Winchester Business Systems
AtSignOn™

RSA SecurID Ready Implementation Guide

Last Modified: August 18, 2011

Partner Information

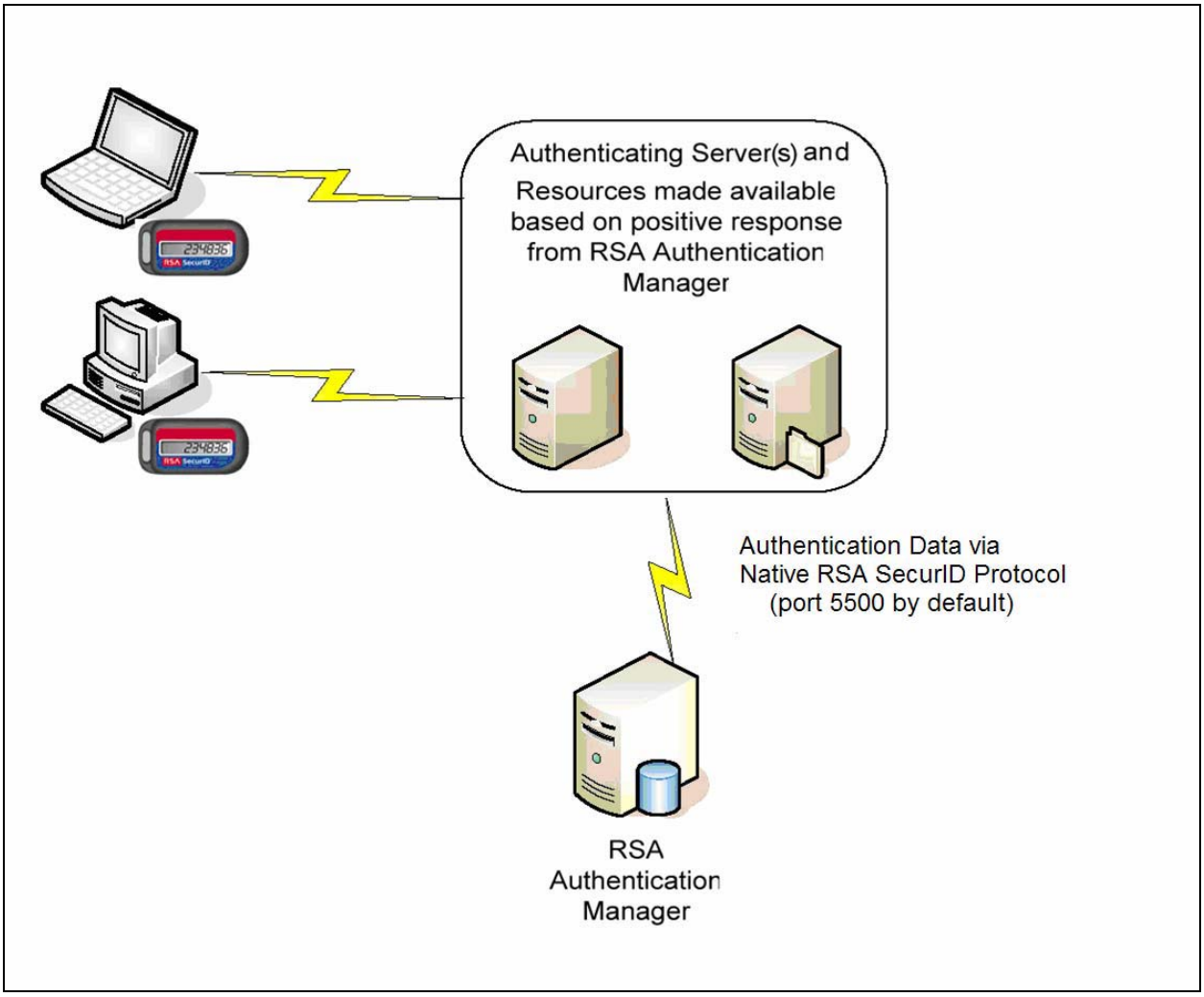
Product Information	
Partner Name	Winchester Business Systems
Web Site	**www.wbsnet.com**
Product Name	AtSignOn™
Version & Platform	Version 8.6 for Platform: Domino/Windows
Product Description	AtSignOn for Lotus® Domino™ software uses RSA SecuID® two-factor authentication to enhance security on Lotus Domino R5, R6, R6.5, R7, R8 and R8.5 Web servers. The Agent enhances the authentication of those who use Web browsers to access Lotus Domino resources, such as Lotus databases (address books, calendars, email), URL directories and files on a Domino server that are protected by RSA SecurID®. When AtSignOn protection is enables on a Web server, users who attempt to view protected resources are prompted to enter an RSA SecurID PASSCODE. If the PASSCODE is valid, the user is given access to the protected resource. If the PASSCODE is not valid, the user is denied access. Only those users who are registered as token holders in the RSA® Authentication Manager database are able to access the RSA SecurID-protected Web resources

