



RSA SecurID Ready Implementation Guide

Last Modified: December 15, 2014


Partner Information

Product Information	
Partner Name	Hitachi ID Systems Inc
Web Site	www.hitachi-id.com
Product Name	Password Manager
Version & Platform	Hitachi ID Password Manager 8.2.6, Connector Pack 2.5.1 (Windows 2012 R2)
Product Description	<p>Hitachi ID Password Manager is a total password management solution that includes password synchronization, self-service reset, security policy enforcement, profile builders, and more.</p> <p>The Hitachi ID Connector Pack includes connectors which are programs that enable software to integrate with target systems.</p>
Product Category	Provisioning



Solution Summary

Hitachi ID Password Manager 8.2.6 has been integrated with RSA Authentication Manager to support RSA SecurID two-factor authentication. The integration uses a Hitachi plug-in called *valiance.exe* and an out-of-the-box RSA Authentication Manager Web server agent, which is installed on the Password Manager server. Once these components have been configured, end-users can authenticate to the Password Manager Self-Service console using their RSA SecurID tokens.

 **Note:** Hitachi ID Password Manager can also be configured to enable self-service operations for RSA SecurID tokens.


See the *Hitachi ID Password Manager 8.2.6 Installation and Configuration Guide* or RSA partner Engineering's *Hitachi ID Password Manager 8.2.6 RSA Authentication Manager 8.1 Provisioning* implementation guide for details.

Hitachi ID Password Manager also supports RSA Risk-Based Authentication (RBA). Risk-Based Authentication strengthens RSA SecurID authentication and traditional password-based authentication by analyzing a user's behavior and device to identify potentially risky or fraudulent authentication attempts. If the assessed risk is unacceptable, RSA Authentication Manager will challenge the user with a secondary authentication method to further confirm the user's identity.

RSA SecurID supported features	
Hitachi Password Manager	
RSA SecurID Authentication via Native RSA SecurID Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	No
On-Demand Authentication via Native SecurID Protocol	No
On-Demand Authentication via API	No
RSA Authentication Manager Replica Support	Yes
Risk-Based Authentication	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No

Before You Begin

This document provides instructions for enabling RSA SecurID two-factor authentication for Hitachi ID Password Manager users. You should have working knowledge of RSA Authentication Manager and Hitachi ID Password Manager, as well as access to the appropriate end-user and administrative documentation. Ensure that both products are running properly prior to configuring the integration.

 **Note:** This document is not intended to suggest optimal installations or configurations.

You must also install the *valiace7.exe* Hitachi ID plug-in and an RSA Authentication Manager agent on the Hitachi ID Password Manager server before you proceed. See the *Hitachi ID Password Manager 8.2.6 Installation and Configuration Guide* for more information.

Authentication Agent Configuration


RSA Authentication Agents are custom or ready-made software applications that securely pass user authentication requests to and from RSA Authentication Manager. RSA provides the RSA Authentication Agent API for building custom agents, as well as a variety of out-of-the-box agents for protecting access to various operating systems and web resources.

All agents must be registered with RSA Authentication Manager in order for the server to locate them and establish secure communication channels with them. Use the RSA Security Console to register an agent for your Password Manager server

You need the following information to register a Password Manager agent:


- the hostname of the Password Manager server
- IP addresses for all of the Password Manager server's network interfaces

When you register an Authentication Agent, set its agent type to *Standard Agent*.

