Hitachi ID Systems Inc

Identity Manager 8.2.6

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	Identity Manager
Version & Platform	Hitachi ID Identity Manager 8.2.6, Connector Pack 2.5.1 (Windows 2012 R2)
Product Description	Hitachi ID Identity Manager is an integrated solution for managing identities and security entitlements across multiple systems and applications. Organizations depend on Identity Manager to ensure that users get security entitlements promptly, are always assigned entitlements appropriate to their needs and in compliance with policy and are deactivated reliably and completely when they leave the organization. The Hitachi ID Connector Pack includes connectors which are programs that enable software to integrate with target systems.
Product Category	Provisioning

Hitachi ID Systems, Inc.

Solution Summary

Hitachi ID Identity 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 Identity Manager server. Once these components have been configured, users can authenticate to the Identity Manager console using their RSA SecurID tokens.

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

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

Hitachi ID Identity 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 Identity 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
RSA SecurID Protection of Administrative Interface	No

Before You Begin

This document provides instructions for enabling RSA SecurID two-factor authentication for Hitachi ID Identity Manager users. You should have working knowledge of RSA Authentication Manager and Hitachi ID Identity 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: 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 Identity Manager server before you proceed. See the *Hitachi ID Identity 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 Identity Manager server

You need the following information to register a Connect Secure agent:

- the hostname of the Identity Manager server
- IP addresses for all of the Identity 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

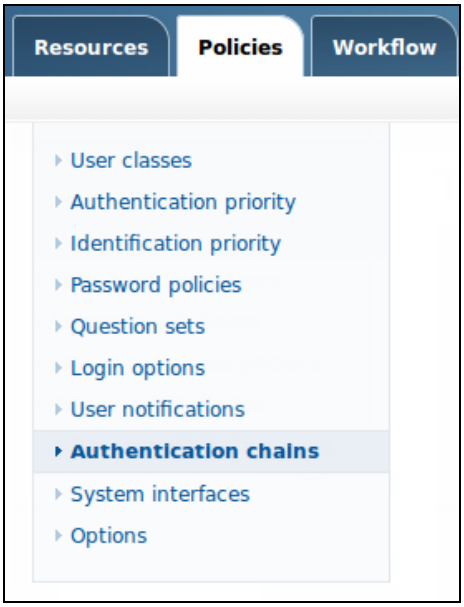
RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	*C:\Windows\System32*
Node Secret	*C:\Windows\System32*
sdstatus.12	*C:\Windows\System32*
sdopts.rec	*C:\Windows\System32*

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

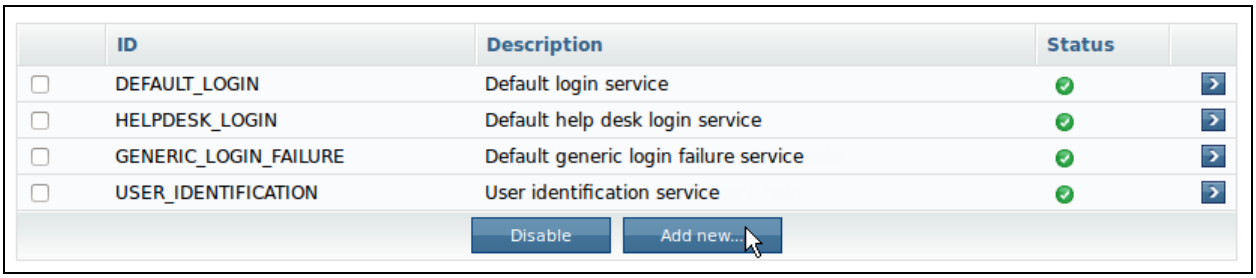
Hitachi Identity Manager SecurID Configuration

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

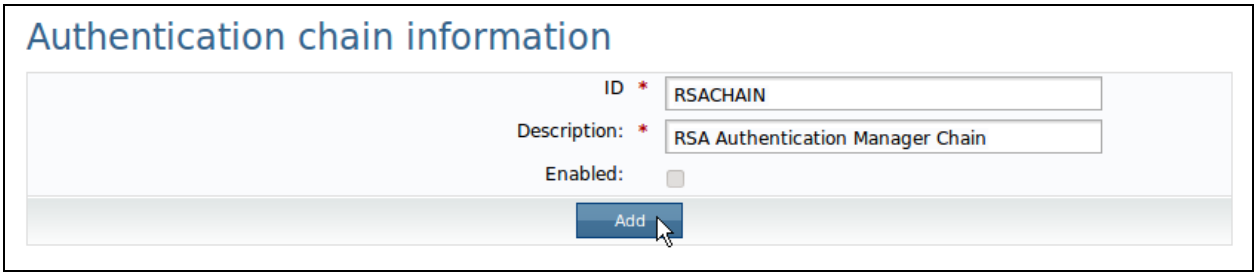
2. Select the **Policies** tab and click the **Authentication chains** link.