Solution Summary

AtSignOn for Lotus® Domino™ software uses RSA SecurID® two-factor authentication to enhance security on Lotus Domino R5, R6, R7, R8 and R8.5 Web servers. The Agent enhances the authentication of those who use Web browsers to access Lotus Domino resources, such as Lotus databases (address books, calendars, mail), URL directories and files on a Domino server that are protected by RSA Authentication Manager (SecurID). This Agent is used in combination with the RSA Authentication Manager® authentication management software and RSA SecurID® tokens.

When AtSignOn protection is enabled on a Web server, users who attempt to view protected resources are prompted to enter an RSA SecurID PASSCODE. If the PASSCODE is valid, the user is given access to the protected resource. If the PASSCODE is not valid, the user is denied access. Only those users who are registered as token holders in the RSA Authentication Manager database are able to access the RSA SecurID-protected Web resources.

RSA SecurID supported features AtSignOn Version 8.6	
RSA SecurID Authentication via Native RSA SecurID Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	No
On-Demand Authentication via Native SecurID Protocol	Yes
On-Demand Authentication via RADIUS Protocol	No
On-Demand Authentication via API	Yes
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	No
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	Yes


Authenticating Server(s) and
Resources made available
based on positive response
from RSA Authentication
Manager
Authentication Data via
Native RSA SecurID Protocol
(port 5500 by default)
RSA
Authentication
Manager

Authentication Agent Configuration

Agent Host Records contain information that allows an RSA Authentication Manager server to locate its clients and establish secure communication channels with them. The server's database must contain an Agent Host Record to identify each AtSignOn host in a given environment. In order to create this record, the following information is required for each AtSignOn instance:

- Hostname
- IP Addresses for network interfaces

Set the Agent Type to "Standard Agent" when adding the Authentication Agent. This setting is used by the RSA Authentication Manager to determine how communication with AtSignOn will occur.

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

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	%SYSTEMROOT%\system32\sdconf.rec File
Node Secret	None stored
sdstatus.12	%SYSTEMROOT%\system32\sdstatus.12
sdopts.rec	%SYSTEMROOT%\system32\sdopts.rec

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

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the AtSignOn™ 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 AtSignOn™ components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuring AtSignOn™ for RSA SecurID Authentication

