Amiura
Amiura SignOn Agent

RSA SecurID Ready Implementation Guide

Last Modified: June 17th, 2009

Partner Information

Product Information	
Partner Name	Amiura
Web Site	www.amiura.com
Product Name	Amiura SignOn Agent
Version & Platform	2.0, Windows / Linux
Product Description	The Amiura SignOn Agent's purpose is to enhance security by enabling users to login to IBM Lotus Domino web server using a two factor authentication mechanism based on RSA Security SecurID one time passwords (OTP). Customers may publish Domino based information on the web in a secure and simple way without the need of a VPN.
Product Category	Access Management

Solution Summary

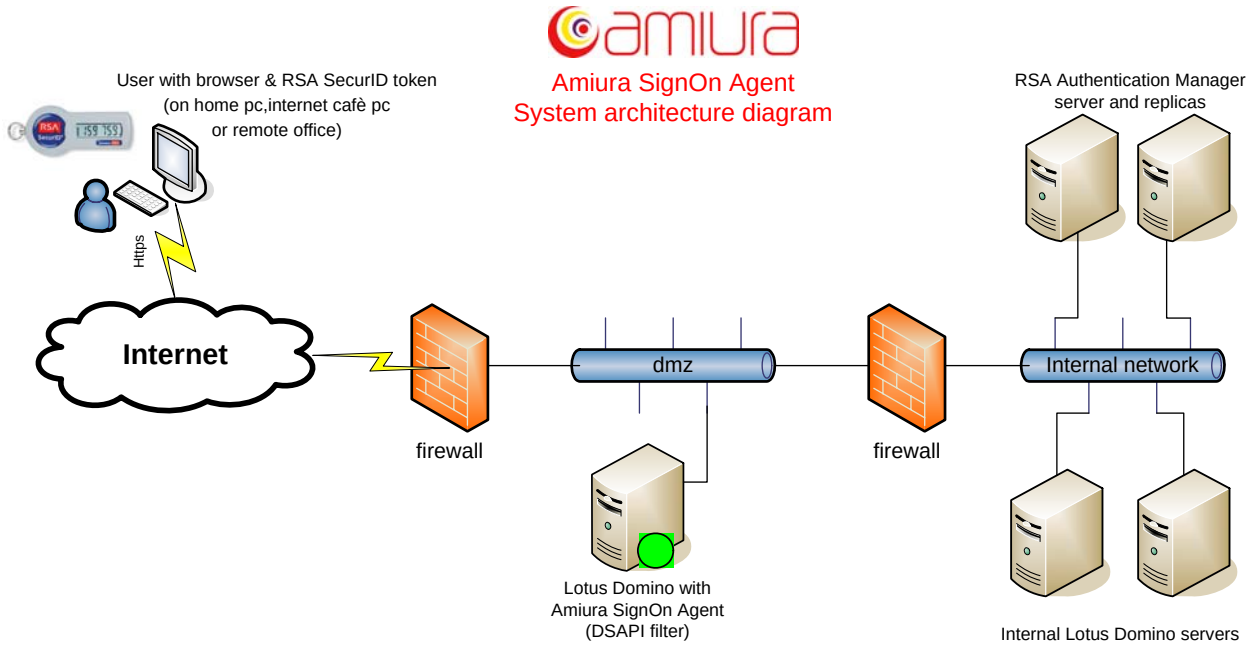
Amiura SignOn Agent is a Domino Server API (DSAPI) filter that checks authentication requests and verifies that a valid passcode is typed by the user. The login form in IBM Lotus Domino is extended with a field where the user types the passcode. The RSA PIN may be the same as the IBM Lotus Domino internet password (if the user has set them to be the same); in this case, the filter composes the passcode by appending the tokencode to the Domino internet password/RSA PIN.

The deployment consists of configuring the Lotus Domino web server to load the Amiura SignOn Agent filter on startup, copying the needed files to the Lotus Domino server host, and setting a few parameters on the Domino server notes.ini file.

The agent solves a problem posed by multiple authentication steps required to access corporate systems: login to VPN systems and then to web servers. With Amiura SignOn Agent, the security achieved is the same as that obtained with VPN systems and it takes place in one single step.

The addition of Amiura SignOn Agent to an IBM Lotus Domino infrastructure allows a company to make available on the internet email and Domino applications in a secure way.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication
RSA SecurID Library Version Used	Native C 6.1
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	N/A
RSA Authentication Agent Host Type for 6.1	UNIX
RSA Authentication Agent Host Type for 7.1	Standard Agent
RSA SecurID User Specification	Designated Users, All Users
RSA SecurID Protection of Administrative Users	No
RSA Software Token and RSA SecurID 800 Automation	No



Product Requirements

Partner Product Requirements: Amiura SignOn Agent DSAPI filter (server side)	
Version	Lotus Domino v 7.0.x
	Lotus Domino v 8.0.x
	Lotus Domino v 8.5

Operating System	
Platform	**Required Patches**
Windows 2003 32 bit	Service pack 1 or later
Linux RedHat 5.2	All Patch Levels Supported

Partner Product Requirements: Amiura SignOn Agent (client side)	
Browsers supported	Internet Explorer
	FireFox
	Safari

Operating System	
Platform	**Required Patches**
Windows 2003 32 bit	Service pack 1 or later
Linux RedHat 5.2	All Patch Levels Supported

Note: Cookies must be enabled within the Web Browser.

