EMC
IRM

RSA SecurID Ready Implementation Guide

Last Modified: 4/15/2009

Partner Information

Product Information	
Partner Name	EMC
Web Site	http://www.emc.com/products/detail/software/irm-services.htm
Product Name	EMC Documentum Information Rights
Version & Platform	IRM 4.5.1 for Windows 2003 SP2, Solaris 9 or 10
Product Description	EMC IRM Services enables you to control, secure, and track sensitive information wherever it resides—within a work group, across departments, or with partners and suppliers outside the firewall. With IRM Services information rights management technology, you can enhance your document security by applying rights for who can view, edit, print, or forward information, ensuring that sensitive information remains secure as it is shared both internally and externally. When your business needs change, you can dynamically change or revoke access policies and confirm compliance with corporate policies through a detailed audit trail of all activity.
Product Category	e-mail, Workflow, Office Automation

Solution Summary

This guide details the EMC Documentum IRM Server - RSA SecurID integration. After this integration has been implemented, IRM Server users who attempt to access protected content will be prompted for their SecurID tokencodes. When compared to traditional password protection, this two-factor authentication provides organizations with a stronger and more reliable level of security for access to their restricted documents.

IRM Server users are assigned to specific authentication domains, each of which defines an authentication method. IRM currently offers the ability to create and configure LDAP, password, certificate and SecurID domains. By extending RSA Authentication Manager security to IRM services, business customers can protect sensitive information with granular authorization policies fronted by a strong authentication mechanism.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication
List Library Version Used	Library Version 6.1
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	N/A
RSA Authentication Agent Host Type	Net OS
RSA SecurID User Specification	All Users
RSA SecurID Protection of Administrative Users	No
RSA Software Token and RSA SecurID 800 Automation	No
Use of Cached Domain Credentials	No

IRM Server Requirements

Operating System Support:

Partner Product Requirements: IRM Server 4.5.1	
Operating System	
Platform	**Required Patches**
Microsoft 2003 Server	SP 2
Solaris 9	
Solaris 10	

Agent Host Configuration

Important: "Agent Host" and "Authentication Agent" are synonymous. "Agent Host" is a term used with the RSA Authentication Manager 6.x servers and below. RSA Authentication Manager 7.1 uses the term "Authentication Agent".

Important: All "Authentication Agent" types for 7.1 should be set to "Standard Agent".

To facilitate communication between IRM and the RSA Authentication Manager an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies the IRM within its database and contains information about communication and encryption.

To create the Agent Host record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces

When adding the Agent Host Record, configure the IRM Server as NET OS. This setting is used by the RSA Authentication Manager to determine how communication with the IRM Server will occur.

Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.

Please refer to the appropriate RSA Security documentation for additional information about Creating, Modifying and Managing Agent Host records.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	C:/WINNT/system32 on Windows; /var/ace/ on UNIX
Node Secret	C:/WINNT/system32 on Windows; /var/ace/ on UNIX
sdstatus.12	C:/WINNT/system32 on Windows; /var/ace/ on UNIX
sdopts.rec	Not implemented

Partner Product Configuration

Before You Begin

This section provides instructions for integrating the IRM Server with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

IRM Server Configuration

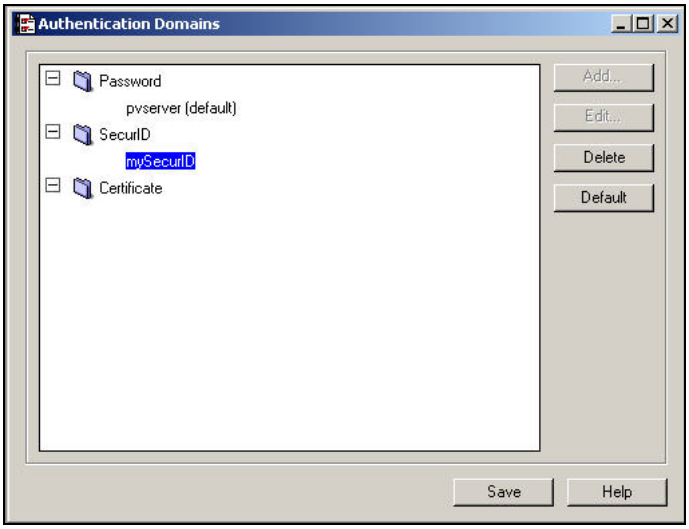
Prerequisites

- In order to add a SecurID domain, you must first install and configure the RSA Authentication Manager Agent on your IRM Server computer. For installation instructions, see the RSA Authentication Manager documentation.
- IRM Server Administrator only allows you to set up one SecurID domain.
- If users authenticate to the IRM Server using a SecurID, they cannot use the work offline capabilities of their IRM client application.
- Once you create a SecurID domain, you cannot edit it.

