EMC
eRoom

RSA SecurID Ready Implementation Guide

Last Modified: March 5, 2014

Partner Information

Product Information	
Partner Name	EMC, Inc.
Web Site	www.emc.com
Product Name	eRoom
Version & Platform	7.44.504.53
Product Description	The eRoom digital workplace is a cross-enterprise collaborative environment that integrates with a company's enterprise systems and platforms and mission-critical business processes, providing a unified environment for complex project work and business.

Solution Summary

EMC eRoom web-based workplaces allow distributed teams to create and manage projects, discuss ideas and share information, all within a central location. For added security, the eRoom server supports both RSA SecurID two-factor authentication and RSA Risk-Based Authentication (RBA) for eRoom site members. You may enforce either RSA SecurID authentication at the eRoom site or group level, or on a member-by-member basis. However, RBA can only be enforced at the Site-level.

RSA SecurID supported features eRoom v7.44.5	
RSA SecurID Authentication via Native RSA SecurID Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	No
On-Demand Authentication via Native SecurID 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

! **Important**: eRoom 7.44 does not support RSA Authentication Manager On-Demand Authentication.

RSA Risk-Based Authentication Overview

RSA Risk-Based Authentication is a multi-factor authentication platform that analyzes a user's device[1] and behavior during authentication in order to identify fraudulent activity. If the analysis finds the potential for risk exceeds a predefined threshold, the platform will challenge the user with a secondary authentication method to further confirm the user's identity.

In order to integrate a third-party product with RBA, the product must be web-based, and it must support RSA SecurID authentication. However, the product isn't responsible for prompting users to authenticate and doesn't need to contain any RBA logic. Instead, it delegates these responsibilities to a stand-alone RBA web application.

! **Important**: In order to enable RBA, you must also enable RSA SecurID.

In a typical integration, the 3rd-party product's administrator enables RSA SecurID authentication and modifies the RSA SecurID login page to call a custom JavaScript function when the page loads. The function (named *redirectToIdP*) collects information from the login form to allow the RBA platform to post SecurID credentials back to it after successful RBA authentications. The function then posts this information to an RBA service to kick-off the authentication process.

When the RBA application authenticates a user, it generates a one-time password (OTP) and posts the user's username and OTP to the original login form's submit action. This triggers the 3rd-party product's standard RSA SecurID integration, which sends the credentials to the RSA Authentication Manager Server for validation. When the server responds to confirm that the credentials are valid, the product grants the user access.

[1] In the case of eRoom integrations, "device" refers to the end-user's computer.

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.

You must register agents 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 eRoom server. You need the following information to do so:

- the hostname of the eRoom server
- IP addresses for all of the network interfaces on the eRoom server's host machine

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.

Consult the *RSA Authentication Manager Administrator Guide* for more information about RSA Authentication Manager Agents.

RSA SecurID files

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

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

Partner Product Configuration

Before You Begin

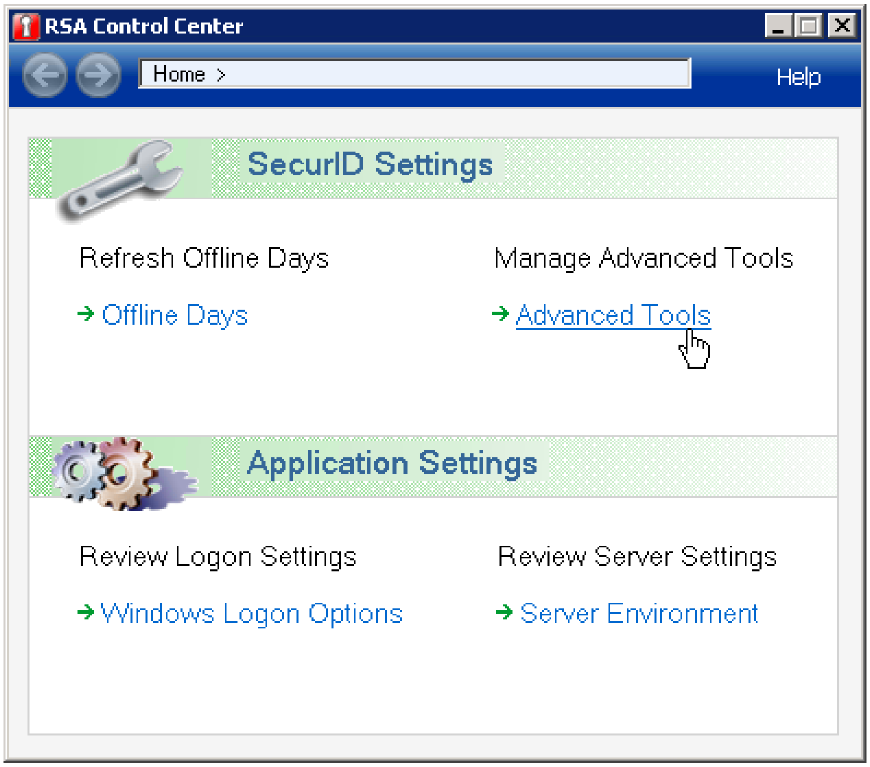
This document provides instructions for enabling RSA SecurID two-factor authentication and Risk-Based Authentication for eRoom users. You should have working knowledge of eRoom, RSA Authentication Manager and RSA RBA (if you intend to use it), as well as access to the appropriate administrative documentation. Ensure that eRoom and RSA Authentication Manager are running properly prior to configuring the integration.

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

Enable RSA SecurID Authentication

Configure the RSA Authentication Agent

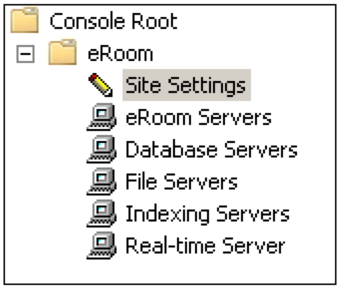
1. Install the RSA Authentication Agent for Windows on the PC that is hosting your eRoom server. You will be prompted to reboot the system when you finish the installation.
2. When the system reboots, open the **RSA Control Center** utility, click the **Advanced Tools** link, click the **Test Authentication** link and perform a SecurID logon.



