



RSA SecurID Ready Implementation Guide

Last Modified: Nov 24, 2008

Partner Information

Product Information	
Partner Name	Lieberman Software Corporation
Web Site	www.liebsoft.com
Product Name	Account Reset Console
Version & Platform	5.0.1
Product Description	Account Reset Console is a central point of management for user logon account password resets and password reset auditing for the Microsoft Windows platform.
Product Category	User Provisioning



LIEBERMANSOFTWARE

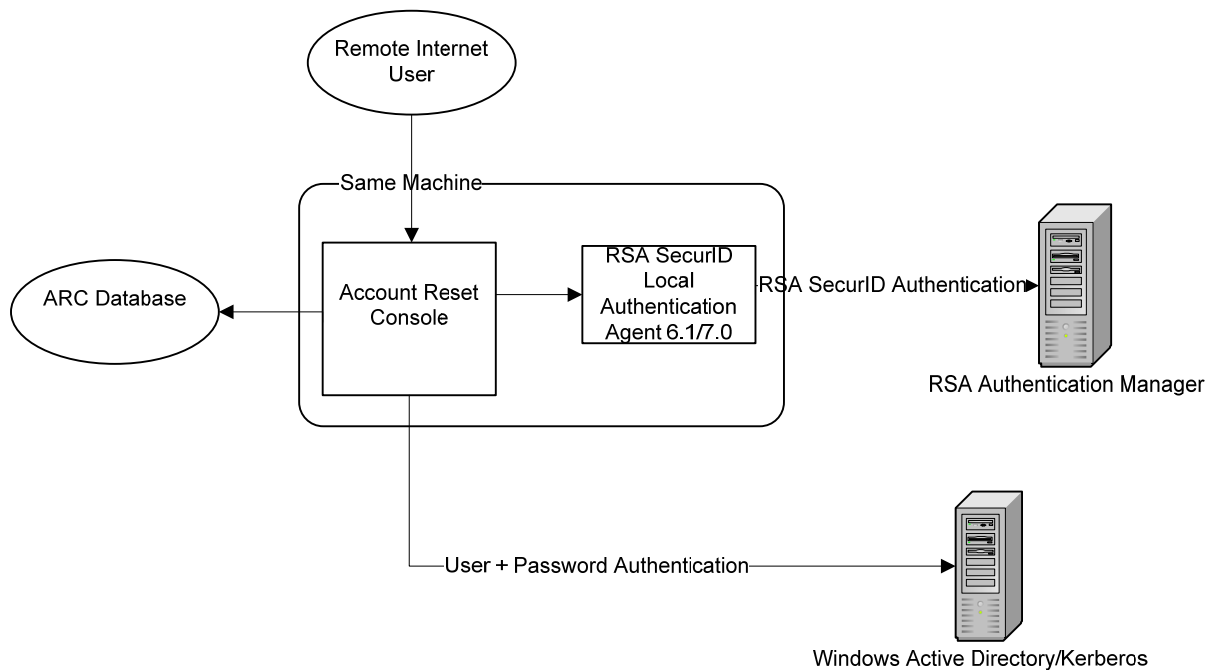


Solution Summary

Account Reset Console is a privileged password management platform. It provides the Help Desk with the ability to reset domain account passwords/account flags, and allows users to reset their own forgotten or expiring passwords in a fully audited and delegated manner via any web browser.

RSA SecurID authentication controlled access is provided to the web users of the application. Full token management including Next Token and New PIN selection are provided. Both RSA Authentication Manager and Account Reset Console track RSA SecurID logons for audit purposes.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication
List Library Version Used	6.1
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	No
RSA Authentication Agent Host Type for 6.1	Net OS
RSA Authentication Agent Host Type for 7.1	Standard Agent
RSA SecurID User Specification	Designated Users (via group membership)
RSA SecurID Protection of Administrative Users	Yes
RSA Software Token and RSA SecurID 800 Automation	No





Product Requirements

Partner Product Requirements: Account Reset Console	
Version	
Account Reset Console 5.0 or later	
IIS 5, 6 and 7	ASP must be enabled

Operating System	
Platform	Required Patches
Windows 2000	SP4 and later
Windows XP	SP2 and later
Windows 2003	SP1 and later



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 Account Reset Console 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 Account Reset Console 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 Account Reset Console as Net OS. This setting is used by the RSA Authentication Manager to determine how communication with the Account Reset Console 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:\Windows\system32
Node Secret	C:\Windows\system32
sdstatus.12	C:\Windows\system32
sdopts.rec	Not implemented

 **Note: Go to the appendix of this document to get detailed information regarding these files.**



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.