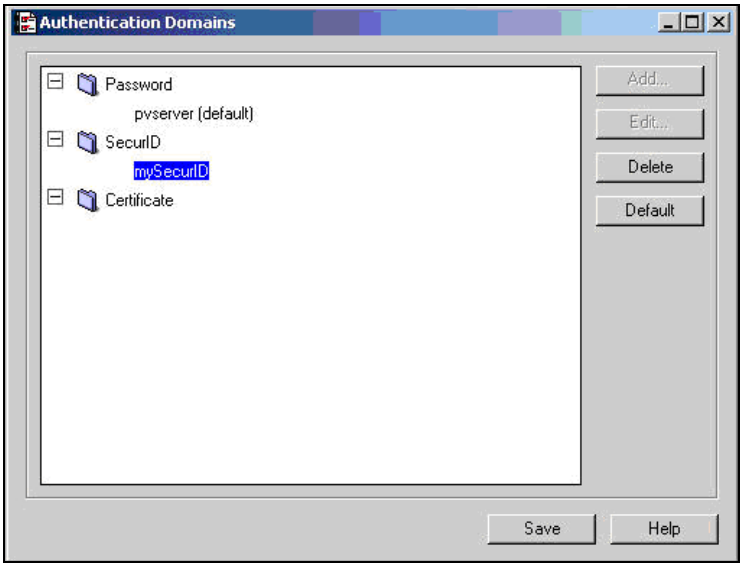
Note: If you set up a SecurID domain using a remote SecurID server on Solaris, users may get the error message "user not authenticated". To solve this problem, make sure that the current sdconf.rec SecurID configuration file is in the /var/ace/ directory. If you don't know where to find sdconf.rec file, see your RSA Authentication Manager administrator.

To add a SecurID domain:

1. Launch the **IRM Server Administrator**
2. Choose Users > Authentication Domains.
3. Select **SecurID** and click **Add**.



4. The Add SecurID Domain dialog box appears. Enter any name you choose to identify the domain in the **Domain Name** field. Click **OK**.
5. The domain appears in the Authentication Domains dialog box.



6. Click **Save**.

Certification Checklist For RSA Authentication Manager v6.x

Date Tested: April 15, 2009

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	6.1	Windows 2003 Server
RSA Authentication Agent	6.1.1	Windows 2003 Server
IRM Server	4.5.1	Windows 2003 Server

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
User Selectable	✓	User Selectable	N/A
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	N/A
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	N/A
Passcode			
16 Digit Passcode	✓	16 Digit Passcode	N/A
4 Digit Password	✓	4 Digit Password	N/A
Next Tokencode Mode	✓	Next Tokencode Mode	N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	N/A
Name Locking Enabled	✓	Name Locking Enabled	N/A
No RSA Authentication Manager	✓	No RSA Authentication Manager	N/A
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
RSA SecurID 800 Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
Credential Functionality			
Determine Cached Credential State	N/A	Determine Cached Credential State	N/A
Set Credential	N/A	Set Credential	N/A
Retrieve Credential	N/A	Retrieve Credential	N/A

JGS

✓ = Pass ✗ = Fail N/A = Non-Available Function

Certification Checklist For RSA Authentication Manager v7.1

Date Tested: April 15, 2009

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1	Windows 2003 Server
RSA Authentication Agent	6.1.1	Windows 2003 Server
IRM Server	4.5.1	Windows 2003 Server

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
User Selectable	✓	User Selectable	N/A
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	N/A
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	N/A
PASSCODE			
16 Digit PASSCODE	✓	16 Digit PASSCODE	N/A
4 Digit Password	✓	4 Digit Password	N/A
Next Tokencode Mode			
Next Tokencode Mode	✓	Next Tokencode Mode	N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	N/A
Name Locking Enabled	✓	Name Locking Enabled	
No RSA Authentication Manager	✓	No RSA Authentication Manager	N/A

Additional Functionality			
RSA Software Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
RSA SD800 Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
Domain Credential Functionality			
Determine Cached Credential State	N/A	Determine Cached Credential State	
Set Domain Credential	N/A	Set Domain Credential	
Retrieve Domain Credential	N/A	Retrieve Domain Credential	

JGS

✓ = Pass ✗ = Fail N/A = Non-Available Function

Appendix

Node Secret:

The Node Secret is stored in C:\WINNT\system32\securid on Windows and /var/ace/securid on UNIX.

sdconf.rec:

The sdconf.rec file is stored in the C:\WINNT\system32\ directory on Windows and the /var/ace/ directory on UNIX.

sdopts.rec:

The sdopts.rec is not used in the EMC IRM integration.

sdstatus.12:

The sdstatus.12 file is stored in the C:\WINNT\system32\ directory on Windows and the /var/ace/ directory on UNIX.