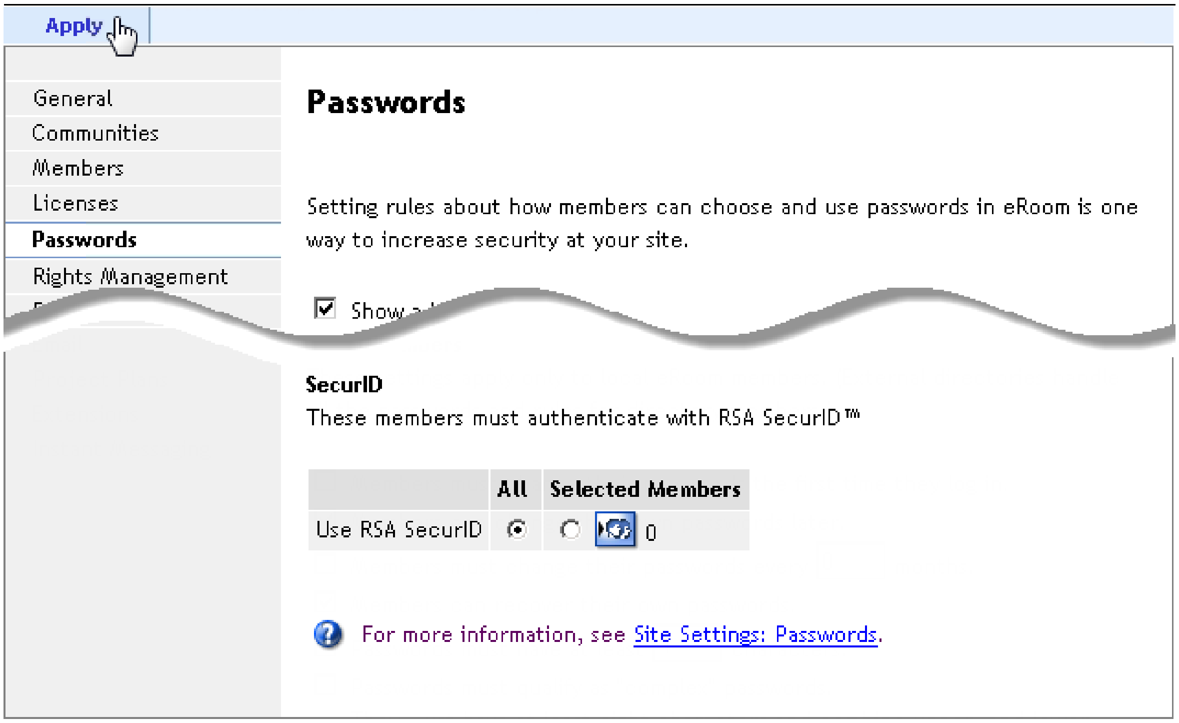
3. Once you have authenticated, verify that the *securid* node secret file is in the *%windir%\system32* directory. If it isn't, copy it and the *sdconf.rec* and *sdstatus.12* files from *C:\Program Files\Common Files\RSA Shared* to *%windir%\system32*.
4. Verify that the *aceclnt.dll* and *sdmsg.dll* API libraries are installed in the *%windir%\system32* directory. If they aren't, copy them from *C:\Program Files\Common Files\RSA Shared* to *%windir%\system32* and reboot the PC.

Configure the eRoom Server for RSA SecurID Authentication

1. Open the eRoom Server Admin Console and select the **Site Settings** icon on the left hand pane.



2. Click the **Passwords** tab in the left-hand menu and scroll down to the **SecurID** section.



Passwords

Setting rules about how members can choose and use passwords in eRoom is one way to increase security at your site.

☑ Show a

SecurID

These members must authenticate with RSA SecurID™

	All	Selected Members
Use RSA SecurID	●	○ 0

For more information, see Site Settings: Passwords.

3. If you want every Site member to authenticate with RSA SecurID, select the **All** radio button. (You must select this option if you are enabling RBA.)

   If you want a smaller subset of members to authenticate with SecurID, click the **Selected Member** radio button, click the icon to its right and select the appropriate members/groups. Consult eRoom Administrative documentation for more information configuring eRoom Sites.

! ▹ **Important**: You must enforce RBA at the eRoom Site-level. If you are configuring RBA, make sure you select the **All** radio button in the step above.

4. Click the **Apply** button on the top of the page.

Enable RSA Risk-Based Authentication

The following subsections contain instructions for enabling Risk-Based Authentication on an eRoom Server. Before you continue, make sure that you have configured RSA SecurID authentication on the server. To test the configuration, create an eRoom user and an RSA Authentication Manager user with the same username and perform a test authentication. If you don't have a SecurID token, assign a static password to the user. See the RSA Authentication Manager Administrator's guide for more information.

Important: You must **configure the RSA Authentication Agent for Windows** and **enable RSA SecurID authentication** on your eRoom server before proceeding.

Configure and Deploy the RSA RBA eRoom Server Extension

The RSA RBA eRoom Server Extension implements the majority of the integration. When an unauthenticated user requests access to an eRoom Site, the extension generates a page to redirect the user to the RBA application. When the RBA application authenticates a user and posts SecurID credentials back to the eRoom server, the extension receives the credentials, sends them to RSA Authentication Manager for validation and creates a session for the user.

Follow the instructions below to deploy the extension in your eRoom environment.

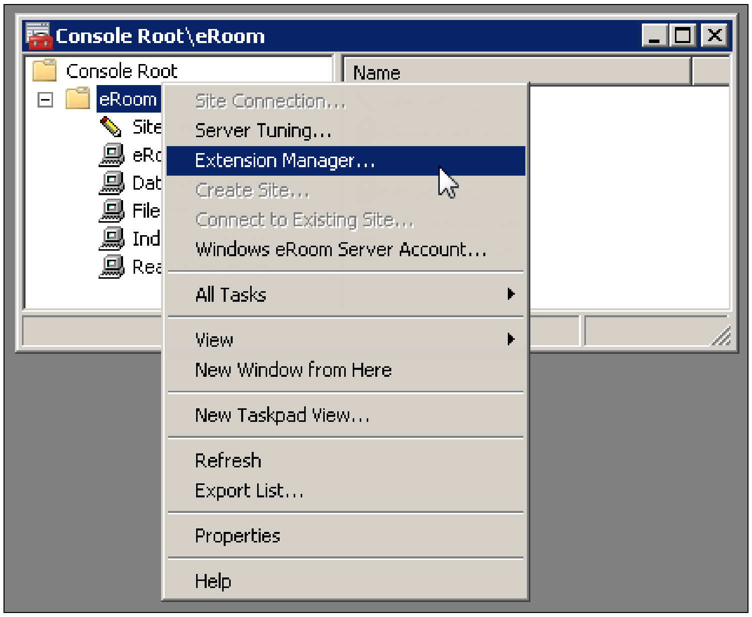
1. Use the link below to download the eRoom-RBA integration kit to your eRoom server host PC. If you have trouble downloading the file, try copying the link and pasting it into your browser's address field/

https://sftp.rsa.com/human.aspx?Username=partner&password=rsasecured&arg01=978386477&arg12=downloaddirect&transaction=signon&quiet=true