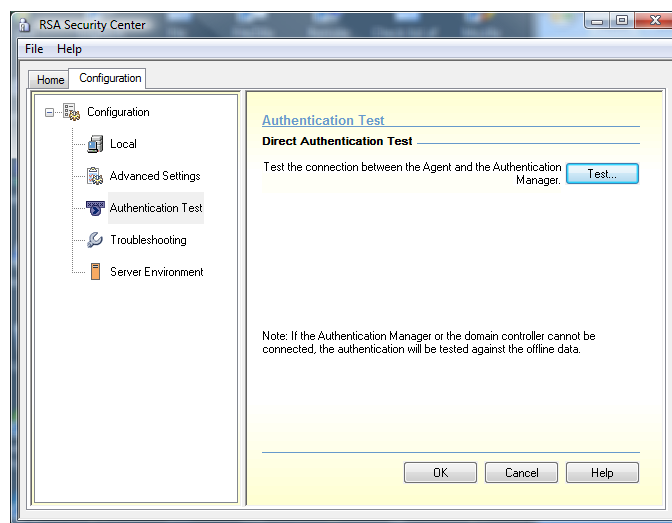
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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.

Documenting the Solution

Confirm RSA Authentication Agent Functions Correctly:

Prior to the use of RSA SecurID Authentication by this application, confirm that the RSA SecurID Authentication Agent is capable of authentication by using the **RSA Security Center** application to do an authentication test.



Do not attempt to set up application use of RSA SecurID Authentication until you can successfully authenticate with the RSA Security Center application. If you don't get the agent to authenticate, you will not be able to successfully get the application to use RSA SecurID Authentication.

Name format used for RSA Authentication Manager

If the user logs on to ARC as local user, his/her RSA credential will be username only.

If the user logs on to ARC as domain user, his/her RSA credential will be domainname\username.



Add user group(s) that require(s) RSA SecurID Authentication

1. Log into Account Reset Console and navigate to **Management | Program Access**.
2. Check **Require Web Logon with SecurID** and enter the group name.
3. Click **Add Rule**. All users that belong to the group will require RSA SecurID Authentication.

Note: If a user belongs to both “Allow Web Logon without SecurID” and “Require Web Logon with SecurID” groups, he/she will be required to perform an RSA SecurID Authentication.

LIEBERMANSOFTWARE
Account Reset Console

Logged-in user: **lanicu** [\[Log Out\]](#)

Accounts Scheduling/Reporting Management Configuration Index

Manage Program Access Permissions

<p>Program Access</p> <p>Group Access</p> <p>Helpdesk Reset Features</p> <p>Self Reset Features</p> <p>Configure Email Settings</p> <p>Appearance</p> <p>Mobile Settings</p>	<p>Add a New Global Program Access Rule:</p> <p><input type="checkbox"/> Allow Web Logon without SecurID</p> <p><input checked="" type="checkbox"/> Require Web Logon with SecurID</p> <p><input type="checkbox"/> Allow Reset of Other Users' Accounts</p> <p><input type="checkbox"/> View Console Logs and Task Reports</p> <p><input type="checkbox"/> Manage All Web Access Controls</p> <p style="text-align: right;">Domain: rsagroup <input type="button" value="Add Rule"/></p> <p>Global Program Access Rules</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #f2f2f2;"> <th>Global Access Category</th> <th>Allowed Windows Groups</th> </tr> </thead> <tbody> <tr> <td>Allow Web Logon without SecurID</td> <td>administrators [del]</td> </tr> <tr> <td>Manage All Web Access Controls</td> <td>administrators [del]</td> </tr> <tr> <td>Allow Reset of Other Users' Accounts</td> <td>administrators [del]</td> </tr> <tr> <td>View Console Logs and Task Reports</td> <td>administrators [del]</td> </tr> </tbody> </table>	Global Access Category	Allowed Windows Groups	Allow Web Logon without SecurID	administrators [del]	Manage All Web Access Controls	administrators [del]	Allow Reset of Other Users' Accounts	administrators [del]	View Console Logs and Task Reports	administrators [del]
Global Access Category	Allowed Windows Groups										
Allow Web Logon without SecurID	administrators [del]										
Manage All Web Access Controls	administrators [del]										
Allow Reset of Other Users' Accounts	administrators [del]										
View Console Logs and Task Reports	administrators [del]										