 **Note:** Hostnames must resolve to valid IP addresses on the local network.

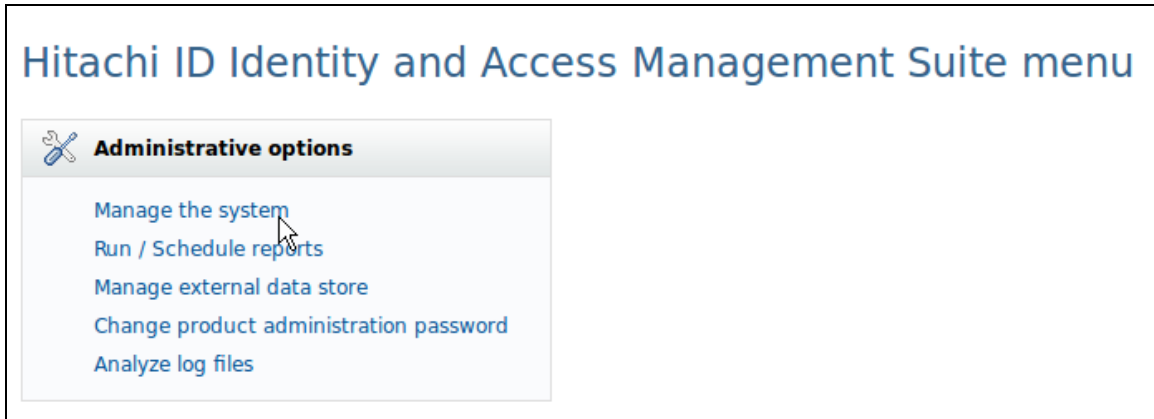
RSA SecurID files

RSA SecurID Authentication Files	
Files	Location
<i>sdconf.rec</i>	C:\Windows\System32
<i>Node Secret</i>	C:\Windows\System32
<i>sdstatus.12</i>	C:\Windows\System32
<i>sdopts.rec</i>	C:\Windows\System32

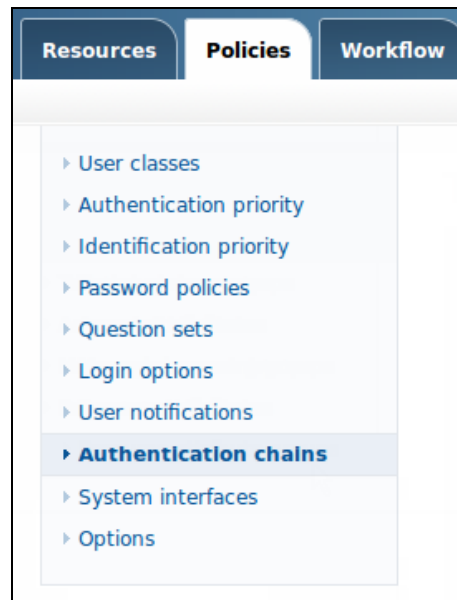
 **Note:** The appendix of this document contains more detailed information regarding these files.

Hitachi Password Manager SecurID Configuration

1. Log in to the Password Manager Self Service console and click the **Manage the system** link.



2. Select the **Policies** tab and click the **Authentication chains** link.



3. Click the **Add New** button at the bottom of the **Authentication Chains** table.

	ID	Description	Status	
<input type="checkbox"/>	DEFAULT_LOGIN	Default login service	✓	>
<input type="checkbox"/>	HELPDESK_LOGIN	Default help desk login service	✓	>
<input type="checkbox"/>	GENERIC_LOGIN_FAILURE	Default generic login failure service	✓	>
<input type="checkbox"/>	USER_IDENTIFICATION	User identification service	✓	>
		Disable	Add new...	

4. Enter a unique name for the chain in the **ID** field.
5. Enter a description of the chain in the **Description** field.
6. Click the **Add** button.

Authentication chain information

ID * RSACHAIN

Description: * RSA Authentication Manager Chain

Enabled:

Add

7. Click the **Add new...** button in the **Modules** section.

Authentication chain information

ID * RSACHAIN

Description: * RSA Authentication Manager Chain

Enabled:

Modules:

Module	Control type	Description	Parameters	Order
Add new...				

8. Select *External program* from the **Module** drop-down list
9. Select the binding radio button from the **Control Type** options group.
10. Click the **Update** button.

Module configuration:

Module: * External program

Control type: * **binding** - if the module succeeds and no earlier module in the chain has failed, the chain is immediately terminated and access is granted. If the module fails, the rest of the chain is executed, but access is ultimately denied.


required - if the module succeeds, the rest of the chain is executed. If all modules fail, access is granted. If any module fails, access is denied. If all modules succeed, access is granted. If any module fails, access is denied.

sufficient control type, at least one module must succeed in order for access to be granted.

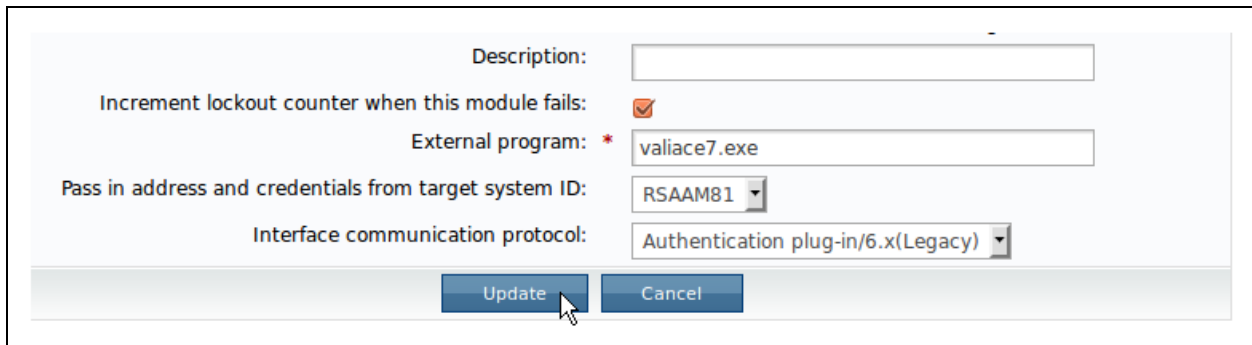
Description:

Update Cancel

11. Scroll to the bottom of the page and optionally check the checkbox labeled **Increment lockout counter when this module fails**.
12. Enter *valiace7.exe* in the **External program** field.
13. If you wish to make RSA SecurID authentication available for all users, leave the **Pass in address and credentials from target system ID** field empty. Otherwise, set the field's value to the name of the target system where SecurID authentication should be enabled.

 **Note:** In the example below, RSA SecurID would only be enabled in the *RSAAM81* target system

14. Select *Authentication plug-in/6.x (Legacy)* from the **Interface communication protocol** list.

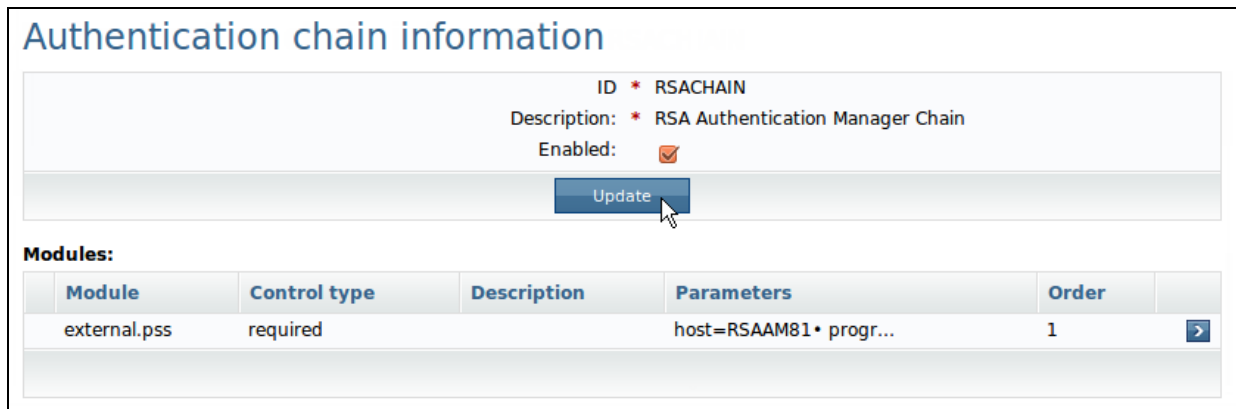


The screenshot shows a configuration form with the following fields and values:

- Description: [Empty text box]
- Increment lockout counter when this module fails:
- External program: * valiace7.exe
- Pass in address and credentials from target system ID: RSAAM81
- Interface communication protocol: Authentication plug-in/6.x(Legacy)


At the bottom of the form are two buttons: "Update" and "Cancel". A mouse cursor is pointing at the "Update" button.

15. Check the **Enabled** checkbox and lick the **Update** button.

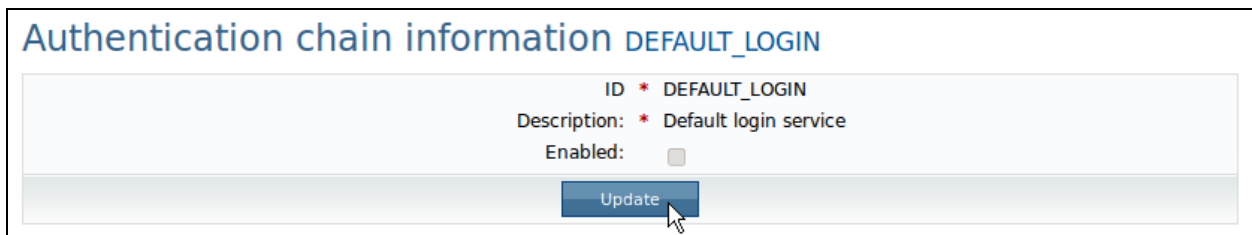


The screenshot shows the "Authentication chain information" page for the chain ID **RSACHAIN**. The description is "RSA Authentication Manager Chain" and the "Enabled" checkbox is checked. An "Update" button is visible below the form.