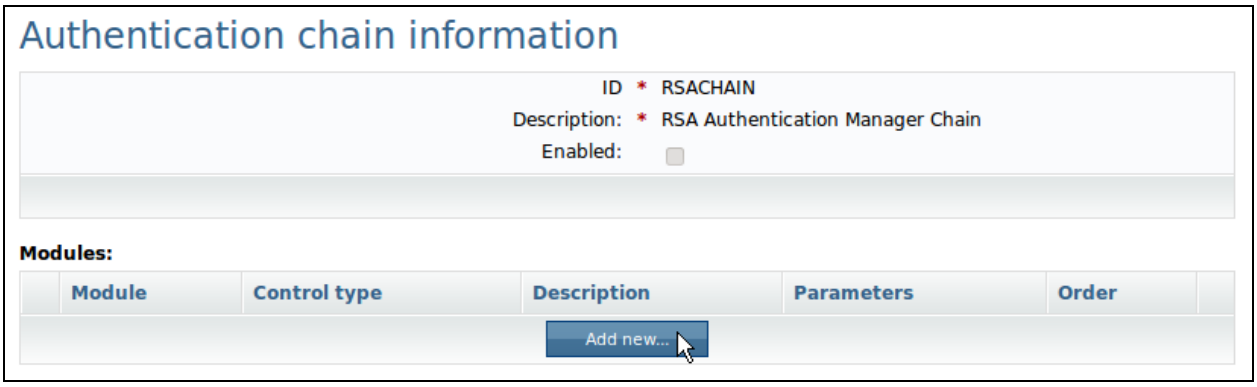
3. Click the **Add New** button at the bottom of the **Authentication Chains** table.



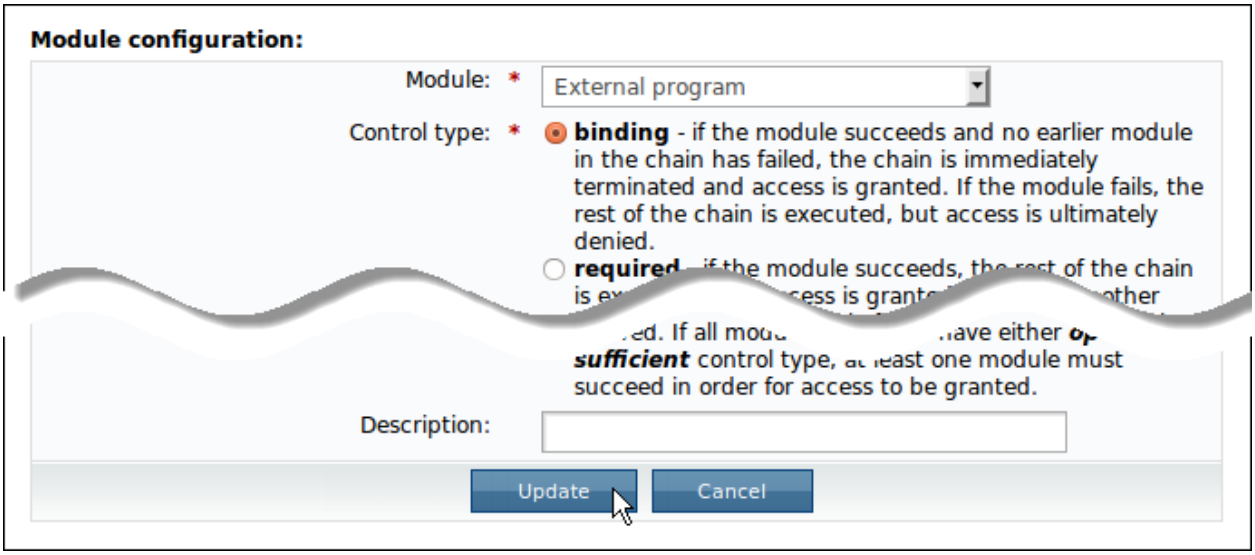
4. Enter a unique name for the chain in the **ID** field.
5. Enter a description of the chain in the **Description** field.
6. Click the **Add** button.