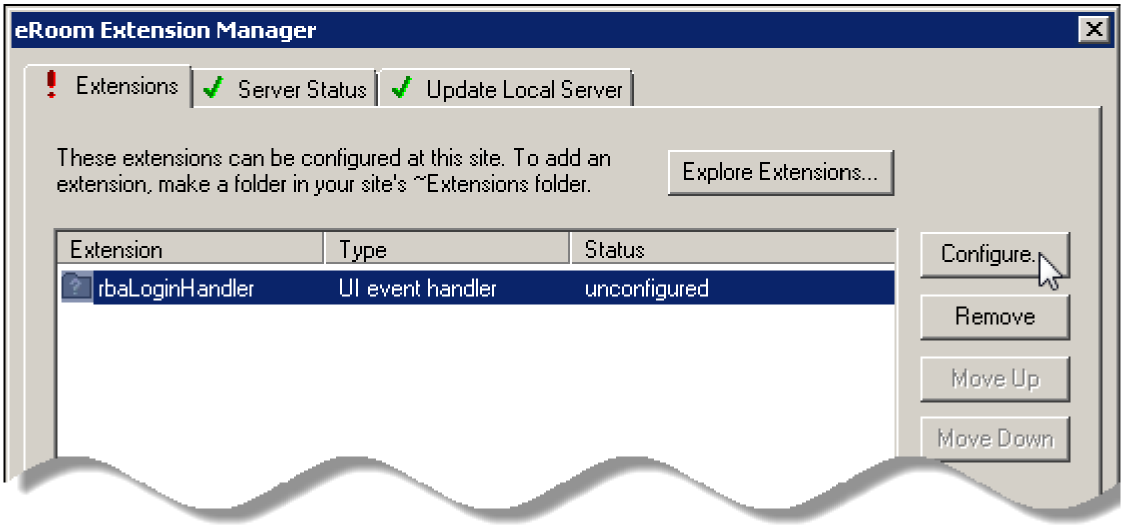
Unzip the kit in a temporary directory to extract the server extension folder and RBA JavaScript template:

- *RBALoginEventHandler* **–** This folder contains RSA's custom eRoom server extension for RBA.
- *eRoom_7.4.xml* – This *XML* file is an RBA integration template that you will use to generate a JavaScript file. It contains functions the server extension needs to communicate with the RSA RBA application.

2. Copy the *RBALoginEventHandler* folder to the eRoom file server's *~Extension* directory.
3. Launch the eRoom Admin MMC console, right-click the **eRoom** folder icon on the left and select the **Extension Manager** menu item.



4. Select the **Extensions** tab, highlight the *rbaLoginHandler* extension and click the **Configure** button.

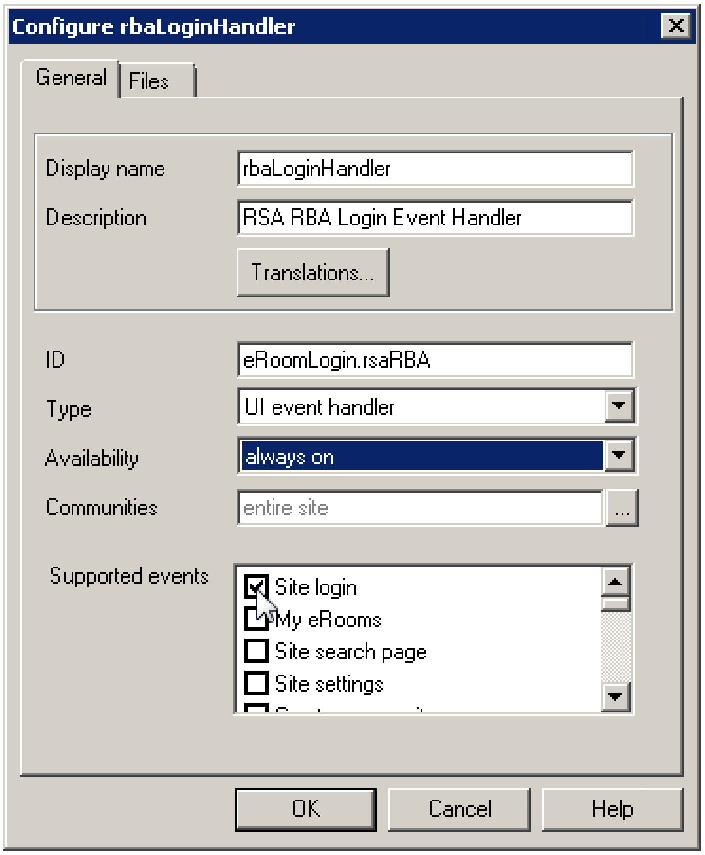


eRoom Extension Manager

These extensions can be configured at this site. To add an extension, make a folder in your site's ~Extensions folder.

Extension	Type	Status
rbaLoginHandler	UI event handler	unconfigured

5. Select *always on* from the **Availability** dropdown list and check the **Site login** checkbox in the **Supported events** list. Don't modify the remaining default values.



Configure rbaLoginHandler

Display name: rbaLoginHandler

Description: RSA RBA Login Event Handler

ID: eRoomLogin.rsaRBA

Type: UI event handler

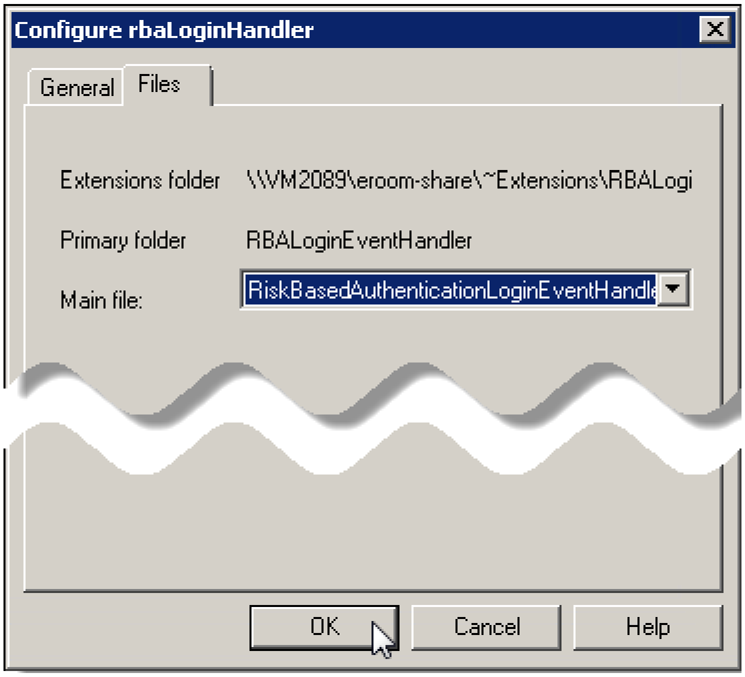
Availability: always on

Communities: entire site

Supported events:
☑ Site login
□ My eRooms
□ Site search page
□ Site settings

! **Important**: Ensure the **Communities** field is set to *entire site*.