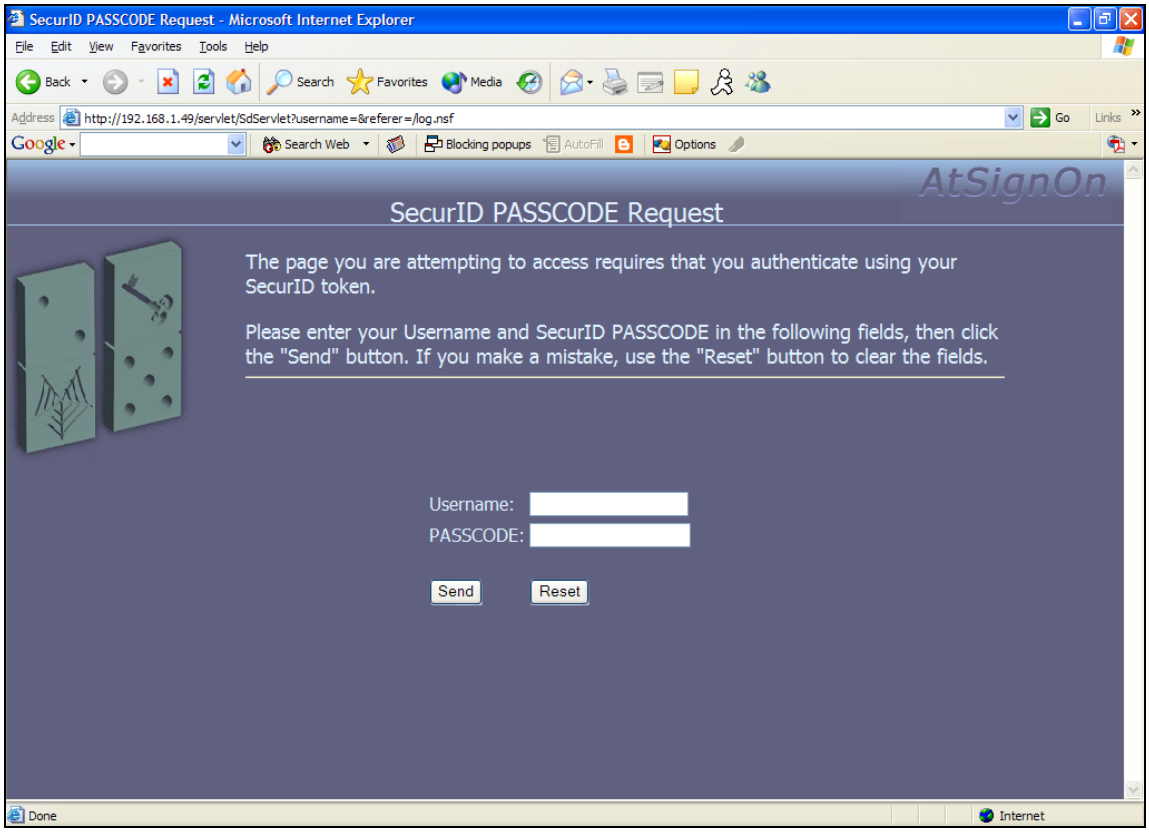
1. Sign into the Domino Administrator as the system administrator ir a user with access to run unrestricted access and code. Select the **SECURID.NSF** database and go to the **Internet Protocols** tab.
2. Select the the **HTTP** sub tab and verfy that the **DSAPI Filter File Name** field contains the *sddomino.dll* file's absolute path.
    - For Domino R5, enter *%SYSTEMROOT%\system32\sddomino.dll*
    - For Domino R6, R7 and R8, enter *%DominoProgramPath%\jvm\bin\sddomino.dll*

    Note: This value can be set in the Domino Site document if option "Load Internet configurations from Server\Internet Sites documents" is enabled in the Domino Server Document.
3. Select the **Domino Web Engine** sub tab verify the **Maximum cached users** field's value is *0*. (This is required for Lotus Domino R6.0.x, R6.5.x, R7.x and R8.x).
4. Verify that either *Domino Servlet Manager* or *Third Party Servlet Support* is specified in the **Java Servlet Support** field.
5. Restart http task on Domino using the **tell http quit** and **load http** commands.

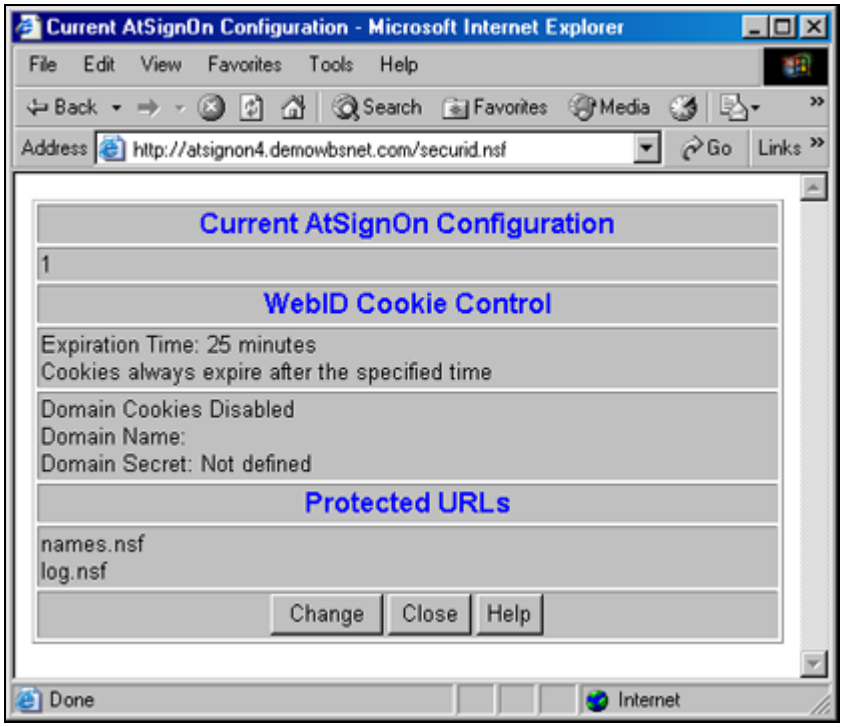
Configuring the Protected Resources:

1. Start your Web browser and then open the following AtSignOn Administration database URL: *http://servername/securid.nsf*, where *servername* is the name or IP address of the Domino server.
2. When prompted, enter your RSA SecurID® username and PASSCODE.

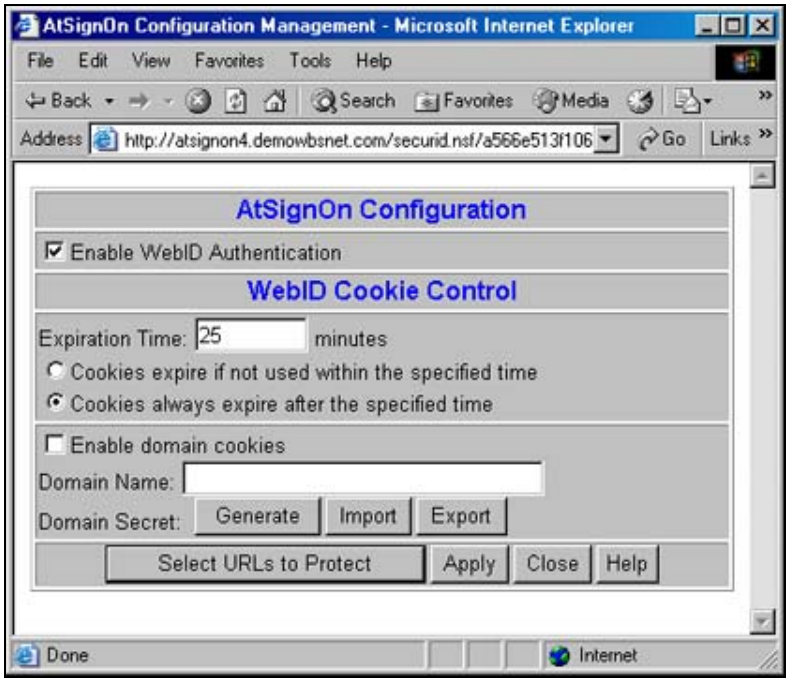
> **Note: The administrator of this database must have full-unrestricted access to run all methods and operations.**



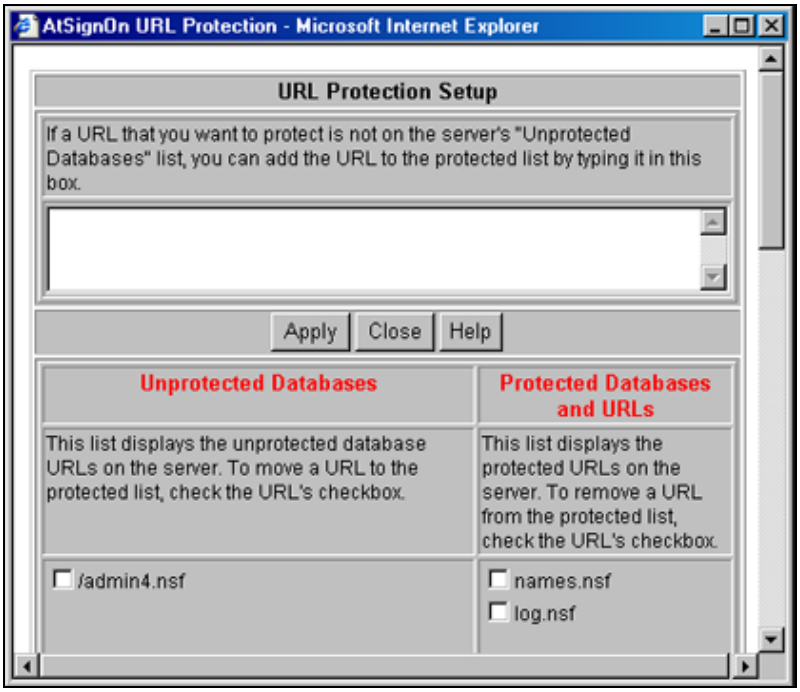
3. The AtSignOn Administration window opens in View mode, where you can see the current configuration settings and list of protected resources.