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



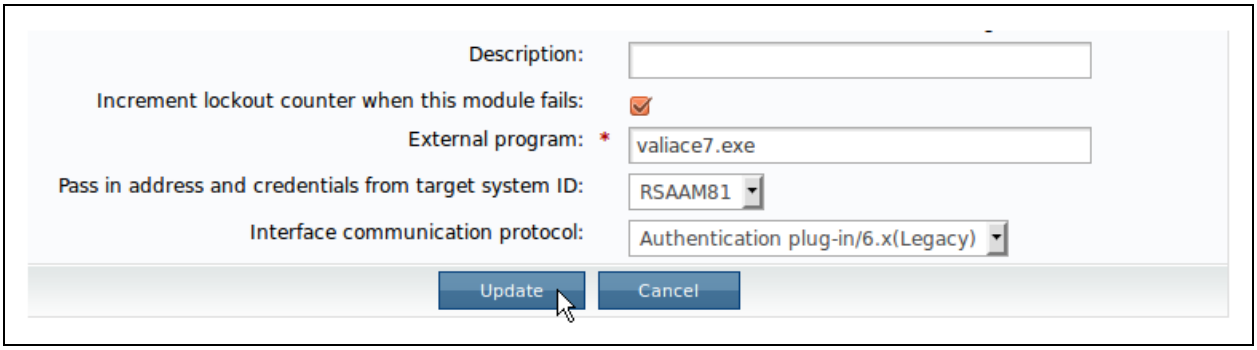
8. Select *External program* from the **Module** drop-down list
9. Select the binding radio button from the **Control Type** options group.
10. Click the **Update** button.



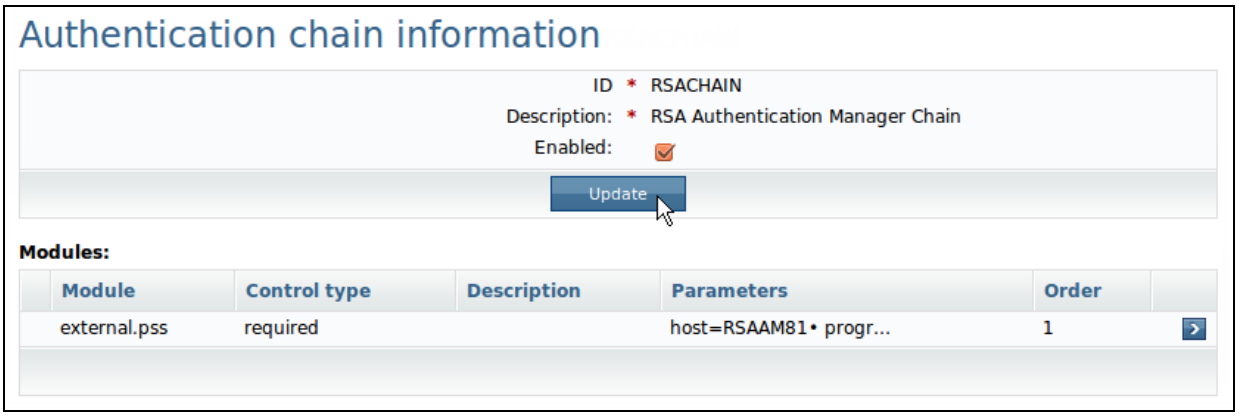
11. Scroll to the bottom of the page and optionally check the checkbox labeled Increment **lockout counter when this module fails**.
12. Enter *valiace7.exe* in the **External program** field.
13. If you wish to make RSA SecurID authentication available for all users, leave the ***Pass in address and 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

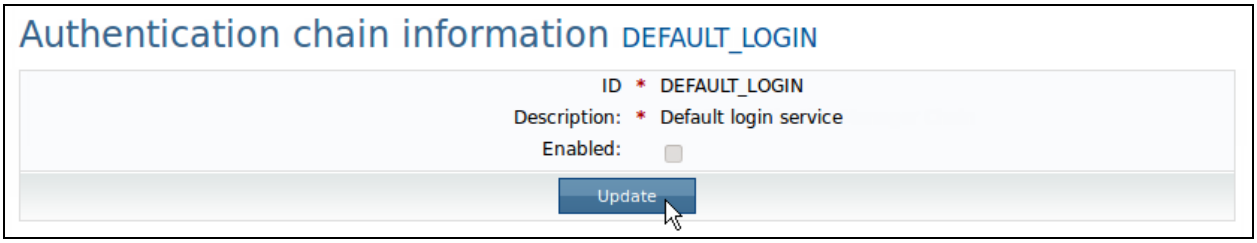
14. Select *Authentication plug-in/6.x (Legacy)* from the **Interface communication protocol** list.



