Integrating RSA Authentication Agent for Web with RSA® Authentication Manager 8.3 Risk-Based Authentication

This document describes how to integrate the RSA Authentication Agent for Web 7.1 and 8.0 with the risk-based authentication (RBA) feature of RSA® Authentication Manager 8.3.

Note: The RSA Authentication Agent for Web 8.0 can support TCP/IP networking. However, if you are using RBA, you must keep the default UDP networking support on the Web Agent.

It is assumed that you have a working knowledge of Authentication Manager.

For information about using RSA Authentication Manager 8.3 with risk-based authentication, see the RSA Authentication Manager Security Console Help.

Protect Web-Based Resources with Risk-Based Authentication

To protect web-based resources with risk-based authentication (RBA), you must download the RSA Authentication Agent for Web software and deploy the integration script to the agent's default logon page. The integration script redirects the user from the RSA Agent for Web default logon page to a logon page that allows Authentication Manager to authenticate the user with RBA.

RSA Authentication Agent for Web is software that performs as an agent that can add strong authentication to web-based resources. The RSA Agent for Web natively supports SecurID and on-demand authentication. You can make the RSA Agent for Web support RBA by adding the RBA integration scripts to the web-server or web application that you want to protect with RBA.

You need the following files, if you want to protect a web-based resource with RBA:

- **RSA Authentication Agent for Web software**—This software is not pre-installed on the Authentication Manager appliance. You must download this software.
- **RSA Authentication Manager integration script template**—This template is pre-installed on the Authentication Manager appliance.

Use the following steps to protect a web-based resource with RBA:

1. Integrating RSA Authentication Agent for Web with RSA® Authentication Manager 8.3 Risk-Based Authentication above
2. Add the Agent for Web to Authentication Manager on the next page
3. Install the Agent for Web Software on the next page
4. Make the SecurID Logon Page File Writable on the next page
5. Copy the Integration Script into the Agent for Web Logon Page on page 3
6. Configure the Agent for Web to Protect a Web-Based Resource on page 4

Download the RSA Authentication Agent for Web Software

Download the RSA Authentication Agent for Web software. Go to https://www.rsa.com/en-us/products-services/identity-access-management/securid/authentication-agents.

If an integration script template is available on the website or included with the agent software, confirm that you

have the latest version by comparing the existing template on the RSA Authentication Manager appliance to the one that you download.

The integration script template is an XML file that you can open in a text editor to find the version tag. Use the value in <Version>version number</Version> to compare versions of the integration script template.

If your integration script template on your Authentication Manager appliance is out of date, copy **RSAWebAgent.xml** to the **/opt/rsa/am/utils/rba_agents** directory. If you have more than one primary instance, for example, if you have a test environment and a production environment, copy the integration script template to each primary instance. You do not need to copy the template to replica instances.

Add the Agent for Web to Authentication Manager

You must add the Agent for Web to your Authentication Manager deployment, generate the integration script, and generate the configuration file. The integration script and the configuration file define the communication between an Agent for Web and Authentication Manager.

Procedure

1. On the RSA Security Console, go to **Access > Authentication Agents > Add New**, and add the Web agent.

   Note: Hostname and IP Address are required. Other fields are optional.

2. In the RBA section of the Authentication Agent page, click **Save Agent & Go to Download Page**.
3. In the **Integration Javascript** section, from the **Agent Type** drop down list select **RSA Authentication Agent for Web**.
4. Click **Download File** to generate and download the **am_integration.js** integration script for your authentication agent.
5. Go to **Access > Authentication Agents > Generate Configuration File**, and click **Generate Config File**.
6. Save the **AM_Config.zip** file where it is accessible when you install the agent.

   The **AM_Config.zip** file contains the **sdconf. rec** file that you will need when you install the Agent for Web.

Install the Agent for Web Software

Install the Agent for Web software, using the instructions provided with the software. The installer will prompt you for the **sdconf.rec** file that you created in the previous procedure.

