Click Studios
Passwordstate

RSA SecurID Ready Implementation Guide

Last Modified: October 3, 2013

Partner Information

Product Information	
Partner Name	Click Studios SA Pty Ltd
Web Site	www.clickstudios.com.au
Product Name	Passwordstate
Version & Platform	V6 & Microsoft Platform
Product Description	Passwordstate is a web-based solution for secure management of passwords, for both individuals and teams of people.

Solution Summary

Passwordstate uses SecurID tokens, either physical or software, to provide two-factor authentication for users accessing the Passwordstate web site, or individual Password Lists once initial access has been granted.

RSA Authentication Manager supported features	
Click Studios Passwordstate 6.1	
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
Risk-Based Authentication	No
Risk-Based Authentication with Single Sign-On	No
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	No

Authentication Agent Configuration

Authentication Agents are records in the RSA Authentication Manager database that contain information about the systems for which RSA SecurID authentication is provided. All RSA SecurID-enabled systems require corresponding Authentication Agents. Authentication Agents are managed using the RSA Security Console.

The following information is required to create an Authentication Agent:

- 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 Passwordstate 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	'/securid' folder in the Passwordstate web site
Node Secret	'/securid' folder in the Passwordstate web site
sdstatus.12	'/securid' folder in the Passwordstate web site
sdopts.rec	'/securid' folder in the Passwordstate web site

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

Configure Passwordstate with RSA SecurID Authentication

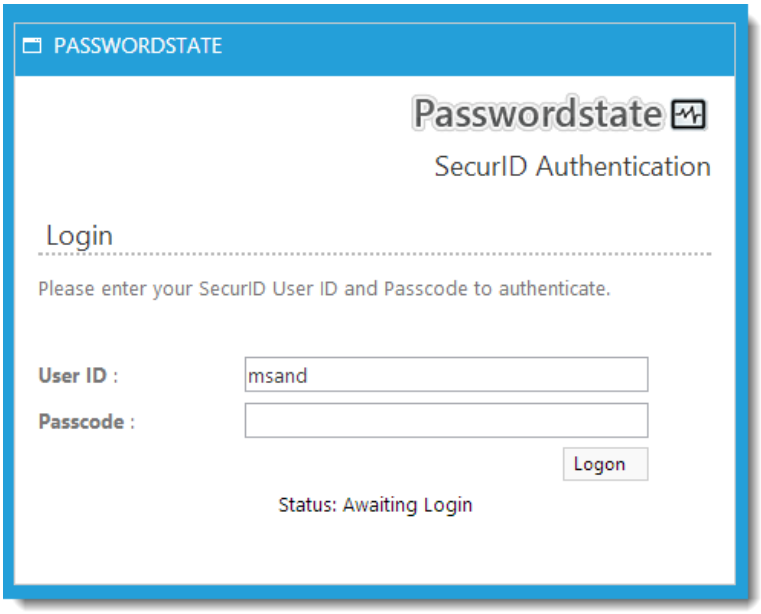
1. Download the sdconf.rec agent configuration file from the Security Console of your RSA Authentication Manager Server.
2. Copy the sdconf.rec agent configuration file into the '/securid' folder of the Passwordstate web site. The default path for this directory is:

```
c:\inetpub\passwordstate\securid
```

Click Studios Passwordstate is now configured for RSA SecurID Authentication.