Modules:

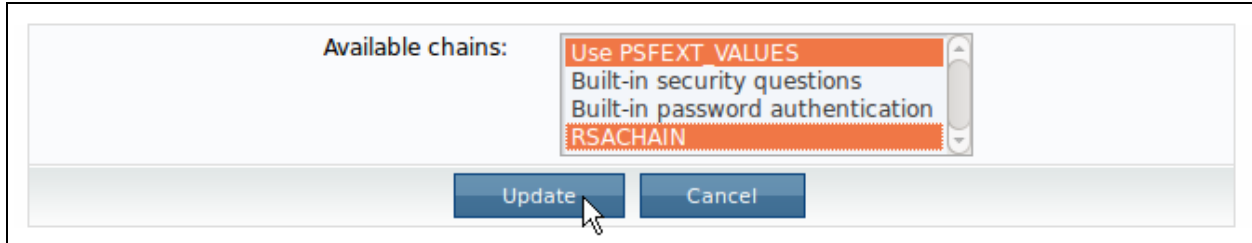
Module	Control type	Description	Parameters	Order	
external.pss	required		host=RSAAM81 • progr...	1	

16. Select the **Policies** tab, click the **Authentication chains** link and elect the **DEFAULT_LOGIN** chain in **the Authentication Chains** table.
17. Uncheck the **Enabled** checkbox to disable the authentication chain and click the **Update** button.

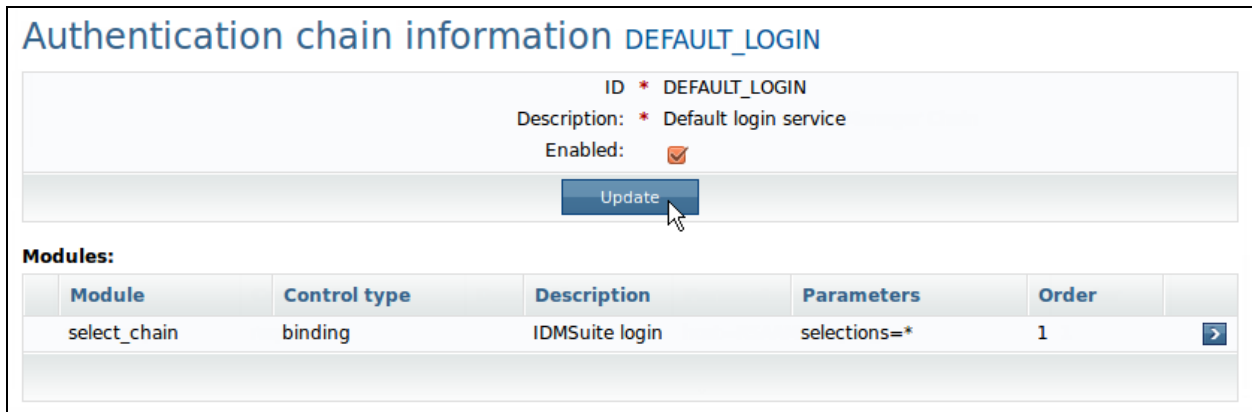


The screenshot shows the "Authentication chain information" page for the chain ID **DEFAULT_LOGIN**. The description is "Default login service" and the "Enabled" checkbox is unchecked. An "Update" button is visible below the form.

18. Click the **select_chain** module and scroll to the bottom of the page.
19. Hold the control button on your keyboard and **select the name of your RSA Authentication Manager authentication chain** from the **Available Chains** list.
20. Click the **Update** button.




21. Check the **Enabled** checkbox to enable the default login chain again.
22. Click the **Update** button.



Risk-Based Authentication Configuration

If you plan to enable RSA Risk-Based Authentication (RBA) for Hitachi-ID Password Manager, you have to [configure RSA SecurID authentication](#) first. Once you have done so, follow the instructions below.

 **Note:** In order for an application to support RBA, it must also support RSA SecurID authentication. Before you configure RBA for Password Manager, make sure you have enabled RSA SecurID authentication. RBA **does not** require RSA SecurID tokens.

To enable RBA for Password Manager, you must generate a JavaScript file from a custom template, copy it to your Password Manager server and modify Password Manager's standard RSA SecurID login page.