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

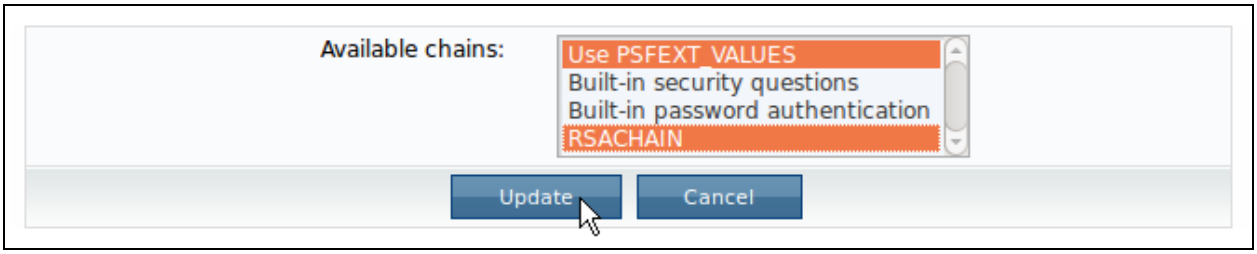


16. Select the **Policies** tab, click the **Authentication chains** link and elect the DEFAULT_LOGIN chain in **the Authentication Chains** table.
17. Uncheck the **Enabled** checkbox to disable the authentication chain and click the **Update** button.

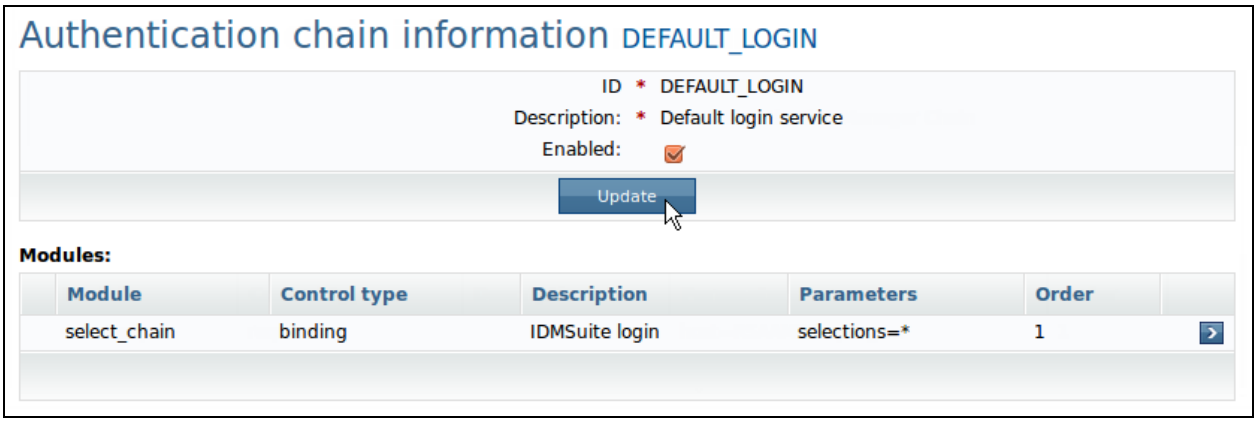


18. Click the **select_chain** module and scroll to the bottom of the page.

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 Identity 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 Identity Manager, make sure you have enabled RSA SecurID authentication. RBA **does not** require RSA SecurID tokens.