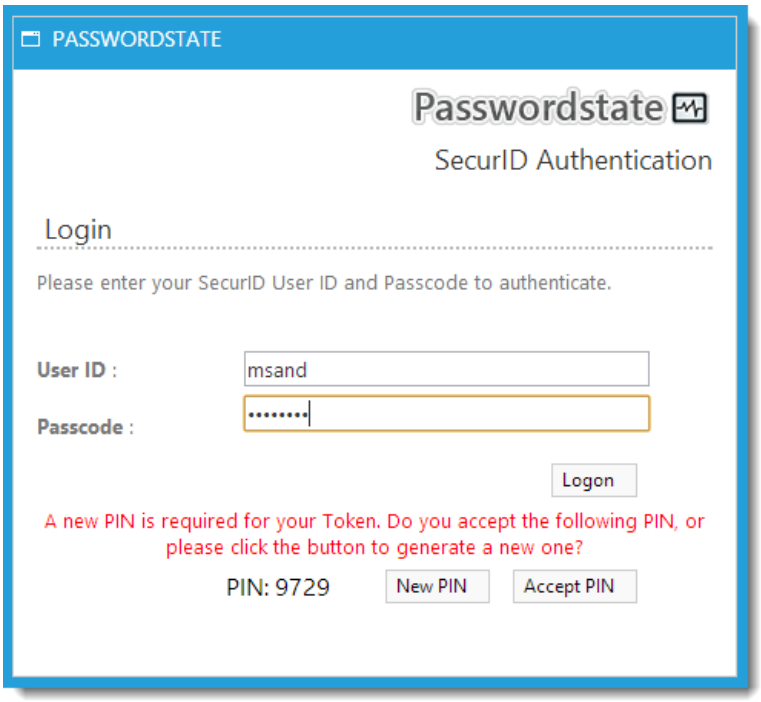
RSA SecurID Login Screens

Login screen:

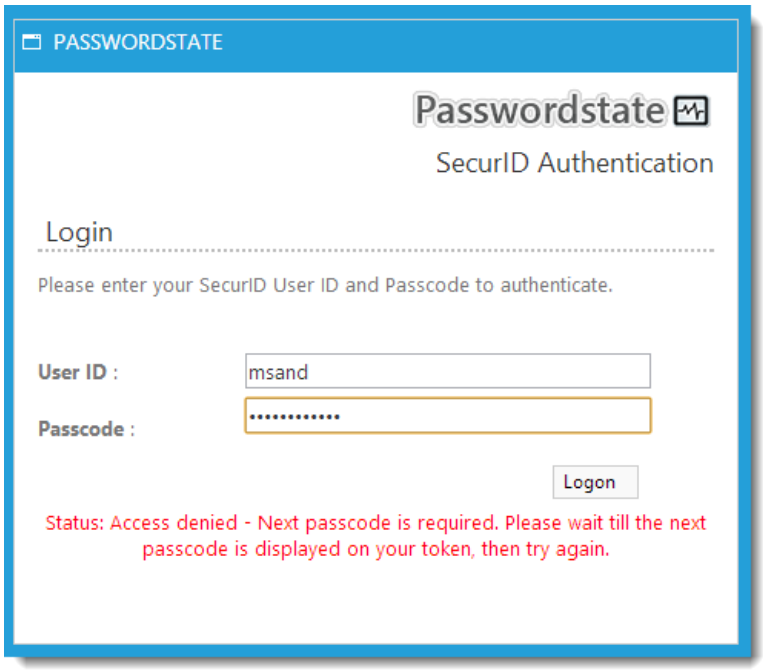


User-defined New PIN:

System-generated New PIN:



Next Tokencode:



Certification Checklist for RSA Authentication Manager

Date Tested: October 1, 2013

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.0	Virtual Appliance
Click Studios Passwordstate	6.1	Windows Server 2012

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 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

PEW / PAR

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

Appendix

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

Node Secret:

The node secret (securid) file is located in the '/securid' folder in the Passwordstate web site. Delete the file to clear the node secret.

sdconf.rec:

The sdconf.rec configuration file is located in the '/securid' folder in the Passwordstate web site. Overwrite the sdconf.rec file to update the RSA Authentication Manager configuration.

sdopts.rec:

The sdopts.rec file (optional) is located in the '/securid' folder in the Passwordstate web site.

sdstatus.12:

The sdstatus.12 file is located in the '/securid' folder in the Passwordstate web site.

Agent Tracing:

Enable agent tracing by specifying the appropriate registry keys in the Windows system registry. Refer to RSA Agent documentation for more information on agent tracing.