4. Click click the **Change** button to enter Edit mode. Modify the configuration settings if necessary.



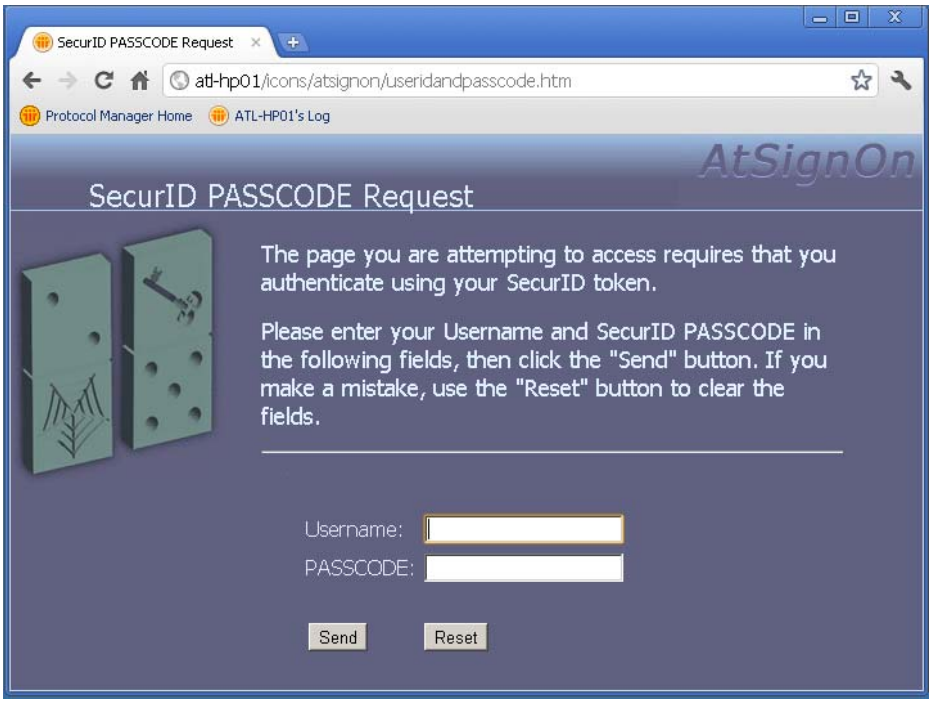
5. Click **Select URLs to Protect** button and add the URLs you wish to protect to the list.



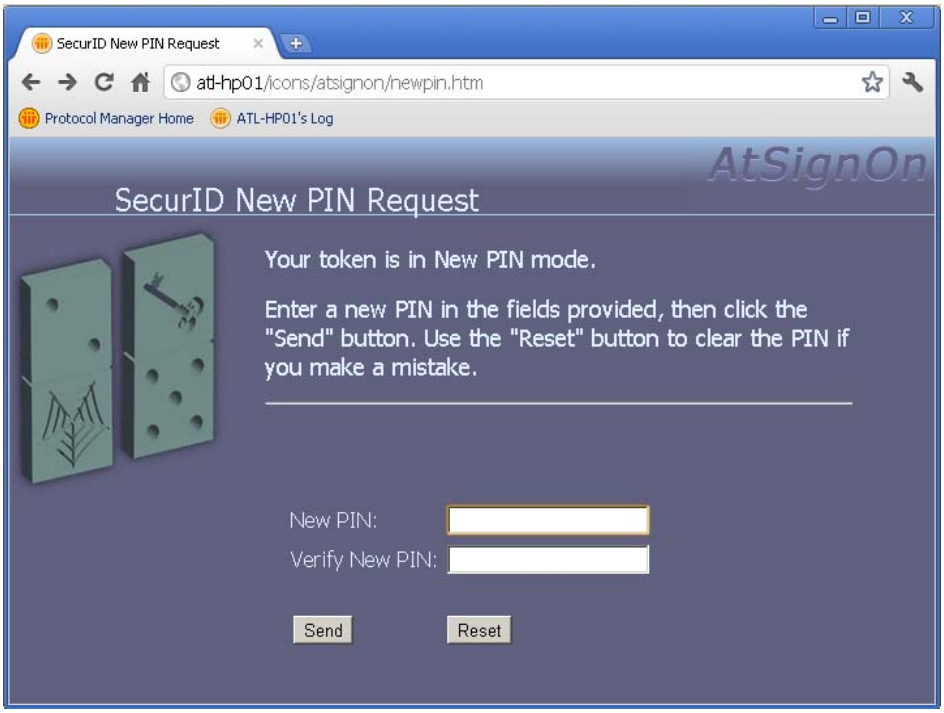
6. To save your changes, click the **Apply** button. To cancel your changes, click the **Close** button.
7. Click the **Close** button in the summary window to return to the AtSignOn Administration window in View mode.
8. Restart the Domino server's **HTTP** task to put your changes into effect.