Install or Update the Password Manager RBA Template

1. Download the Hitachi ID Password Manager RBA integration script template and save it to a temporary directory:
<https://sftp.rsa.com/human.aspx?Username=partner&password=rsasecured&arg01=153382526&arg12=downloaddirect&transaction=signon&quiet=true>
2. Connect to your RSA Authentication Manager server's virtual appliance using an SCP or SSH client, navigate to the `/opt/rsa/am/utills/rba-agents` directory and see if it contains a Hitachi-ID Password Manager template. The template will be named `HitachiID_Password_Manager_<version>.xml`.
3. If you find a Password Manager RBA template, and it's same as or newer than the one you downloaded, skip step 4 and continue to the [Generate the Password Manager RBA JavaScript File](#) section.
4. Upload the `HitachiID_Password_Manager_8.2.6.xml` file from your temporary directory to the `/opt/rsa/am/utills/rba-agents` directory and disconnect your SCP/SSH client session.

Generate the Password Manager RBA JavaScript File

1. Log in to the RSA Authentication Manager Security Console, open your Hitachi-ID Password Manager agent for editing, scroll to the Risk-based Authentication section and check the **Enable this Agent for risk-based authentication** checkbox.
2. Set the access restriction and authentication method options based on your requirements and click the **Save agent & Go to Download Page** button.
3. Select *Hitachi ID Password Manager 8.2.6* from the **Agent Type** list box and click the **Download File** button.

Integration Javascript

Select the agent type and download the integration script that you will use to configure RBA for this RSA Authentication Agent. For more information, see the Administrator's Guide and the Implementation Guide for your agent, which is available at RSAsecured.com. Save the file when prompted.

Agent Type:

Filename: am_integration.js

Download: Click to download the integration script for the Pulse Connect Secure 8.0.

4. RSA Authentication Manager will generate a JavaScript file named *am_integration.js*. Copy the file to the *C:\Program Files (x86)\Hitachi ID\DM Suite\%INSTANCE%\wwwdocs\default\js* directory on your Password Manager server, where *%INSTANCE%* is the name of your Password Manager server instance.
5. Navigate to the *C:\Program Files (x86)\Hitachi ID\DM Suite\%INSTANCE%\design\src\common* directory and open the *authchain.m4* file for editing.
6. Insert the following lines between the *%HIDDEN_VIEWS%* and *%AUTH_VIEWS%* variables:

```
<script src="_JSDIR/am_integration.js?_CACHEENUM" type="text/javascript"><script>  
<input type="hidden" name="USER_IDENT_AM" value="%LOGGEDIN_USERID%" />
```

7. Navigate to the *C:\Program Files (x86)\Hitachi ID\DM Suite\%INSTANCE%\design\src\common* directory and open the *authchain.m4* file for editing. “
8. Insert the lines below between the *%AUTH_VIEWS%* variable and the *INCLUDE FOOTER* section:

```
<script type="text/javascript">  
  window.addEventListener( 'load', function( e ){  
    if( document.getElementById( 'input[name=01]' ) )  
      redirectToIdP();  
  });  
</script>
```

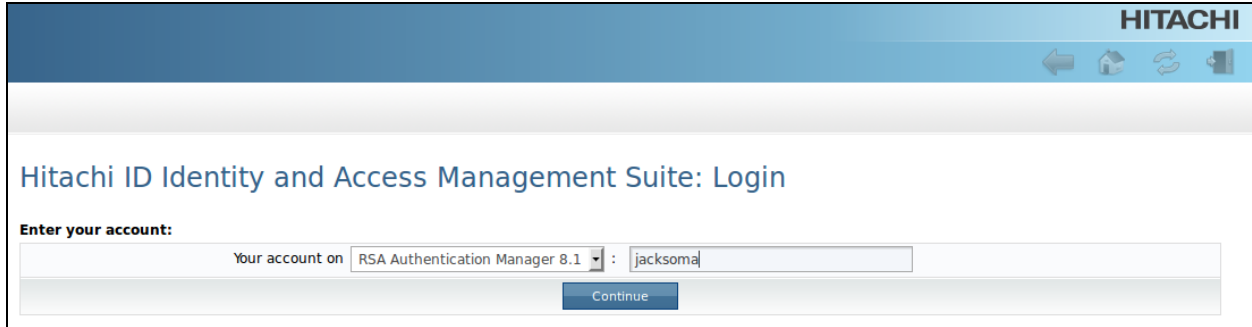
When you're done modifying the page, the section described above should look like the snippet below:

```
%HIDDEN_VIEWS%  
  
<script src="_JSDIR/am_integration.js?_CACHEENUM" type="text/javascript"><script>  
<input type="hidden" name="USER_IDENT_AM" value="%LOGGEDIN_USERID%" />  
  
%AUTH_VIEWS%  
  
<script type="text/javascript">  
  window.addEventListener( 'load', function( e ){  
    if( document.getElementById( 'input [name=01]' ) )  
      redirectToIdP();  
  });  
</script>  
  
INCLUDE FOOTER
```