6. Select the **Files** tab, select *RiskBasedAuthenticationLoginEventHandler.asp* from the **Main file** dropdown list and click the **OK** button.



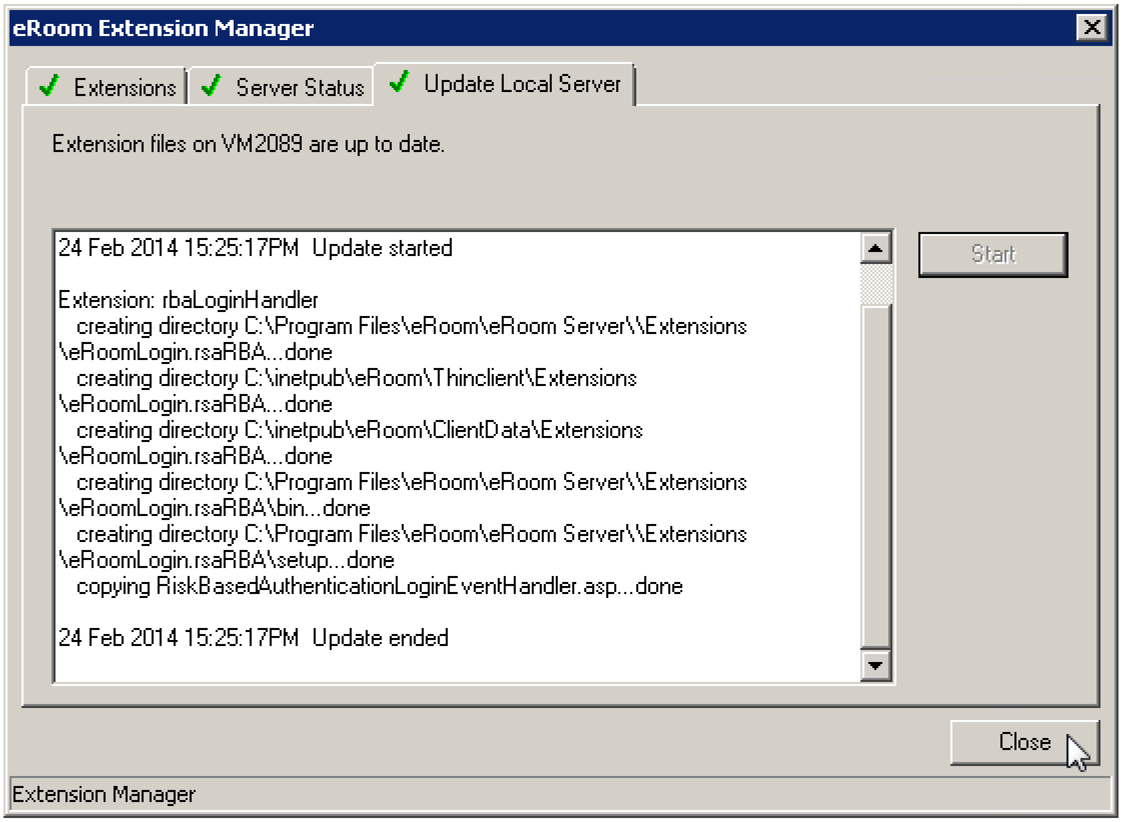
Configure rbaLoginHandler

Extensions folder \\VM2089\eroom-share\~Extensions\RBALogi

Primary folder RBALoginEventHandler

Main file: RiskBasedAuthenticationLoginEventHandle

7. Select the **Update Local Server** tab, click the **Start** button and click the **Close** button.



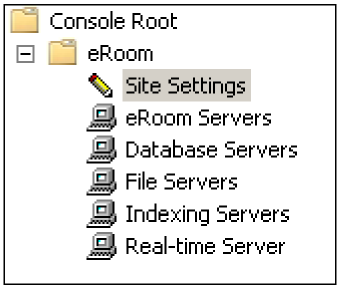
eRoom Extension Manager

Extension files on VM2089 are up to date.

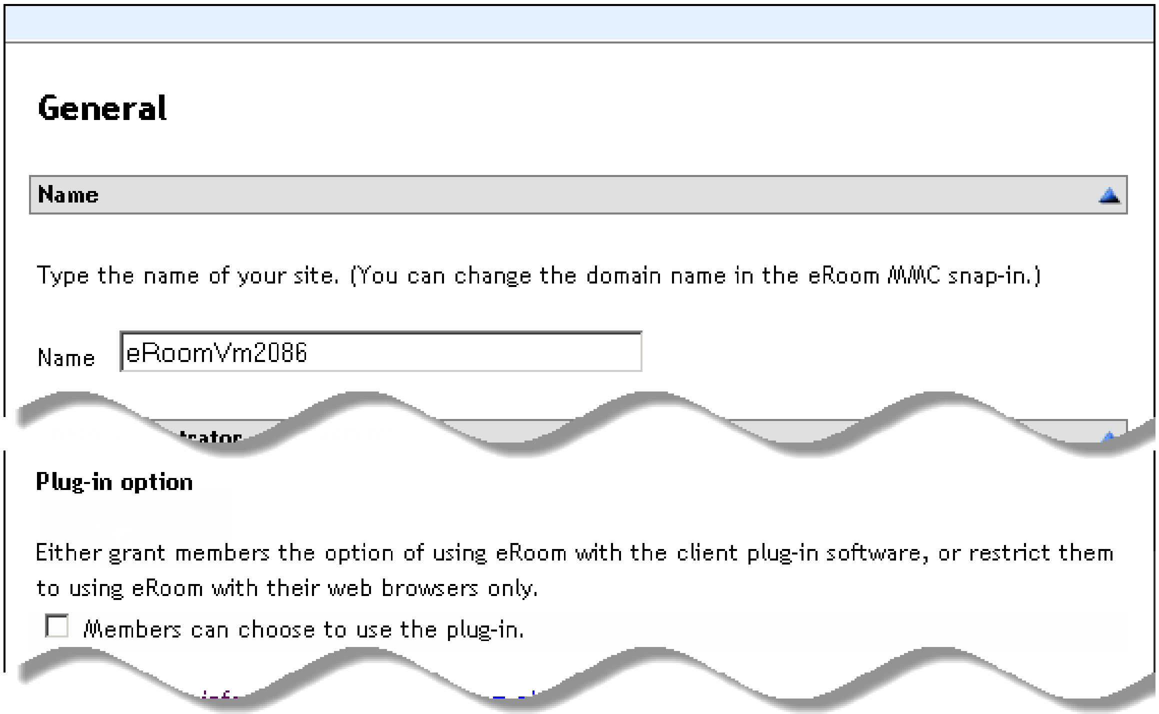
```
24 Feb 2014 15:25:17PM  Update started

Extension: rbaLoginHandler
   creating directory C:\Program Files\eRoom\eRoom Server\\Extensions
\eRoomLogin.rsaRBA...done
   creating directory C:\inetpub\eRoom\Thinclient\Extensions
\eRoomLogin.rsaRBA...done
   creating directory C:\inetpub\eRoom\ClientData\Extensions
\eRoomLogin.rsaRBA...done
   creating directory C:\Program Files\eRoom\eRoom Server\\Extensions
\eRoomLogin.rsaRBA\bin...done
   creating directory C:\Program Files\eRoom\eRoom Server\\Extensions
\eRoomLogin.rsaRBA\setup...done
   copying RiskBasedAuthenticationLoginEventHandler.asp...done

24 Feb 2014 15:25:17PM  Update ended
```