User Experience

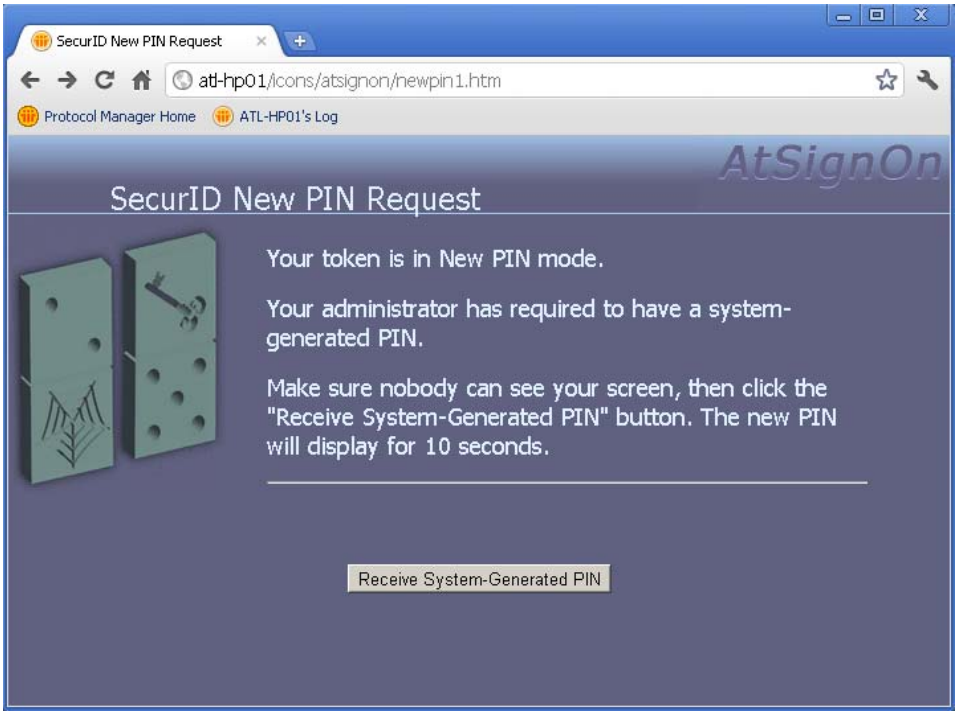
Login screen:



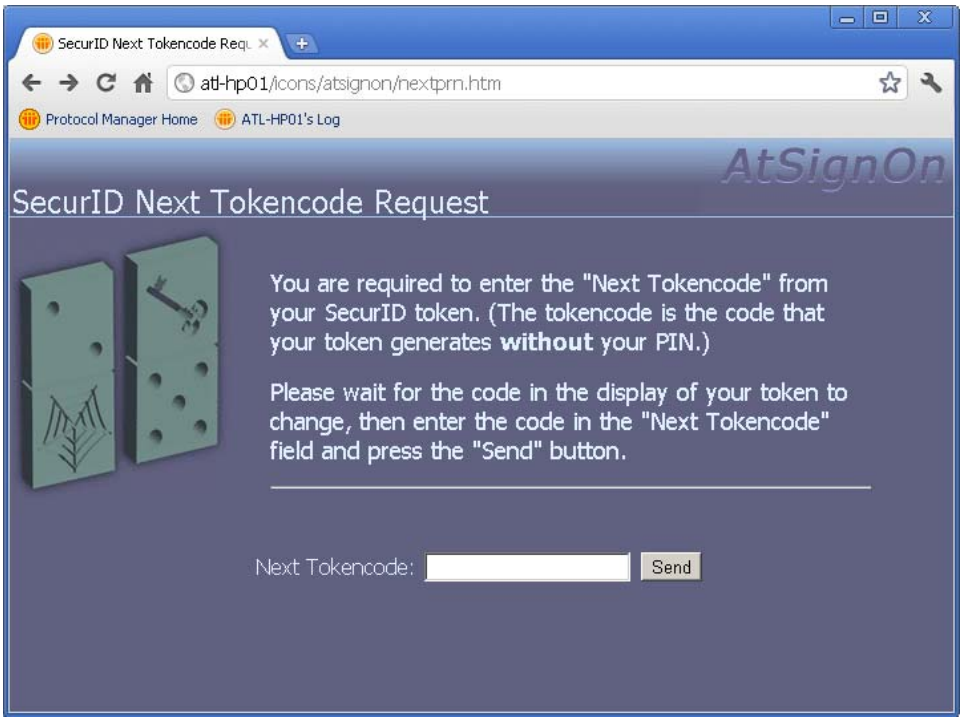
User-generated New PIN:



System-generated New PIN:



Next Tokencode:


SecurID Next Tokencode Requ
atl-hp01/icons/atsignon/nextprn.htm
Protocol Manager Home
ATL-HP01's Log
AtSignOn
SecurID Next Tokencode Request
You are required to enter the "Next Tokencode" from your SecurID token. (The tokencode is the code that your token generates **without** your PIN.)
Please wait for the code in the display of your token to change, then enter the code in the "Next Tokencode" field and press the "Send" button.
Next Tokencode:
Send

Certification Checklist for RSA Authentication Manager

Date Tested: June 26, 2007

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1	Windows 2008
RSA Authentication Agent	Domino Server R8.5	Windows 7
RSA Remote Authentication Client	Google Chrome 13.0	Windows XP
AtSignOn	8.6	Windows 7

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/ PAR

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

Certification Checklist for RSA Authentication Manager

RSA Software Token Automation Functionality			
RSA Native Protocol		**RADIUS Protocol**	
PINless Token	N/A	PINless Token	N/A
PINpad-style Token	N/A	PINpad-style Token	N/A
Fob-style Token	N/A	Fob-style Token	N/A
16-Digit Passcode	N/A	16-Digit Passcode	N/A
Alphanumeric PIN	N/A	Alphanumeric PIN	N/A
New PIN Mode	N/A	New PIN Mode	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
Password-Protected Token	N/A	Password-Protected Token	N/A

RSA SecurID 800 Token Automation Functionality			
RSA Native Protocol		**RADIUS Protocol**	
PINless Mode	N/A	PINless Mode	N/A
16-Digit Passcode	N/A	16-Digit Passcode	N/A
New PIN Mode	N/A	New PIN Mode	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A

JGS / PAR

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

Appendix

Partner Integration Details	
RSA SecurID API	AuthSDK_C_v8.1.1.109 06/03/11 03:16:51
RSA Authentication Agent Type	Domino web server Web Agent
RSA SecurID User Specification	All Users
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	Yes

Node Secret:

- To remove the Node Secret from AtSignOn, you will need to manually delete a specific RSA Authentication Manager reference “NodeSecret” located in the following registry key:

  “HKEY_LOCAL_MACHINE\SOFTWARE\SDTI\ACECLIENT”.

sdconf.rec:

- To remove the sdconf.rec references from AtSignOn, you will need to manually delete them from the Window’s system directory. (typically c:\WINDOWS\system32)

sdopts.rec:

- To remove the sdopts.rec references from AtSignOn, you will need to manually delete them from the Window’s system directory. (typically c:\WINDOWS\system32)

sdstatus.12:

- To remove the sdstatus.12 references from AtSignOn, you will need to manually delete them from the Window’s system directory. (typically c:\WINDOWS\system32)

Agent Tracing:

- To enable Agent Tracing for AtSignOn, you will need to manually create three specific RSA Authentication Manager references located in the following registry key:

  “HKEY_LOCAL_MACHINE\SOFTWARE\SDTI\ACECLIENT”.
  1. “TraceDest” Value data: 4 Base: Hexadecimal
  2. “TraceLevel” Value data: f Base: Hexadecimal
  3. “TraceProc” Value data: 0 Base: Hexadecimal