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

Install or Update the Identity Manager RBA Template

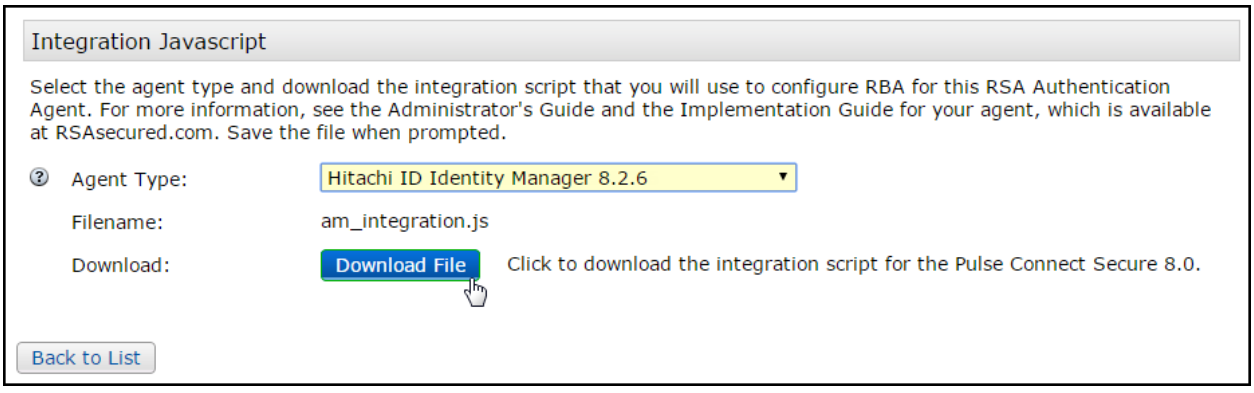
1. Download the Hitachi ID Identity Manager RBA integration script template and save it to a temporary directory:

   https://sftp.rsa.com/human.aspx?Username=partner&password=rsasecured&arg01=153374119&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/utils/rba-agents* directory and see if it contains a Hitachi-ID Identity Manager template. The template will be named *HitachiID_Identity_Manager_<version>.xml*.
3. If you find an Identity Manager RBA template, and it's same as or newer than the one you downloaded, skip step 4 and continue to the Generate the Identity Manager RBA JavaScript File section.
4. Upload the *HitachiID_Identity_Manager_8.2.6.xml* file from your temporary directory to the */opt/rsa/am/utils/rba-agents* directory and disconnect your SCP/SSH client session.

Generate the Identity Manager RBA JavaScript File

1. Log in to the RSA Authentication Manager Security Console, open your Hitachi-ID Identity 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 Identity Manager 8.2.6* from the **Agent Type** list box and click the **Download File** button.



4. RSA Authentication Manager will generate a JavaScript file named *am_integration.js*. Copy the file to the *C:\Program Files (x86)\Hitachi ID\IDM Suite\%INSTANCE%\wwwdocs\default\js* directory on your Identity Manager server, where *\%INSTANCE%* is the name of your Identity Manager server instance.
5. Navigate to the *C:\Program Files (x86)\Hitachi ID\IDM 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?_CACHENUM" type="text/javascript"><script>
<input type="hidden" name="USER_IDENT_AM" value="%LOGGEDIN_USERID%" />
```

7. Navigate to the *C:\Program Files (x86)\Hitachi ID\IDM 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.addEvent( 'load', function( e ){
   if( document.getElement( 'input[name=01]' ) )
       redirectToIdP();
   });
</script>
```

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

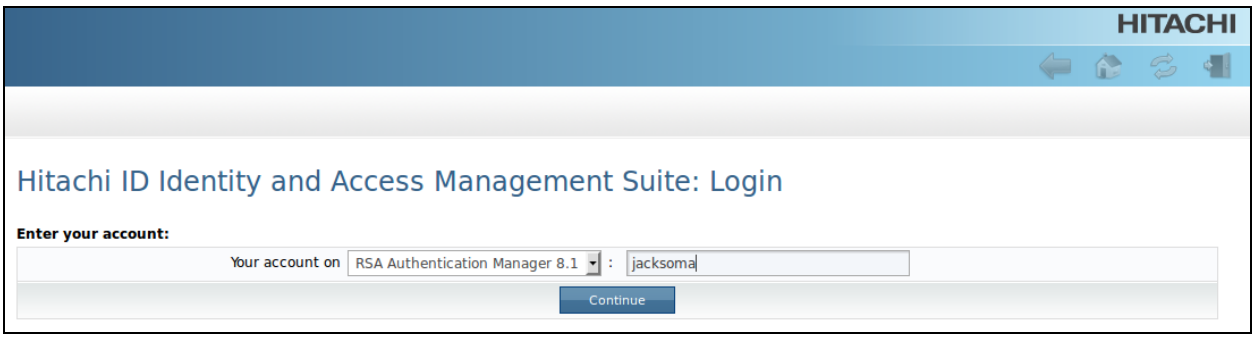
```
%HIDDEN_VIEWS%

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

%AUTH_VIEWS%

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

INCLUDE FOOTER
```