9. Navigate to the *C:\Program Files (x86)\Hitachi ID\DM Suite\%INSTANCE%\design* directory, and type *make default %LANGUAGE_CODE%*, where *%LANGUAGE_CODE%* is the code for the language of the page you are modifying. For example

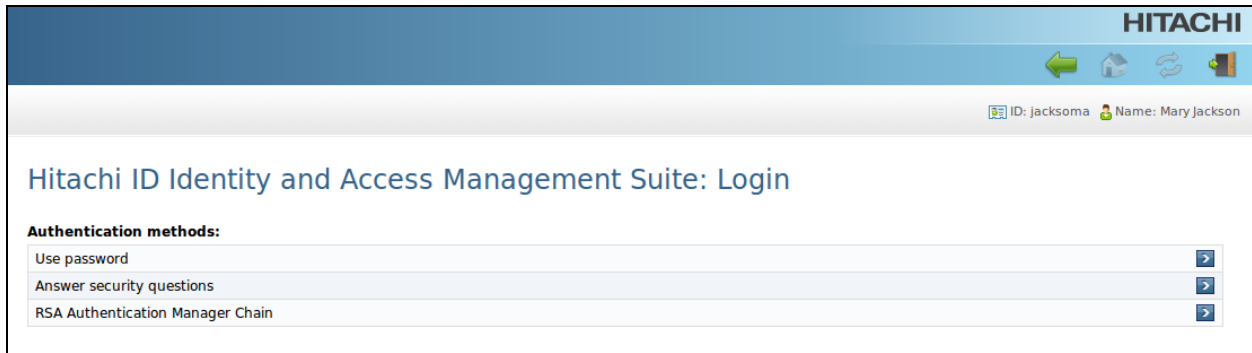
```
make default en-us
```
10. Once the previous command is completed, type *make install default %LANGUAGE_CODE%*

RSA SecurID Login Screens



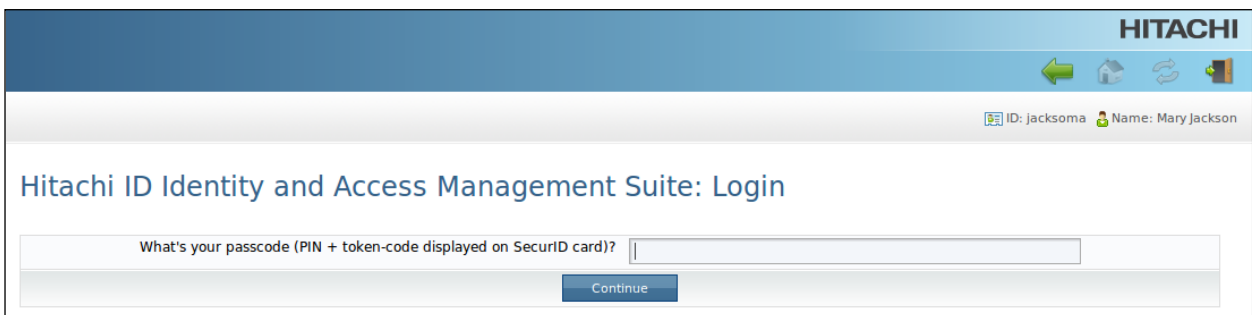
The screenshot shows the top navigation bar with the 'HITACHI' logo and navigation icons. Below the header, the page title is 'Hitachi ID Identity and Access Management Suite: Login'. The main content area is titled 'Enter your account:'. It features a dropdown menu for 'Your account on' set to 'RSA Authentication Manager 8.1', followed by a text input field containing 'jacksoma'. A 'Continue' button is positioned below the input field.

Login ID Prompt



The screenshot shows the top navigation bar with the 'HITACHI' logo and navigation icons. Below the header, the page title is 'Hitachi ID Identity and Access Management Suite: Login'. The main content area is titled 'Authentication methods:'. It lists three options: 'Use password', 'Answer security questions', and 'RSA Authentication Manager Chain', each with a right-pointing arrow button. At the top right of the main content area, the user's ID 'jacksoma' and name 'Mary Jackson' are displayed.

