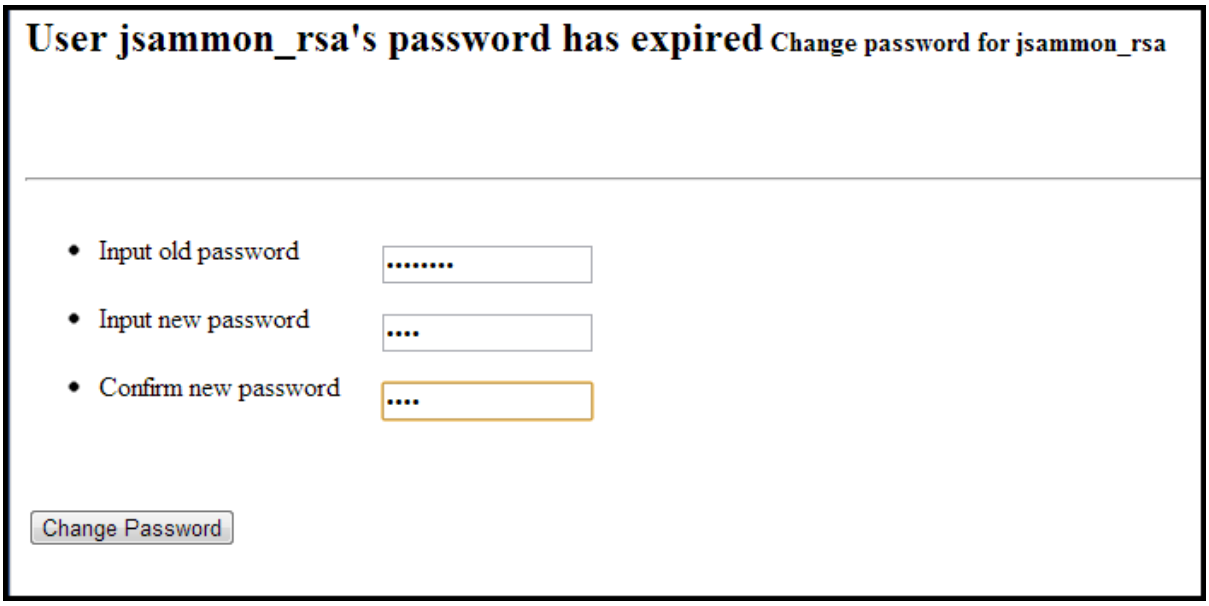
Login Screens

Note: This section contains screenshots of WebSEAL's default login screens for RSA SecurID authentication. See the *WebSEAL Administration* Guide for instructions to customize these screens.

Standard Logon Prompt

Important: WebSEAL's default New PIN Mode form is misleading. It's the same form that WebSEAL displays to prompt users to change their passwords (i.e. for standard password authentication).

The wording on the form instructs users to enter their old password and to enter and confirm their new password (see the screenshot below). However, when the form is used for New PIN Mode, a user must enter his/her passcode and enter and confirm his/her new PIN. You should customize this form so that it contains accurate instructions. See the *WebSEAL Administration* Guide for instructions to customize login screens.



New PIN Mode Prompt

Next Tokencode Prompt

Certification Checklist for RSA Authentication Manager

Date Tested: May 23, 2013

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager Appliance	8.0 (build 1356589)	LINUX Enterprise Server 11
RSA PAM Authentication Agent for Red Hat	7.0	CentOS 6
IBM Security Access Manager	7.0	CentOS 6

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	
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	N/A	
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	N/A	
Deny Numeric PIN	✓	Deny Numeric PIN	N/A	
Deny PIN Reuse	✓	Deny PIN Reuse	N/A	
Passcode				
16-Digit Passcode	✓	16-Digit Passcode	N/A	
4-Digit Fixed Passcode	✓	4-Digit Fixed Passcode	N/A	
Next Tokencode Mode				
Next Tokencode Mode	✓	Next Tokencode Mode	N/A	
On-Demand Authentication				
On-Demand Authentication	✓	On-Demand Authentication	N/A	
On-Demand New PIN	✓	On-Demand New PIN	N/A	
Load Balancing / Reliability Testing				
Failover (3-10 Replicas)	✓	Failover	N/A	
No RSA Authentication Manager	✓	No RSA Authentication Manager	N/A	

JGS

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

RSA Risk-Based Authentication Functionality			
RSA Native Protocol		**RADIUS Protocol**	
Risk-Based Authentication			
Risk-Based Authentication	✓	Risk-Based Authentication	N/A
Risk-Based Authentication with SSO	N/A	Risk-Based Authentication with SSO	N/A

MRQ

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

Known Issues

The ISAM integration doesn’t support RSA SecurID system-generated PINs.

The IBM Security Access Manager integration doesn’t support RSA SecurID system-generated PINs. A user whose token policy requires system-generated PINs will be denied access when his/her token enters New PIN Mode. When you deploy the integration, ensure that users are allowed to choose their PINs.

Appendix

Partner Integration Details	
RSA Authentication Agent Library	PAM 7.0 for Red Hat
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	Designated Users
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	YES (via PAM agent)

Node Secret:

When you install the PAM agent, you will decide where to store the Authentication Manager node secret (*securid*), *sdconf.rec*, *sdopts.rec* and *sdstatus.12* files. By default, WebSEAL searches for these files in a directory named */var/ace*. If you decide to store them in another directory, you must set the *VAR_ACE* environment to the correct path

sdconf.rec

See the **Node Secret** instructions above.

sdopts.rec

See the **Node Secret** instructions above.

sdstatus.12

See the **Node Secret** instructions above.