Make the SecurID Logon Page File Writable

The SecurID Logon Page file on the RSA Agent for Web is named **useridandpasscode.htm**. You must make **useridandpasscode.htm** writable before you can add the integration script because this file is read-only by default.

The following are the default locations for **useridandpasscode.htm**:

- Windows: **C:\Program Files\RSA Security\RSAWebAgent\templates**

  Note: In case of an international locale, the **useridandpasscode.htm** file is also found in **C:\Program Files\RSA Security\RSAWebAgent\templates\nls\en-securid**.

- Apache: **/etc/httpd/rsawebagent/Templates**

You may have installed the agent in a different location.

Before you begin

Make sure to back up **useridandpasscode.htm** before editing it with the integration script.

Make the SecurID Logon Page File Writable

For Windows

1. Right-click **useridandpasscode.htm**, and select **Properties**.
2. Deselect **Read-only**, and click **OK**.

For Apache:

1. From a command shell, type

   ```
   chmod 644 useridandpasscode.htm
   ```

2. Press **Enter**.

Copy the Integration Script into the Agent for Web Logon Page

You must copy the integration script into the SecurID Logon Page integration template. The modification causes the Agent for Web logon page to redirect to the Authentication Manager logon page used for RBA.

Procedure

1. In the **am_integration.js** integration script file, copy all of the text except the comment at the top of the file.
2. In the **useridandpasscode.htm** file, paste the text that you copied from **am_integration.js** immediately before the **</script>** HTML tag.
3. Change the **<BODY>** tag as follows:

   - From: <BODY language="JavaScript" onload="findPlugins()”>
   - To: **<**BODY language="JavaScript" onload="redirectToIdP()">

   Note: For the useridandpasscode.htm file, inside en-securid, change the <BODY> tag as
   From: <BODY language="JavaScript" onload="authenticate()”>
   To: **<**BODY language="JavaScript" onload="redirectToIdP()">

4. Save the **useridandpasscode.htm** file.
5. Restart the Web server.
6. (Apache only) In the **/etc/httpd/rsawebagent/config** directory, run the configuration script. Type:

   ./config *server.domain.com*

7. (Apache only) Press ENTER twice, and disable the option to "Use separate user name and PASSCODE pages." (Option 3 in Web Agent 7.1 or option 2 in Web Agent 8.0).

Note: If a SharePoint site is being protected, then the administrator has to edit the useridandpasscode_fba.htm in addition to useridandpasscode.htm. In the useridandpasscode_fba.htm file, change the <BODY> tag as
From :<BODY language="JavaScript" onload="initPage()" onunload="check_cancel()"> and
To:<BODY language="JavaScript" onload="redirectToIdP()">

Configure the Agent for Web to Protect a Web-Based Resource

You must specify the web-based resource that you want the Agent for Web to protect. For instructions, see your Agent for Web documentation.

Support and Service

You can access community and support information on RSA Link at https://community.rsa.com. RSA Link contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

The RSA Ready Partner Program website at www.rsaready.com provides information about third-party hardware and software products that have been certified to work with RSA products. The website includes Implementation Guides with step-by-step instructions and other information on how RSA products work with third-party products.

Before You Call Customer Support

Please have the following information available when you call:

- Access to the RSA Authentication Manager appliance.
- Your license serial number. To locate the license serial number, do one of the following:
  - Look at the order confirmation e-mail that you received when your ordered the product. This e-mail contains the license serial number.
  - In the RSA Security Console, click **Setup** > **Licenses** > **Status > View Installed Licenses**. From the **License ID** drop-down menu, click **View**.
- The Authentication Manager appliance software version information. You can find this information in the top, right corner of the Quick Setup, or in the RSA Security Console. Log on to the Security Console, and click **Software Version Information**.

January 2018

Trademarks

Intellectual Property Notice

Open Source License