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 the Amiura SignOn Agent and the 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 Amiura SignOn Agent 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, you should configure the Amiura SignOn Agent as Standard Agent. This setting is used by the RSA Authentication Manager to determine how communication with the Amiura SignOn Agent 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	%systemroot%\system32\sdconf.rec
Node Secret	%systemroot%\system32\securid
sdstatus.12	%systemroot%\system32\sdstatus.12
sdopts.rec	Not implemented

Partner Product Configuration

Before You Begin

This section provides instructions for integrating the partners' product 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 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.

Solution Overview

Please review the installation process completely before starting installation.

Installation overview:

1. Register Lotus Domino host record on the Authentication Manager server.
2. Copy ASA login form to domcfg.
3. Create ASAForms.nsf (from ASAForms.ntf provided).
4. Copy nAmiuraSignOnAgent.dll the filter library to the Domino program folder.
5. Set DSAPI field in the web site configuration document.
6. Set notes.ini variables.
7. Stop and restart http task.

> **Note: During the installation we refer to the agent library as nAmiuraSignOnAgent.dll. If you are using the evaluation version, you should use nAmiuraSignOnAgentEval.dll instead. For the Linux version the filename extension is .so**

Register Lotus Domino Host Record on the Authentication Manager

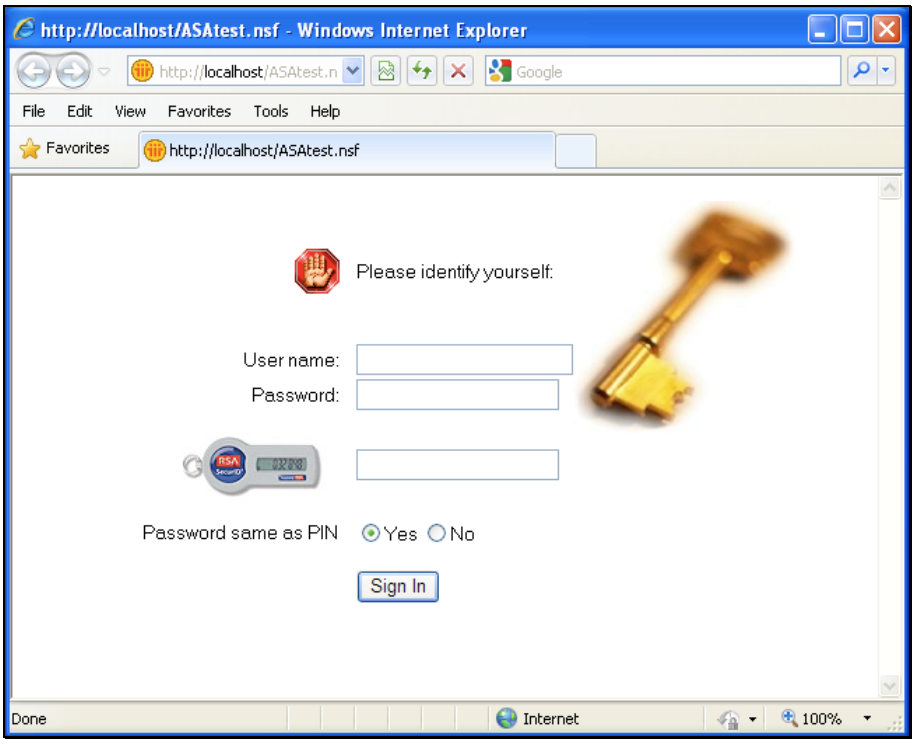
The Amiura SignOn Agent will be requesting authentication services from the RSA Authentication Manager. In this respect, Amiura SignOn Agent is an "agent" and must be setup as such according to the RSA Authentication Manager Administrator's Guide. In this step you will need the help of your Authentication Manager system administrator.

> **Note: We are assuming that the user's default login on the RSA Authentication Manager is the same as the user's username on Domino. For example, for user John Doe, it could be jdoe. If this is not the case, user's must be set up accordingly (add alias as username in person document on Domino Directory or setup login for user on this agent in the Agent Host Activations dialog).**

Copy ASA Login Form to domcfg.nsf

In this step you are going to use IBM Lotus Domino Designer. You need some knowledge of Domino design.

1. From the database ASAdomcfg.ntf, copy the form ASALogin to your Domino server's domcfg.nsf database. This database contains a customized login form (ASALogin) that has a third field for the RSA token code. Copy also the image resource depicting the RSA token.



