



RSA SecurID Ready Implementation Guide

Last Modified: 29 July 2009

Partner Information

Product Information	
Partner Name	NetDocuments
Web Site	www.netdocuments.com
Product Name	NetDocuments
Version & Platform	Professional and Enterprise
Product Description	Online document & email management where you can organize and store all your organization's documents in one secure location in the cloud.
Product Category	Document Security

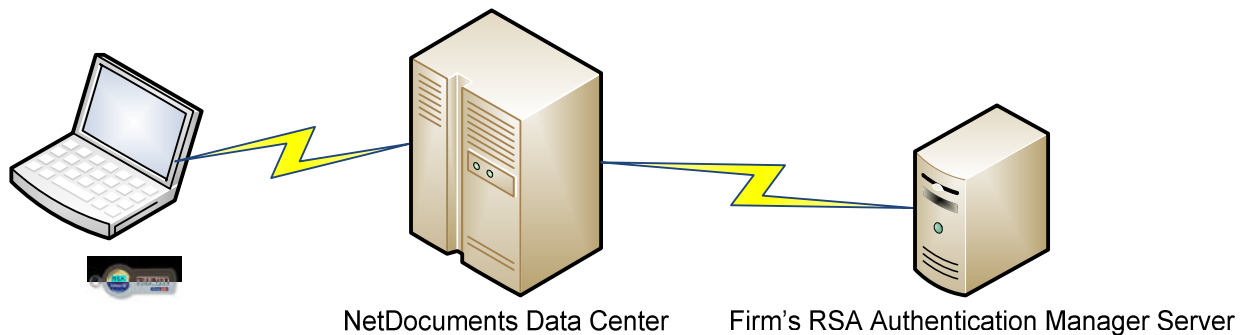




Solution Summary

NetDocuments integrates with RSA SecurID to provide increased security via two-factor authentication. NetDocuments repository administrators define authentication requirements that specify how users must authenticate in order to access the repository's documents. These requirements can include IP address ranges, authentication via Automated Login (Active Directory SSO), authentication via digital certificates, and authentication via RSA SecurID.

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





Product Requirements

Partner Product Requirements: NetDocuments	
NetDocuments Professional or Enterprise Edition	

Agent Host Configuration

To facilitate communication between NetDocuments and RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies the NetDocuments service within its database and contains information about communication and encryption.

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

- Hostname¹ **smtp.vault.netvoyage.com**
- IP Address **198.187.132.47**

When adding the Agent Host Record, you should configure NetDocuments as a standard agent. This setting is used by the RSA Authentication Manager to determine how communication with NetDocuments 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	Uploaded via the Advanced Authentication Configuration page in NetDocuments
Node Secret	Stored internally by NetDocuments
sdstatus.12	Stored internally by NetDocuments
sdopts.rec	Not implemented

Please see the appendix of this document to get detailed information regarding these files.

¹ Note: the hostname and IP address listed above are for the NetDocuments public service. NetDocuments is a hosted application; customers access it online rather than install it on their own servers. These addresses will always be used to configure this integration.



NetDocuments Configuration

Before You Begin

This section provides instructions for enabling RSA SecurID authentication for NetDocuments. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved 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.

Enabling the Integration

1. Using the tools provided with your RSA Authentication Manager installation and the information in the Agent Host Configuration section above, add an Agent Host record to your RSA Authentication Manager database.
2. Download an agent configuration file.
3. Log into NetDocuments as a repository administrator and go to the Repository Administration page. Click the “Add and remove users and groups” link. Then click the “Configure advanced authentication options” link.

Repository Users [Help](#)

To add a person to this repository, enter the person's email address and click Add User.

Email Address:

Internal Users

- Thomas M. Campbell (thomas.campbell@netdocuments.com)
- John T. Kelly (john.kelly@netdocuments.com)
- George M. Kelly (george.m.kelly@netdocuments.com)
- Michael J. Kelly (michael.j.kelly@netdocuments.com)
- Kevin J. Kelly (kevin.j.kelly@netdocuments.com)
- John J. Kelly (john.j.kelly@netdocuments.com)
- Michael J. Kelly (michael.j.kelly@netdocuments.com)

Currently using 7 of 7 internal user accounts.

External Users

- Thomas M. Campbell (thomas.campbell@netdocuments.com)
- John T. Kelly (john.kelly@netdocuments.com)
- George M. Kelly (george.m.kelly@netdocuments.com)
- Michael J. Kelly (michael.j.kelly@netdocuments.com)
- Kevin J. Kelly (kevin.j.kelly@netdocuments.com)
- John J. Kelly (john.j.kelly@netdocuments.com)
- Michael J. Kelly (michael.j.kelly@netdocuments.com)

Currently using 7 of 40 external user accounts.

[View User Report](#) [Purchase more user accounts](#) [Configure advanced authentication options](#)

Cabinet administrators can add external users to the repository.



4. On the Advanced Authentication Configuration page, add an authentication requirement with the authentication method set to RSA SecurID.

Authentication Requirements

Requirement type: Authentication method ▼ RSA SecurID ▼ [Upload configuration file](#)

[Help](#)
[Delete this requirement](#)

[Add another requirement](#)

OK Cancel

5. Click the “Upload configuration file” link. Browse to the configuration file downloaded in step 2 (it will be named sdconf.rec), select it, and click OK to upload this file to NetDocuments.
6. You may want to define additional authentication requirements. For example, if you want to require RSA SecurID authentication from outside your office but don’t want to require it inside the office, add an authentication requirement with the requirement type set to “IP Address” and enter your office’s external IP address range.

User Experience

Once an RSA SecurID authentication requirement has been defined, members of the repository will be prompted to log in with their SecurID credentials after logging in with their NetDocuments credentials, unless their login fulfills a different authentication requirement (such as an IP Address requirement).

Users will first be prompted for their RSA username:

Sand Creek Software RSA Login

Username:

OK Cancel



After entering the username, users will then be prompted for their passcode:

Sand Creek Software RSA Login

Enter PASSCODE:

In some cases, users might also be prompted to select a new PIN or enter the next tokencode from their SecurID token.

Sand Creek Software RSA Login

Enter a new PIN between 4 and 8 alphanumeric characters:

Sand Creek Software RSA Login

Wait for the tokencode to change,
then enter the new tokencode:



Certification Checklist For RSA Authentication Manager 7.x

Date Tested: July 24, 2009

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	7.1	Windows Server 2003
NetDocuments	2009-R5	Windows Server 2003

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
PIN Reuse	<input checked="" type="checkbox"/>	PIN Reuse	<input type="checkbox"/> N/A
Passcode			
16 Digit Passcode	<input checked="" type="checkbox"/>	16 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
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
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
RSA SecurID 800 Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A

JGS / PAR

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



Appendix

Node Secret: Uploaded via the Advanced Authentication Configuration page in NetDocuments. See page 5 for details.

sdconf.rec: Stored internally by NetDocuments

sdopts.rec: N/A

sdstatus.12: Stored internally by NetDocuments