Extension Manager

8. Click the **Site Settings** icon on the left hand pane.



9. Click the **General** tab, scroll down to the **Plug-in option** section and uncheck the checkbox labeled **Members can choose to use the plug-in**.



General

Name

Type the name of your site. (You can change the domain name in the eRoom MMC snap-in.)

Name: eRoomVm2086

Plug-in option

Either grant members the option of using eRoom with the client plug-in software, or restrict them to using eRoom with their web browsers only.

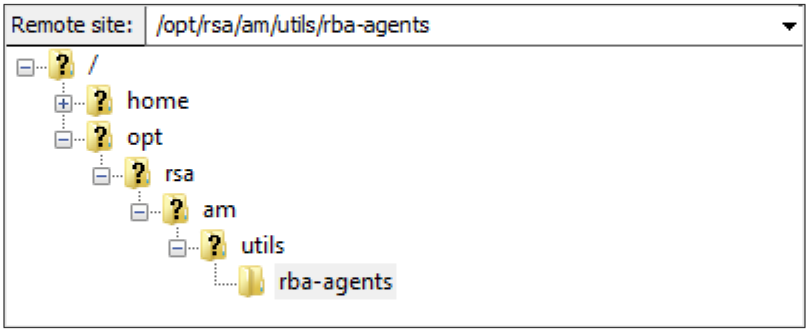
☐ Members can choose to use the plug-in.

! **Important**: The RBA integration doesn’t support the eRoom plug-in. Make sure you disable the plug-in as described in step 9. This will restrict users to access eRoom through a web browser.

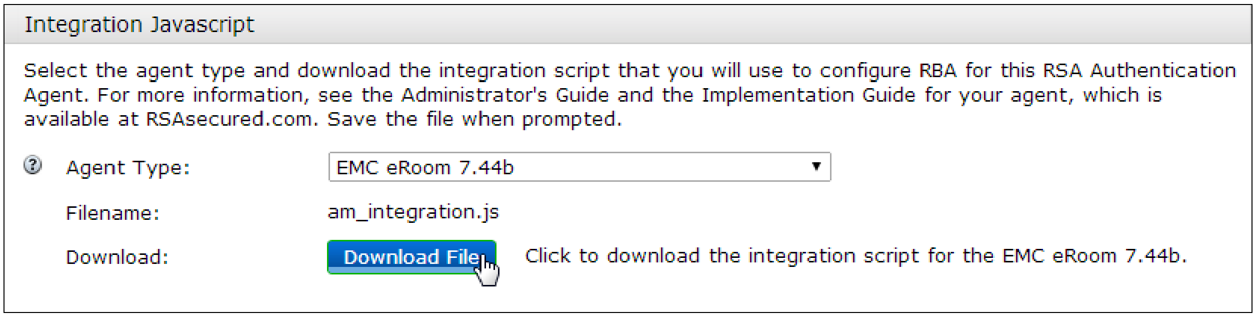
Generate the RSA Risk-Based Authentication JavaScript File

Follow the steps below to generate the RSA RBA JavaScript file for the eRoom web client and install it on your eRoom server.

1. Connect to your RSA Authentication Manager server's virtual appliance using an SCP or SSH client and navigate to the */opt/rsa/am/utils/rba-agents* directory.
2. Upload the *eRoom_7.4.xml* file from your integration kit directory to the *rba-agents* directory above and disconnect your SCP/SSH client session.



3. Log in to the RSA Authentication Manager Security Console and open your eRoom agent for editing.
4. Scroll to the **Risk-based Authentication** section and check the **Enable this Agent for risk-based authentication** checkbox.
5. Set the access restriction and authentication method options based on your requirements and click the **Save agent & Go to Download Page** button.
6. Select *EMC eRoom 7.44b* from the **Agent Type** dropdown list 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: EMC eRoom 7.44b

Filename: am_integration.js

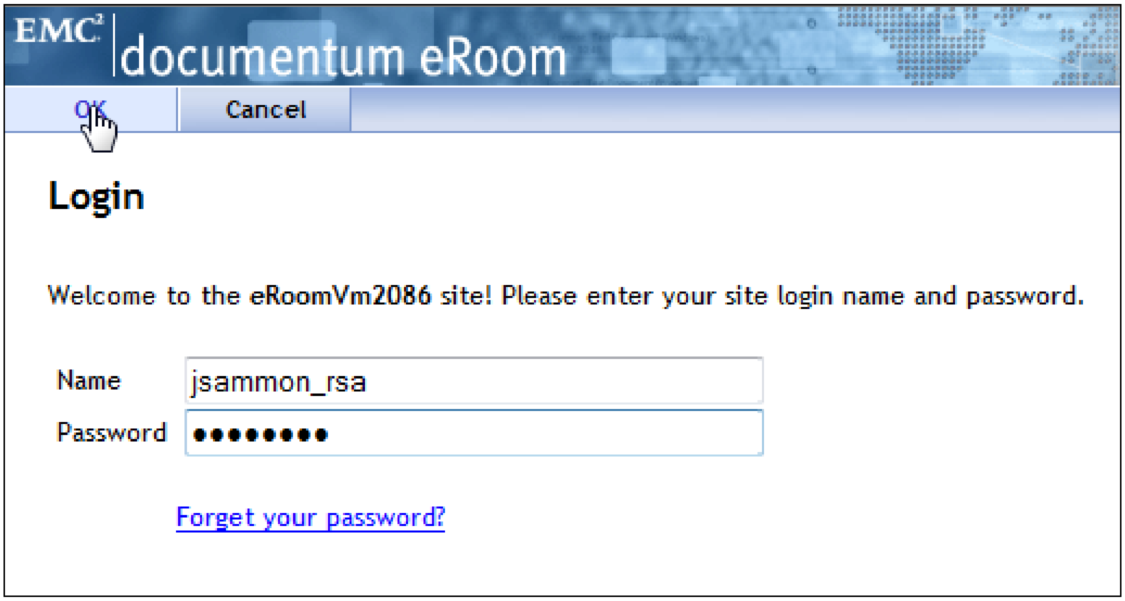
Download: Click to download the integration script for the EMC eRoom 7.44b.