Select Authentication Method Prompt



The screenshot shows the top navigation bar with the 'HITACHI' logo and navigation icons. Below the header, the page title is 'Hitachi ID Identity and Access Management Suite: Login'. The main content area is titled 'What's your passcode (PIN + token-code displayed on SecurID card)?'. It features a text input field for the passcode and a 'Continue' button below it. At the top right of the main content area, the user's ID 'jacksoma' and name 'Mary Jackson' are displayed.

RSA SecurID Passcode Prompt

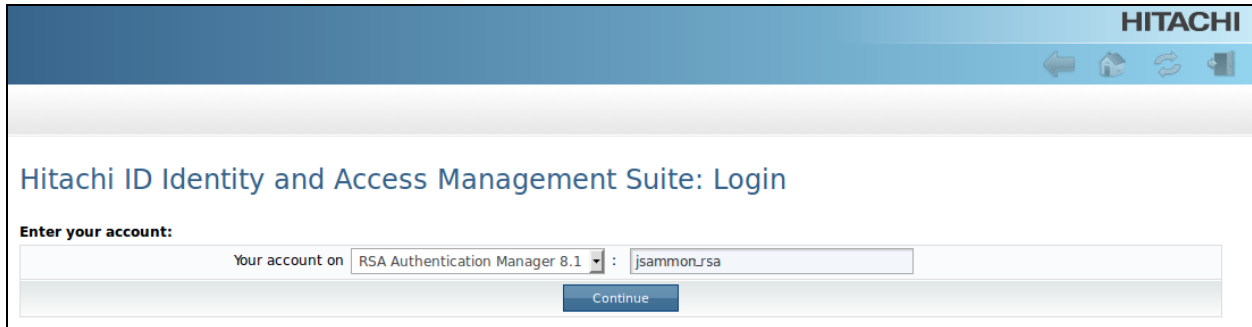
The screenshot shows the Hitachi ID Identity and Access Management Suite login page. At the top right, the HITACHI logo is displayed. Below it, there are navigation icons (back, home, refresh, forward) and user information: ID: jacksoma and Name: Mary Jackson. The main heading is "Hitachi ID Identity and Access Management Suite: Login". The form contains three input fields: the first is for the passcode (PIN/password + token code), the second is for a new PIN (4-8 characters long, alphanumeric), and the third is for the next token code. A "Continue" button is located at the bottom of the form.

New PIN Mode Prompt

This screenshot is identical to the one above, showing the "New PIN Mode Prompt" on the Hitachi ID Identity and Access Management Suite login page. It includes the HITACHI logo, user information (ID: jacksoma, Name: Mary Jackson), the login heading, and the three input fields for passcode, new PIN, and next token code, along with the "Continue" button.

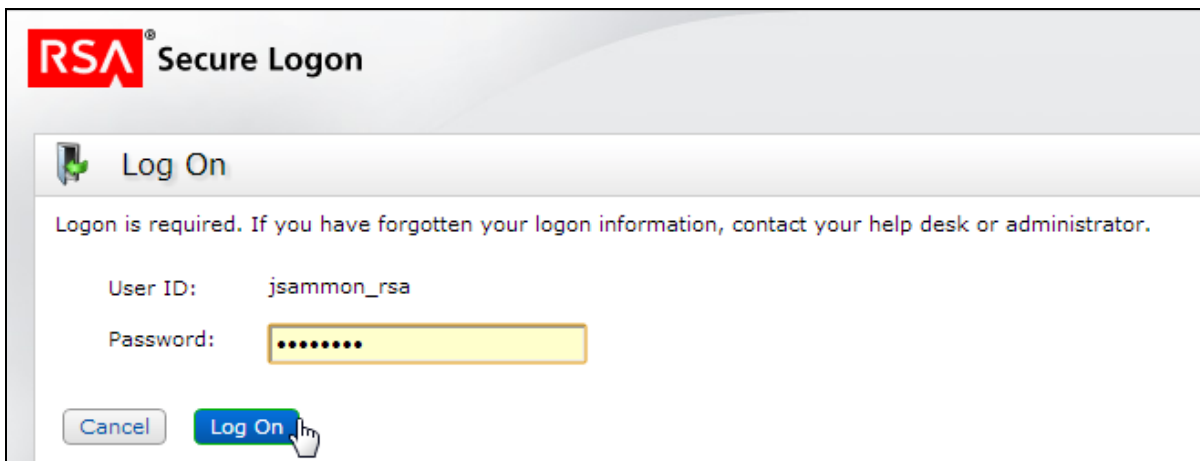
Next Tokencode Prompt

RSA RBA Login Screens



The screenshot shows a web browser window with a blue header bar containing the "HITACHI" logo and navigation icons. Below the header, the page title is "Hitachi ID Identity and Access Management Suite: Login". The main content area is titled "Enter your account:" and contains a form with a dropdown menu set to "RSA Authentication Manager 8.1" and a text input field containing "jsammon_rsa". A "Continue" button is positioned below the input field.