LIEBERMANSOFTWARE
Account Reset Console

Logged-in user: **lanicu** [\[Log Out\]](#)

Accounts Scheduling/Reporting Management Configuration Index

Manage Program Access Permissions

<p>Program Access</p> <p>Group Access</p> <p>Helpdesk Reset Features</p> <p>Self Reset Features</p> <p>Configure Email Settings</p> <p>Appearance</p> <p>Mobile Settings</p>	<p>Add a New Global Program Access Rule:</p> <p><input type="checkbox"/> Allow Web Logon without SecurID</p> <p><input type="checkbox"/> Require Web Logon with SecurID</p> <p><input type="checkbox"/> Allow Reset of Other Users' Accounts</p> <p><input type="checkbox"/> View Console Logs and Task Reports</p> <p><input type="checkbox"/> Manage All Web Access Controls</p> <p style="text-align: right;">Domain: rsagroup <input type="button" value="Add Rule"/></p> <p>Global Program Access Rules</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #f2f2f2;"> <th>Global Access Category</th> <th>Allowed Windows Groups</th> </tr> </thead> <tbody> <tr> <td>Allow Web Logon without SecurID</td> <td>administrators [del]</td> </tr> <tr> <td>Manage All Web Access Controls</td> <td>administrators [del]</td> </tr> <tr> <td>Require Web Logon with SecurID</td> <td>rsagroup [del]</td> </tr> <tr> <td>Allow Reset of Other Users' Accounts</td> <td>administrators [del]</td> </tr> <tr> <td>View Console Logs and Task Reports</td> <td>administrators [del]</td> </tr> </tbody> </table>	Global Access Category	Allowed Windows Groups	Allow Web Logon without SecurID	administrators [del]	Manage All Web Access Controls	administrators [del]	Require Web Logon with SecurID	rsagroup [del]	Allow Reset of Other Users' Accounts	administrators [del]	View Console Logs and Task Reports	administrators [del]
Global Access Category	Allowed Windows Groups												
Allow Web Logon without SecurID	administrators [del]												
Manage All Web Access Controls	administrators [del]												
Require Web Logon with SecurID	rsagroup [del]												
Allow Reset of Other Users' Accounts	administrators [del]												
View Console Logs and Task Reports	administrators [del]												



RSA Logon Screen

Everyone can log into Account Reset Console by providing the username and password. However, any user from the SecurID group has to complete the authentication before he/she can use any functionality of Account Reset Console.



Please log in to access the Account Reset Console.

Username

Password



Logged-in user: **ltao_liebsoft** [\[Log Out\]](#)

Accounts **Scheduling/Reporting** **Management** **Configuration** **Index**

Look up / Reset

Look up / Reset

Change My Password

Please Enter your SecurID Passcode

Passcode

Certification Checklist For RSA Authentication Manager v6.x

Date Tested: Sep, 24, 2008

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1	Windows Server 2003
RSA Authentication Agent	6.1	Windows Server 2003
Account Reset Console	5.0	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
User Selectable	<input checked="" type="checkbox"/>	User Selectable	<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
Passcode			
16 Digit Passcode	<input checked="" type="checkbox"/>	16 Digit Passcode	<input type="checkbox"/> N/A
4 Digit Password	<input checked="" type="checkbox"/>	4 Digit Password	<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
Name Locking Enabled	<input checked="" type="checkbox"/>	Name Locking Enabled	<input type="checkbox"/>
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
User Selectable	<input type="checkbox"/> N/A	User Selectable	<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
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
Credential Functionality			
Determine Cached Credential State	<input type="checkbox"/> N/A	Determine Cached Credential State	<input type="checkbox"/>
Set Credential	<input type="checkbox"/> N/A	Set Credential	<input type="checkbox"/>
Retrieve Credential	<input type="checkbox"/> N/A	Retrieve Credential	<input type="checkbox"/>

BSD / PAR

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

Certification Checklist For RSA Authentication Manager 7.x

Date Tested: Nov, 17, 2008

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	7.1	Windows Server 2003
RSA Authentication Agent	7.0	Windows Vista
Account Reset Console	5.0	Windows Vista

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

BSD / PAR

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



Appendix

Node Secret:

The node secret is maintained by the RSA SecurID Authentication Agent outside of the Account Reset Console application.

sdconf.rec

The node secret is maintained by the RSA SecurID Authentication Agent outside of the Account Reset Console application.

sdopts.rec:

Not used.

sdstatus.12:

The node secret is maintained by the RSA SecurID Authentication Agent outside of the Account Reset Console application.