Note: RSA Authentication Manager will use the *eRoom_7.4.xml* template you uploaded to generate a JavaScript file for the integration. It contains functions the eRoom client will call to collect data from a custom RSA SecurID eRoom login form and post the data to the RBA web application.

7. Save the JavaScript file (*am_integration.js*) to the eRoom data folder on you IIS web server. The folder's default name is *ClientData*, and its default path is *C:\inetpub\eRoom\ClientData*.
8. Restart IIS.

RSA SecurID Login Screens

Standard Login Screen



Login

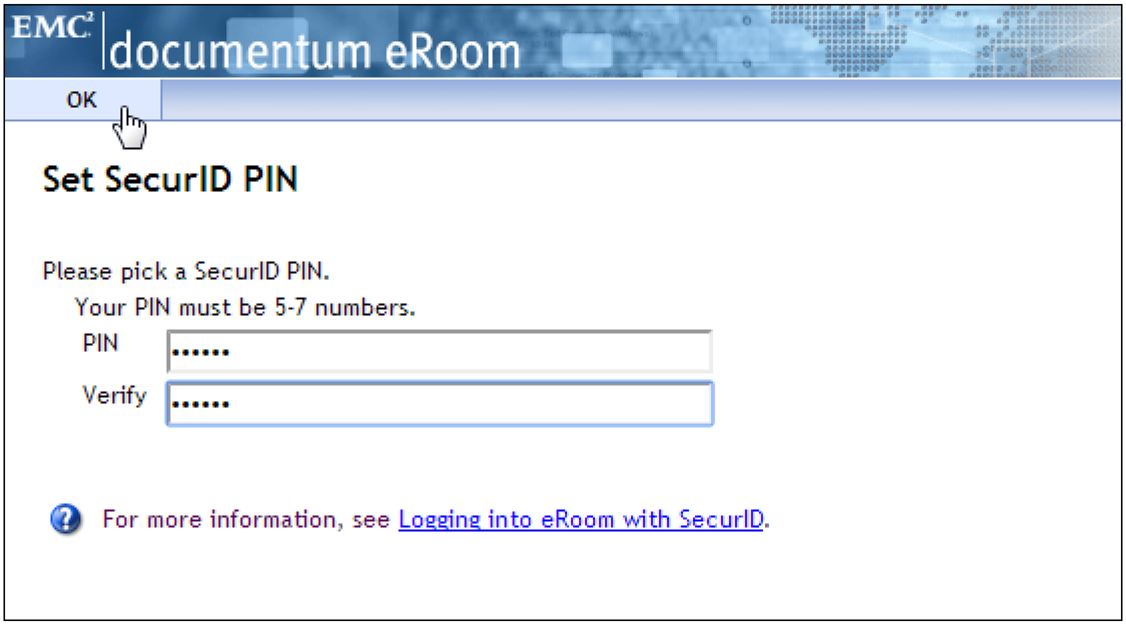
Welcome to the eRoomVm2086 site! Please enter your site login name and password.

Name jsammon_rsa

Password ●●●●●●●●●

Forget your password?

New User-defined PIN Prompt



Set SecurID PIN

Please pick a SecurID PIN.

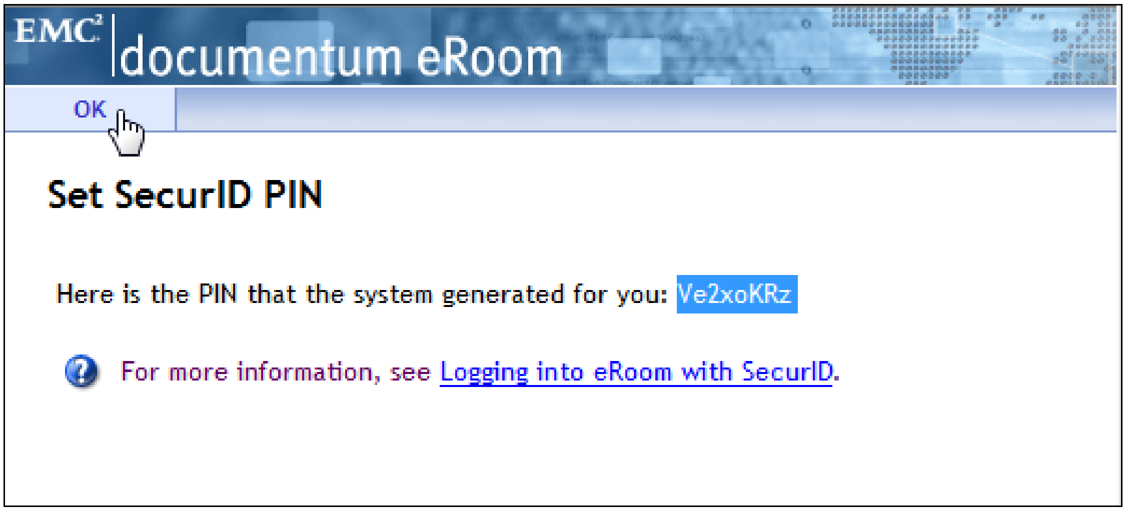
Your PIN must be 5-7 numbers.

PIN ••••••

Verify ••••••

For more information, see Logging into eRoom with SecurID.

