



RSA SecurID Ready Implementation Guide

Last Modified: March 27, 2008

Partner Information

Product Information	
Partner Name	Oracle Corporation
Web Site	www.oracle.com
Product Name	Oracle 10g Single Sign-On Server
Version & Platform	10g (10.1.2.0.2) Solaris and Red Hat
Product Description	Oracle Application Server 10g offers full support for J2EE applications, enterprise portals, high-speed caching, business intelligence, rapid application development, application and business integration, wireless capabilities, web services, and more, all pre-integrated in a single product to save you time and money.
Product Category	Application Servers

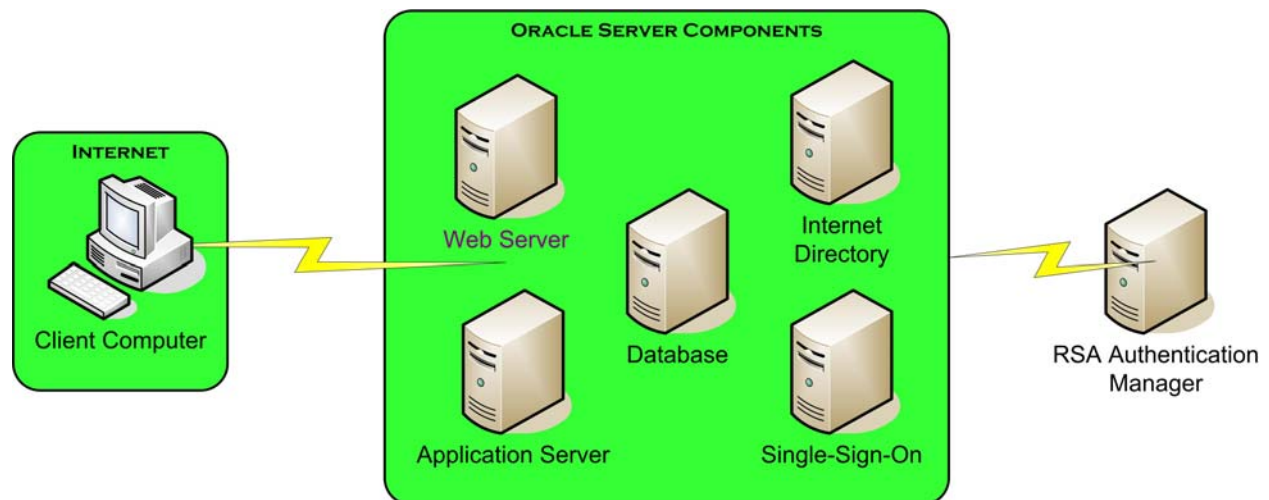




Solution Summary

To achieve Single Sign-On with Oracle 10g, the RSA Authentication Agent for the Web is installed on the Oracle infrastructure web server, and identical usernames are added to both the infrastructure and portal user repositories. The agent is then configured to protect all Oracle resources. Oracle 10g Single-Sign-On server establishes the identity of the user by using the RSA Cookie API to parse the RSA Authentication Agent Web cookie to serve personalized content. This allows strong 2-factor authentication to protect both Oracle and other third party resources, while requiring users to re-authenticate less often.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication
List Library Version Used	N/A
RSA Authentication Manager Name Locking	Yes
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	N/A
Location of Node Secret on Agent	<directory selected by used at install> default :/var/ace
RSA Authentication Agent Host Type	UNIX
RSA SecurID User Specification	All Users
RSA SecurID Protection of Administrative Users	No
RSA Software Token and RSA SecurID 800 Automation	No
Use of Cached Domain Credentials	No





Product Requirements

Partner Product Requirements: Oracle 10g Servers	
System	Please see the Oracle Documentation for system requirements.

Operating System	
Platform	Required Patches
Solaris	8,9
Red Hat	ES 3.0

Integration Module	
File	Location
ssosecuridauth.zip for Solaris	ftp://ftp.rsasecurity.com/pub/partner_engineering/SecurID/Oracle/10g/ssosecuridauth.zip
ssosecuridauth.zip for Red hat	ftp://ftp.rsasecurity.com/pub/partner_engineering/SecurID/Oracle/10g/RH/ssosecuridauth.zip

Agent Host Configuration

To facilitate communication between Oracle 10g 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 Oracle 10g 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 Oracle 10g as UNIX. This setting is used by the RSA Authentication Manager to determine how communication with Oracle 10g 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.