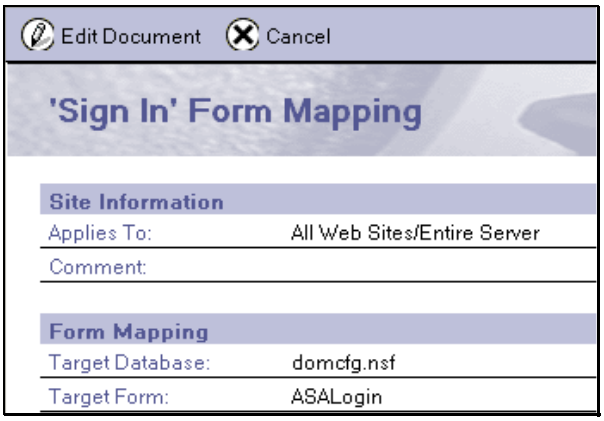
If you like, you may customize this form with your own company logo. Do not change the name of the fields.

This form must be set as the login form for the web site. You do this in the next step by adding a “Sign In Form mapping” on the Domino server domcfg.nsf.

> **Note: The fourth field (Domino internet password same as PIN) indicates if Amiura SignOn Agent should use the Domino internet password as the RSA SecurID PIN to form the passphrase. If tokens are configured for tokencode only, this field may be set to default No and hidden.**

2. Set the **‘Sign In’ form mapping** as follows:

- Target Database: domcfg.nsf
- Target Form: ASALogin



Create db ASAForms

You must create a new database on the Domino server. This database has the forms needed in case the agent needs more information after the passcode is submitted.

1. Create the database on the Domino server as follows:
    - Name the database ASAForms.nsf
    - template ASAForms.ntf

This database default name is ASAForms.nsf. If you need or want to name it otherwise, you have to set the appropriate notes.ini variable (see section on notes.ini settings).

Copy nAmiuraSignOnAgent.dll

This file is a Domino DSAPI filter and it is loaded by the http when configured as DSAPI filter in the Domino configuration for web sites.

You should copy this file to the Domino program folder.

On Windows platforms this is something like:

c:\program files\lotus\domino

Follow these steps:

1. Copy the file nAmiuraSignOnAgent.dll to your Domino executable folder.
2. If you are on Linux, give it execution rights and grant access to the user under which Domino server runs.

Set DSAPI Field

For the Amiura SignOn Agent to be loaded (by the http server task), it must be set up as a DSAPI filter. This is done differently based on the configuration of your Domino server. If your server has the "**Load Internet configurations from Server\Internet Sites documents:**" enabled, then you set up the DSAPI filter in the Web site document, otherwise, you set it up on the Domino server document itself.

We will assume you have a Domino server that uses "**Server\Internet Sites documents**".

1. To set the Amiura SignOn Agent as a DSAPI filter, follow this steps:
    - Open the web site document you want to set the filter on.
    - Go to the Configuration tab.
    - On the DSAPI section put the filter file name (see figure).
    - Save and close the document.

Set notes.ini Variables

The notes.ini variables used by the http filter are the following:

- ASA_Debug: this variable determines whether a debug log is written.
  Values: 0 (zero) no log, 1 log enabled
- ASA_LogFile: set to the file were log should be written (used only if ASA_Debug=1)
  Value: full pathname of log file (i.e. **c:\log.txt**)
- optional variables
- ASA_FormsDB: forms db name (relative to data folder) created in the **Create db ASAForms** section.
  Default if variable not set: ASAForms.nsf

- ASA_MaxSessions: max number of filter sessions (used when token is not in standard state like new pin mode or next token code).
  Default if variable not set: 512

Stop and Restart http Task

For the http task to load the Amiura SignOn Agent, the http task must be restarted.

1. You can do this by issuing the following commands from the Domino server console:

tell http quit

> **Note: Wait for the message "HTTP Server: Shutdown" to appear before moving to the next step.**

2. Once the http task has stopped, issue the following command:

load http

3. You should see a message indicating the Amiura SignOn Agent has been loaded. The message says:

HTTP Server: DSAPI Amiura SignOn Agent Loaded successfully

Certification Checklist for RSA Authentication Manager v6.x

Date Tested: May 5th, 2009

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	6.1	Microsoft Windows Server 2003 32bit
RSA Authentication Agent	IBM Lotus Domino 7.0.2	Microsoft Windows Server 2003 32bit
RSA Remote Authentication Client	Internet Explorer 6.0	Microsoft Windows XP SP2
Amiura SignOn Agent	2.0	Microsoft Windows Server 2003 32bit

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 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	
Set Credential	N/A	Set Credential	
Retrieve Credential	N/A	Retrieve Credential	

BSD / PAR

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

Certification Checklist for RSA Authentication Manager 7.x

Date Tested: May 15th, 2009

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1	Windows Server 2003 32bit
RSA Authentication Agent	IBM Lotus Domino 7.0.2	Windows Server 2003 32bit
RSA Remote Authentication Client	FireFox 3.0	Microsoft Windows XP SP2
Amiura SignOn Agent	2.0	Windows Server 2003 32bit

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
PIN Reuse	✓	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
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	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
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
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A

BSD / PAR

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