New *System-generated PIN Prompt*

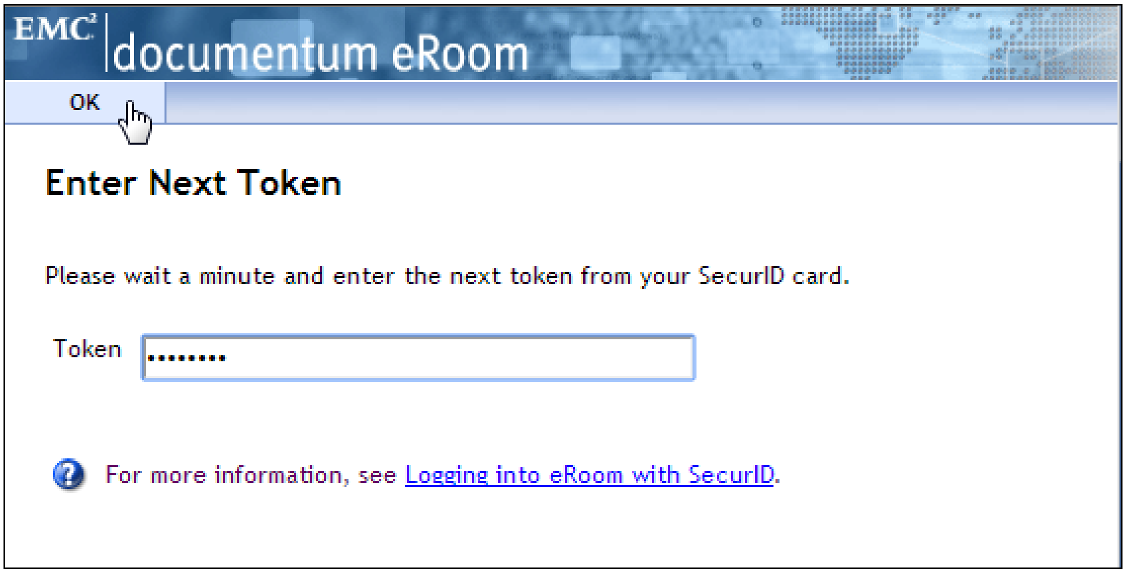


Set SecurID PIN

Here is the PIN that the system generated for you: Ve2xoKRz

For more information, see Logging into eRoom with SecurID.

Next Tokencode Prompt



Enter Next Token

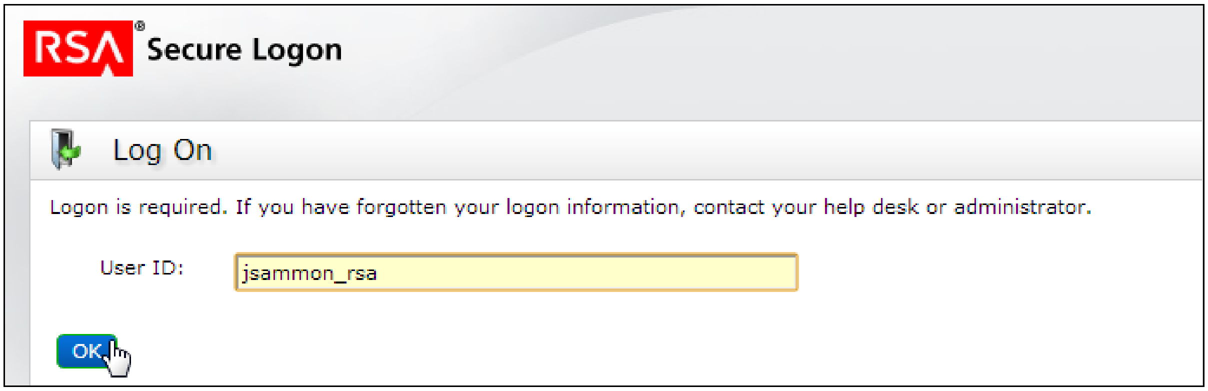
Please wait a minute and enter the next token from your SecurID card.

Token ••••••••

For more information, see Logging into eRoom with SecurID.

RSA RBA Login Screens

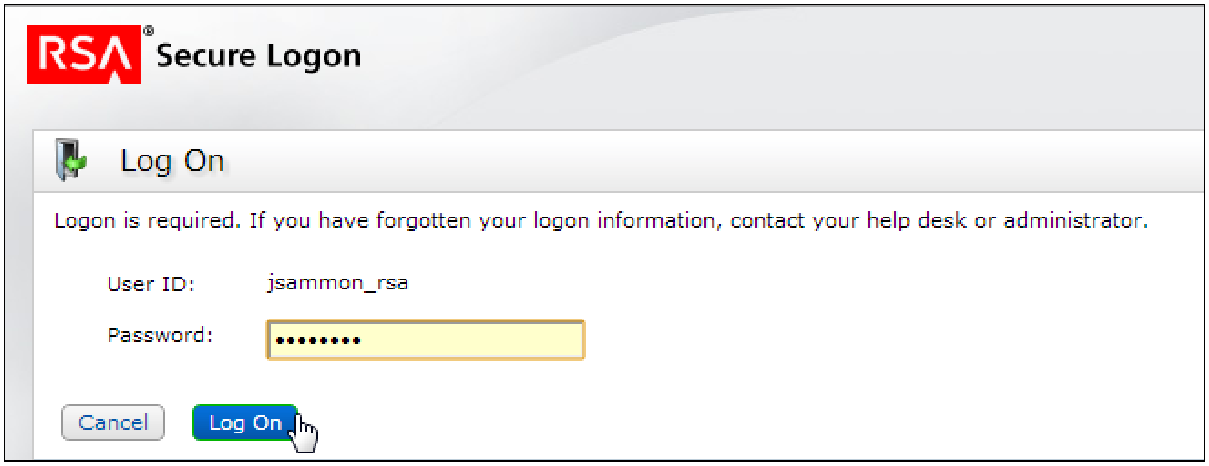
RBA User ID Logon Prompt:



Logon is required. If you have forgotten your logon information, contact your help desk or administrator.

User ID: jsammon_rsa

RBA Password Logon Prompt:

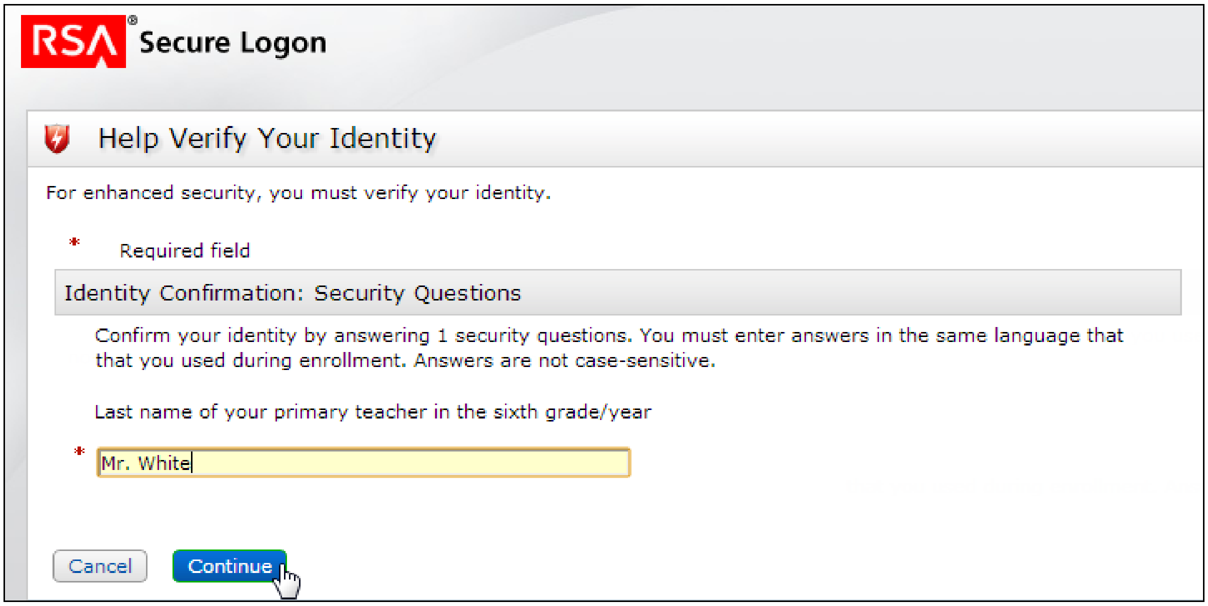


Logon is required. If you have forgotten your logon information, contact your help desk or administrator.