Partner Authentication Agent Configuration

Before You Begin

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”.

This section provides instructions for integrating Oracle 10g Single Sign-On with RSA Authentication Manager 7.1. It 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.

RSA Authentication Agent for Web Installation & Configuration

1. The RSA Authentication Agent for Apache 1.3 must be installed to protect the Oracle web servers. Prior to beginning the installation, stop all Oracle infrastructure services by running the command “runstartupconsole.sh stop all” or use enterprise manager to stop the services. Then proceed with the installation of the RSA Authentication Agent.

Important: The Installation script must be modified so that version checking passes as Oracle changed the string that is returned from the command “httpd -v”. Contact RSA Support for more information on how to do this.

2. After completing the installation, copy the jar files included in the RSA SecurID Integration Module to the <ORACLE_HOME>/j2ee/OC4J_SECURITY/applications/sso/web/WEB-INF/lib directory. If you’re using Red Hat, copy the libsacookieapi.so file to <ORACLE_HOME>/lib. See section 4 for details on obtaining this module.



3. Edit the <ORACLE_HOME>/sso/conf/policy.properties. Change the appropriate authentication plug-in to SSOSeclIDAuth.
4. Restart the Oracle infrastructure servers using “runstartupconsole.sh start all” or the enterprise manager.
5. Run config from the RSA Authentication Agent for Web installation directory. During configuration, be sure to protect the URI for the logon area of the desired areas. For example, protect the logon button for the portal server or the /pls/orasso area of the infrastructure server.

Logging on to Oracle via RSA SecurID Authentication

1. Once the resource has been protected by the web agent, users attempting to access that resource will be challenged to authenticate via RSA SecurID Authentication. For example, an Oracle user attempting to access a restricted intranet portal would see the following page.

RSA SecurID®

RSA SecurID Username Request

The page you are attempting to access requires you to authenticate using your SecurID token.
Enter your username and click **Send**.
Click **Reset** to clear the field if you make a mistake.

Username:

2. After the user successfully authenticates, they are passed on to their destination. The Oracle SSO server will then notice the agent’s cookie and use it to identify and authenticate the user. The user is then redirected to his/her destination (in this case, the personalized home page for the Oracle Portal)

Oracle Application Server
Portal Builder

Home Builder Navigator Help
Edit Customize Account Info Logout

Welcome Build Administer

Welcome ORCLADMIN to OracleAS Portal

Quick Tips
What do you want to do?
• Build pages: Click the Build tab.
• Browse portal objects: Click Navigator at the top of any page.
• Set up the portal: Click the Administer tab.

Documentation
Read the [Release Notes](#) and other helpful [documentation](#) for important information about OracleAS Portal.

New to Portal?
Getting Started with OracleAS Portal on Portal Center

Design your Portal

Add Content to your Portal

Administer your Portal

Community
portalcenter.oracle.com
Join our online community. Share portlets, tips and trick view the Portal Catalog, and get the latest version of the PDK.

Portal and the Industry
www.oracle.com/portal
Great information about OracleAS Portal: Events, customer stories, analyst reviews and much more...



Certification Checklist for RSA Authentication Manager 6.x

Date Tested: April 12, 2006

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1	Windows 2003
RSA Authentication Agent	5.2	Red Hat 3.0 ES Update 4
Oracle 10g	10g (10.1.2.0.2)	Red Hat 3.0 ES Update 4

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
Domain Credential Functionality			
Determine Cached Credential State	<input type="checkbox"/> N/A	Determine Cached Credential State	<input type="checkbox"/>
Set Domain Credential	<input type="checkbox"/> N/A	Set Domain Credential	<input type="checkbox"/>
Retrieve Domain Credential	<input type="checkbox"/> N/A	Retrieve Domain Credential	<input type="checkbox"/>

SWA

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



Certification Checklist for RSA Authentication Manager 7.x

Date Tested: March 27, 2008

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	7.1	Windows 2003 Server R2
RSA Authentication Agent	5.2	Red Hat 3.0 ES Update 4
Oracle 10g	10g (10.1.2.0.2)	Red Hat 3.0 ES Update 4

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 Expiration	<input checked="" type="checkbox"/>	PIN Expiration	<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
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
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

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