Hitachi ID Password Manager Login ID Prompt:



The screenshot shows a "RSA Secure Logon" dialog box. The title bar includes the RSA logo and the text "Secure Logon". Below the title bar, there is a "Log On" header with a green checkmark icon. The main text reads: "Logon is required. If you have forgotten your logon information, contact your help desk or administrator." Below this text, the "User ID:" field is populated with "jsammon_rsa". The "Password:" field is a yellow box filled with seven black dots. At the bottom, there are two buttons: a "Cancel" button and a "Log On" button with a mouse cursor hovering over it.

RBA Password Logon Prompt

RSA[®] Secure Logon

Help Verify Your Identity

For enhanced security, you must verify your identity.

* Required field

Identity Confirmation: Security Questions

Confirm your identity by answering 1 security questions. You must enter answers in the same language that that you used during enrollment. Answers are not case-sensitive.

Last name of your primary teacher in the sixth grade/year

*

RBA Challenge Question Logon Prompt

Remember this Computer

Select whether you want the system to remember this computer.

Yes, I plan to use this computer in the future.

No, this is a public computer or one I do not use often.

RBA Device-Binding Option Prompt:

Certification Checklist for RSA Authentication Manager

Date Tested: November 25, 2014

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	8.1	
Hitachi ID Password Manager	8.2.6	Windows 2012 R2
Hitachi ID Connector Pack	2.5.1	Windows 2012 R2

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
New PIN Mode			
Force Authentication After New PIN	<input checked="" type="checkbox"/>	Force Authentication After New PIN	<input type="checkbox"/> N/A
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input type="checkbox"/> N/A
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input type="checkbox"/> N/A
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input type="checkbox"/> N/A
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input type="checkbox"/> N/A
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input type="checkbox"/> N/A
Deny Numeric PIN	<input checked="" type="checkbox"/>	Deny Numeric PIN	<input type="checkbox"/> N/A
Deny PIN Reuse	<input checked="" type="checkbox"/>	Deny PIN Reuse	<input type="checkbox"/> N/A
Passcode			
14 Digit Passcode	<input checked="" type="checkbox"/>	14 Digit Passcode	<input type="checkbox"/> N/A
4 Digit Fixed Passcode	<input checked="" type="checkbox"/>	4 Digit Fixed Passcode	<input type="checkbox"/> N/A
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input type="checkbox"/> N/A
On-Demand Authentication			
On-Demand Authentication	<input type="checkbox"/> X	On-Demand Authentication	<input type="checkbox"/> N/A
On-Demand New PIN	<input type="checkbox"/> X	On-Demand New PIN	<input type="checkbox"/> N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input type="checkbox"/> N/A
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input type="checkbox"/> N/A

JGS / PAR

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

RSA Risk-Based Authentication Functionality			
RSA Native Protocol		RADIUS Protocol	
Risk-Based Authentication			
Risk-Based Authentication	<input checked="" type="checkbox"/>	Risk-Based Authentication	<input type="checkbox"/> NA
Risk-Based Authentication with SSO	<input type="checkbox"/> NA	Risk-Based Authentication with SSO	<input type="checkbox"/> NA

JGS

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

Appendix

Partner Integration Details	
RSA SecurID API	8.1 SP1
RSA Authentication Agent Type	Web Agent
RSA SecurID User Specification	Designated Users
Display RSA Server Info	yes
Perform Test Authentication	no
Agent Tracing	yes

RSA Configuration Files

Node Secret:

Password Manager stores the node secret in the *C:\Windows\System32* directory.

sdconf.rec:

Password Manager stores the *sdconf.rec* file in the *C:\Windows\System32* directory.

sdopts.rec:

Password Manager stores the *sdopts.rec* file in the *C:\Windows\System32* directory.

sdstatus.12:

Password Manager stores the *sdstatus.12* file in the *C:\Windows\System32* directory.

Known Issues

The integration doesn't support RSA On-Demand tokens.

The Hitachi ID Password Manager integration doesn't support on-demand tokens.