User ID: jsammon_rsa

Password: •••••••••

RBA Challenge Question Logon Prompt:



Secure Logon

Help Verify Your Identity

For enhanced security, you must verify your identity.

* Required field

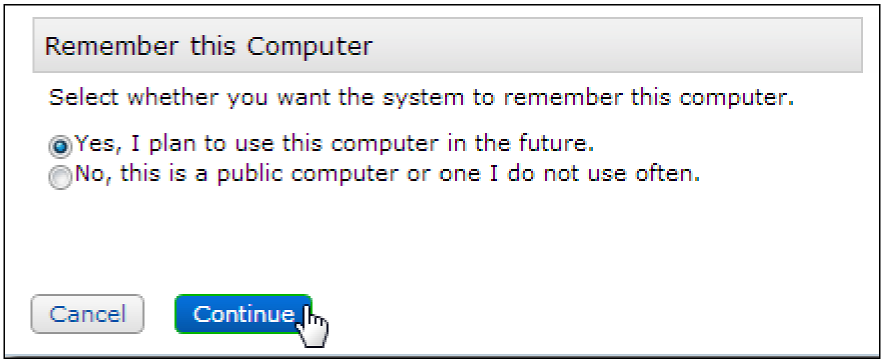
Identity Confirmation: Security Questions

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

* Mr. White

RBA Device-Binding Option Prompt:

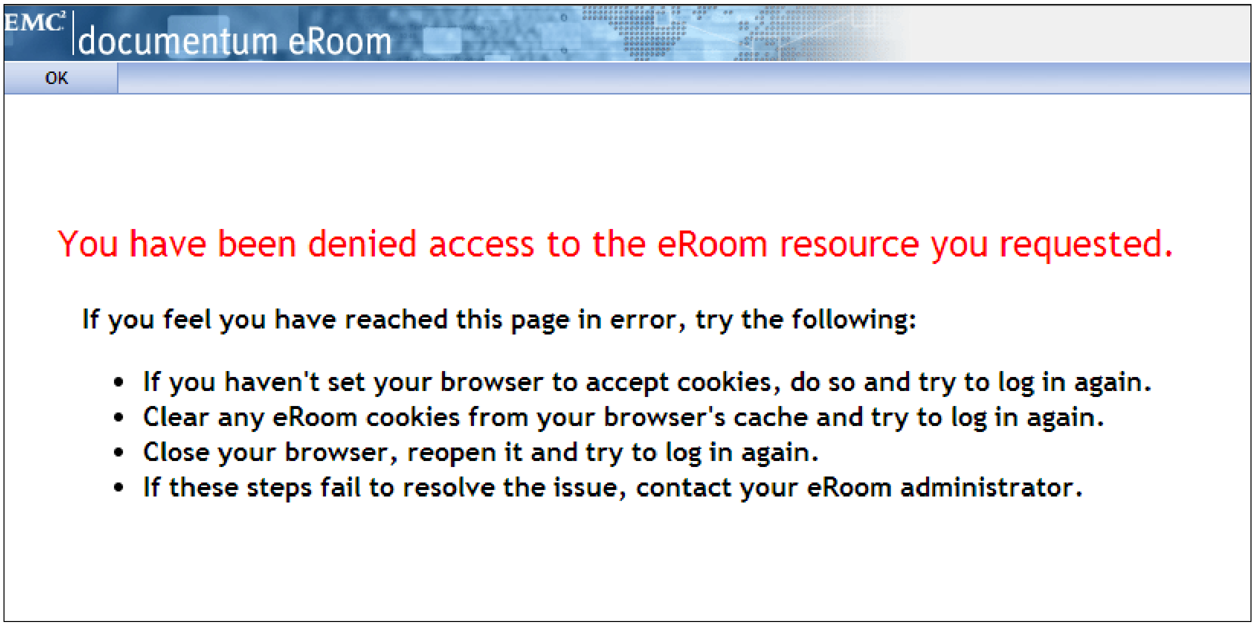


Remember this Computer

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.

Access Denial Message Page



You have been denied access to the eRoom resource you requested.

If you feel you have reached this page in error, try the following:

- If you haven't set your browser to accept cookies, do so and try to log in again.
- Clear any eRoom cookies from your browser's cache and try to log in again.
- Close your browser, reopen it and try to log in again.
- If these steps fail to resolve the issue, contact your eRoom administrator.

Certification Checklist for RSA Authentication Manager

Date Tested: February 3, 2014

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.0	Virtual Appliance
RSA Authentication Agent	7.2.1	Windows 7 Ultimate
eRoom	7.44	Windows 7 Ultimate

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

Date Tested: February 25, 2014

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

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

Known Issues

eRoom doesn’t force authentication after a user sets a new PIN

The eRoom server doesn’t prompt users to re-authenticate after setting a new user-defined or system-generated PIN. Once the user authenticates and resets his/her PIN, eRoom creates a session for the user. In a standard SecurID integration, the system would prompt the user to re-authenticate with the new PIN before proceeding.

eRoom doesn’t support on-demand authentication

This release doesn’t support on-demand authentication.

eRoom doesn’t support SecurID authentication on Window 2008

This release doesn’t support RSA SecurID authentication on Windows 2008.

Appendix

Partner Integration Details	
RSA SecurID API	8.1.2
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	Designated Users, All Users
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	No

Node Secret:

After you **perform a test authentication** from the RSA Control Center console, verify that the node secret file, *securid*, is in the *%windir%\system32* directory. If it isn't, copy it from the *C:\Program Files\Common Files\RSA Shared* directory to *%windir%\system32*.

sdconf.rec:

Verify that the *sdconf.rec* file is in the *%windir%\system32* directory. If it isn't, copy it from the *C:\Program Files\Common Files\RSA Shared* directory to *%windir%\system32*.

sdstatus.12:

Verify that the *sdstatus.12* file is in the *%windir%\system32* directory. If it isn't, copy it from the *C:\Program Files\Common Files\RSA Shared* directory to *%windir%\system32*.

sdopts.rec:

Verify that the *sdopts.rec* file is in the *%windir%\system32* directory. If it isn't, copy it from the *C:\Program Files\Common Files\RSA Shared* directory to *%windir%\system32*.