9. Navigate to the *C:\Program Files (x86)\Hitachi ID\IDM 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

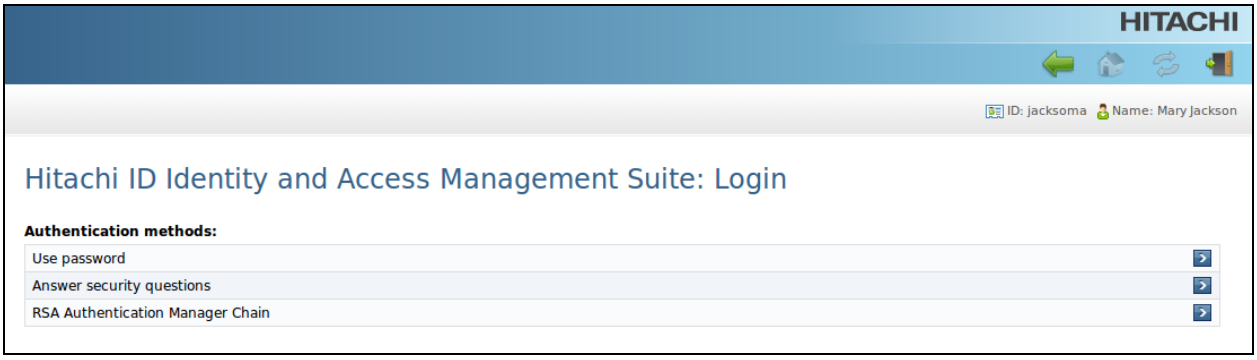
```
make default en-us
```

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

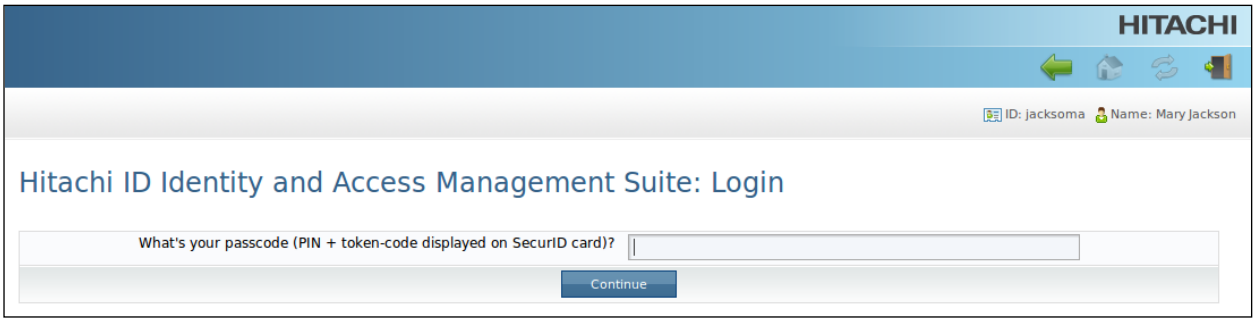
RSA SecurID Login Screens



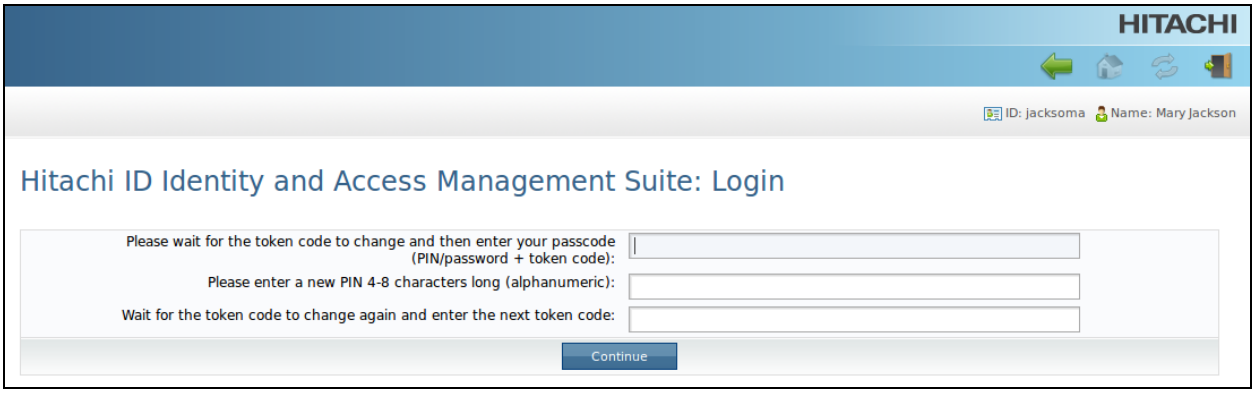
Login ID Prompt



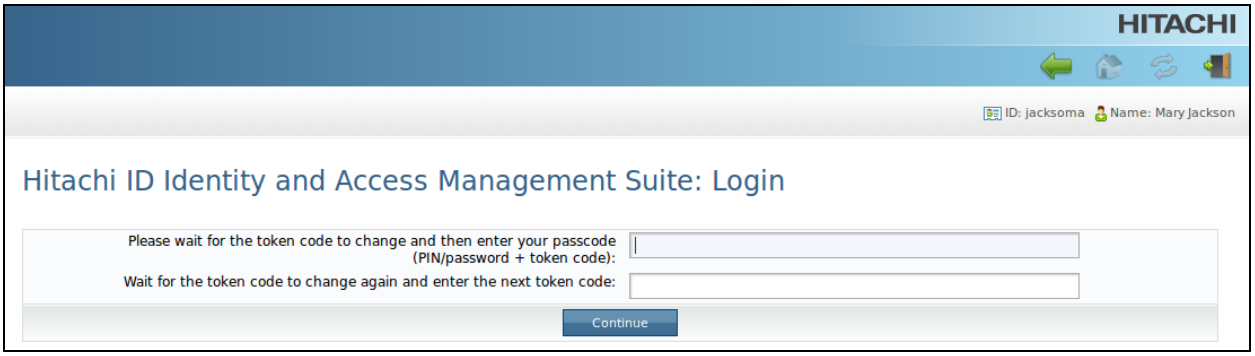
Select Authentication Method Prompt



RSA SecurID Passcode Prompt

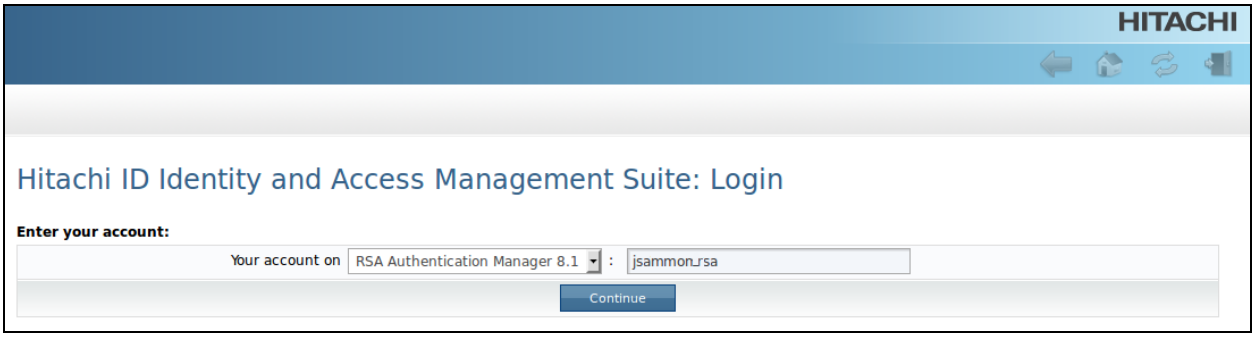


New PIN Mode Prompt

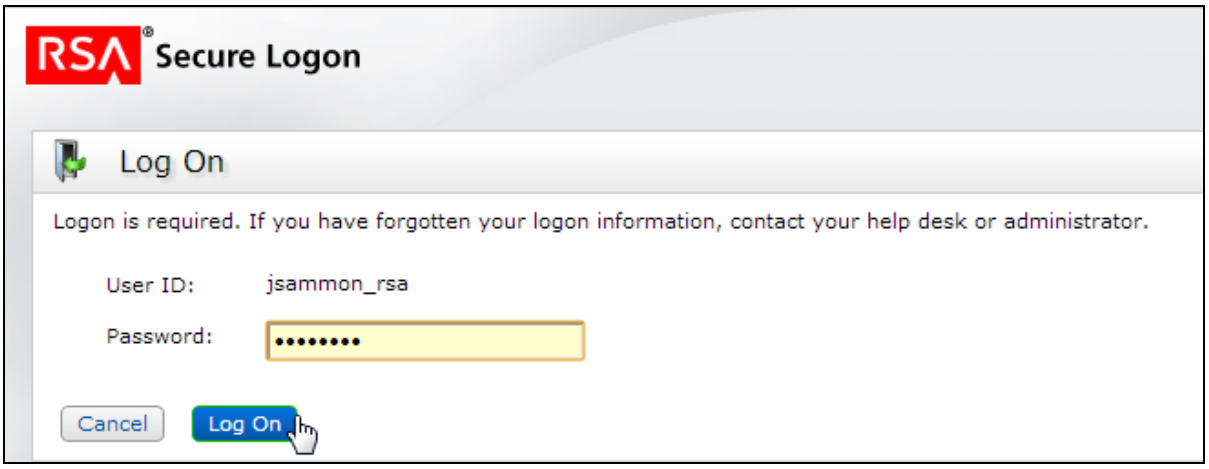


Next Tokencode Prompt

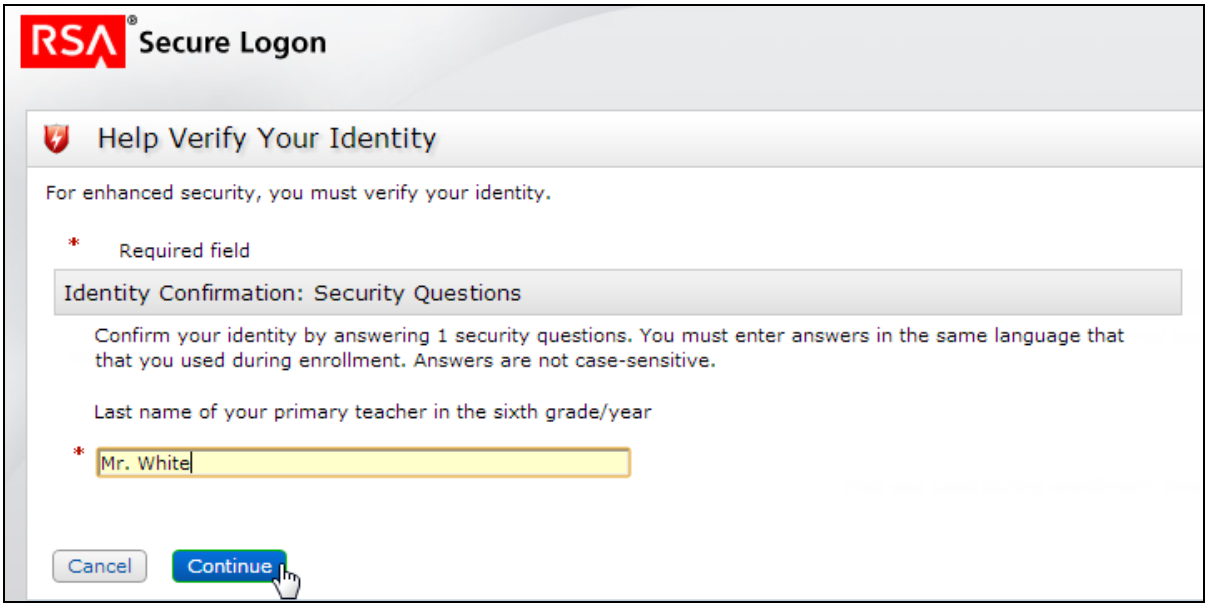
RSA RBA Login Screens



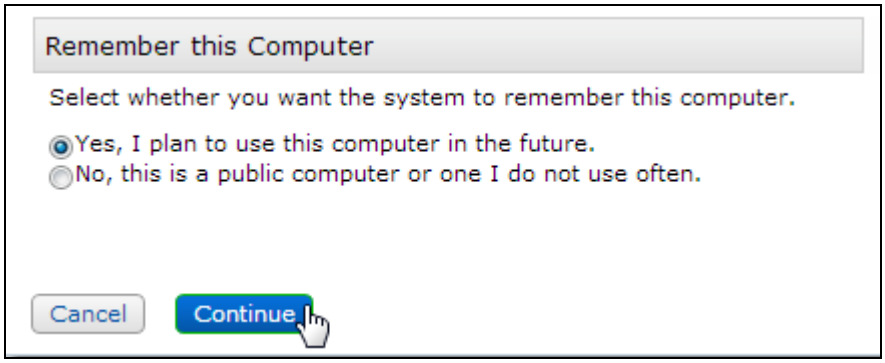
Hitachi ID Password Manager Login ID Prompt:



RBA Password Logon Prompt



RBA Challenge Question Logon Prompt



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 Identity 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	✓	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			
14 Digit Passcode	✓	14 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 / 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	✓	Risk-Based Authentication	NA
Risk-Based Authentication with SSO	NA	Risk-Based Authentication with SSO	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:

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

sdconf.rec:

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

sdopts.rec:

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

sdstatus.12:

Identity 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 Identity Manager integration doesn’t support on-demand tokens.