Oracle Corporation
Oracle Net Advanced Security Option

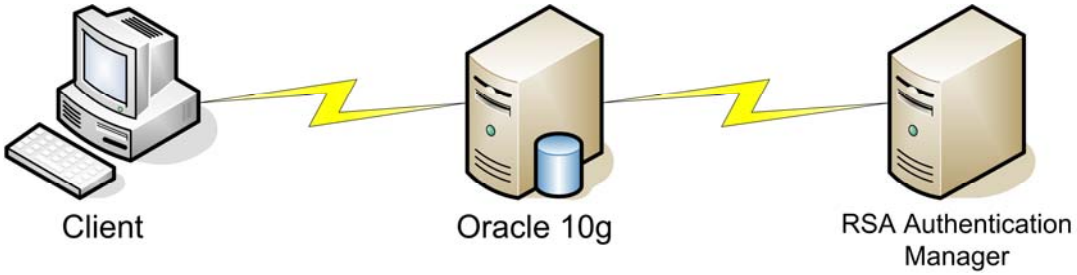
RSA SecurID Ready Implementation Guide

Last Modified: May 14, 2009

Partner Information

Product Information	
Partner Name	Oracle Corporation
Web Site	www.oracle.com
Product Name	Oracle Net Advanced Security Option
Version & Platform	11g
Product Description	Oracle Net's Advanced Security Option provides enhanced security and authentication to the Oracle Net network, as well as integration with a distributed computing environment.
Product Category	Network and Communication

Solution Summary



Oracle Net Advanced Security Option allows for more secure authentication of Oracle clients. Advanced Security Option is configured for the RADIUS protocol in order to achieve interoperability with RSA Authentication Manager. Once configured, the Oracle server will forward login requests to the RSA Authentication Manager as RADIUS requests. The RSA Authentication Manager's built in RADIUS server will service this request and handle the appropriate challenge, including special handling for New PIN and Next Tokencode modes. This configuration enables secure, two-factor authentication for both users and administrators of the Oracle product.

Partner Integration Overview	
Authentication Methods Supported	RADIUS
List Library Version Used	N/A
RSA Authentication Manager Replica Support *	No
Secondary RADIUS Server Support	Yes
RSA Authentication Agent Host Type	Net OS
RSA SecurID User Specification	All Users
RSA SecurID Protection of Administrative Users	Yes
RSA Software Token and RSA SecurID 800 Automation	No

Product Requirements

Oracle 11g Requirements:

Hardware and software requirements for this implementation depend upon the specific Oracle product installed. The full list of these requirements is beyond the scope of this document. For specific hardware requirements, and supported operating systems for your installation, please refer to your Oracle documentation, or ask your Oracle consultant.

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 Oracle Advanced Security 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 Oracle RADIUS Server within its database and contains information about communication and encryption.

To create the Agent Host/RADIUS Client records, you will need the following information.

- Oracle RADIUS server hostname
- IP Addresses for all network interfaces
- RADIUS Secret (When using RADIUS Authentication Protocol)

Add a RADIUS Client from the **RADIUS -> RADIUS Clients** menu, and RSA Authentication Manager will add a corresponding Agent Host record. When adding the Agent Host record, you should configure Oracle as a *Net OS* agent. This setting is used by the RSA Authentication Manager to determine how communication with the RADIUS server will occur. For more information about managing Agent Host records, please see the appropriate RSA Security documentation.

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

Partner Product Configuration

Before You Begin

This section provides instructions for enabling RSA SecurID authenticaiton for Oracle Advanced Security. 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 products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Prerequisites

Please ensure that the following prerequisites have been met before you begin the Oracle Advanced Security Options configuration.

Authentication Manager Prerequisites

1. Install an RSA Authentication Agent on the Oracle Client's host.
2. Create a **RADIUS Client** in the RSA Authentication Manager Security Console application. RSA Authenticaiton Manager will create a corresponding Agent Host Record and automatically link it to the new RADIUS Client. Use the following values:

   RADIUS Client/ Agent Host Record:

   - Enter the Oracle client's fully-qualified hostname in the **Client Name** field.
   - Enter the Oracle client's IP address in the **IP Address** field.
   - Enter a string - 16 characters or less – in the **Shared Secret** field. You'll need to copy or remember this string and save it in a file on the Oracle Client.

Note: The hostname and IP address each must resolve to the other. Please reference the RSA Authentication Manager documentation for detailed information on this and other configuration parameters within this screen. You can also select the Help button at the bottom of the screen for more information.

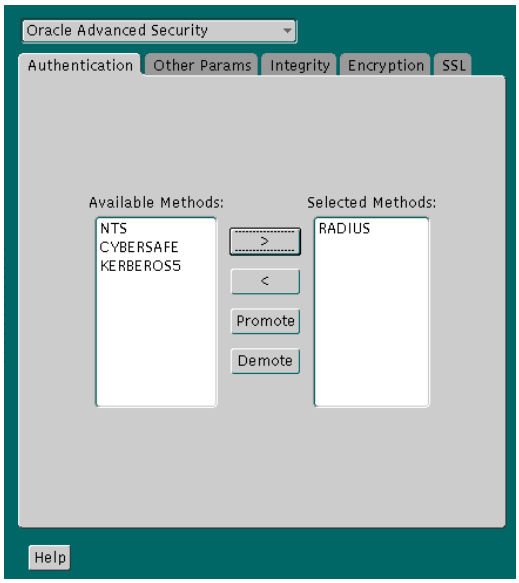
Oracle Server Configuration

Create the RADIUS Secret Key File on the Oracle Server

1. Create a **network\security** directory under the Oracle server's Oracle home directory if it does not already exist.
2. Paste or type the shared secret (and nothing else) into a new document, and save the document as "*radius.key*" in the **network\security** directory.*

Configure RADIUS on the Oracle Client

1. Start Oracle Net Manager. On UNIX, run **$ORACLE_HOME\bin\netmgr**. On Windows, choose **Start → Programs → *Oracle Product* → *Oracle Home* → Configuration and Migration Tools → Net Manager**.
2. In the navigator window, expand the **Local** branch and select "*Profile*".
3. From the drop-down list box in the right pane, select "*Oracle Advanced Security*".

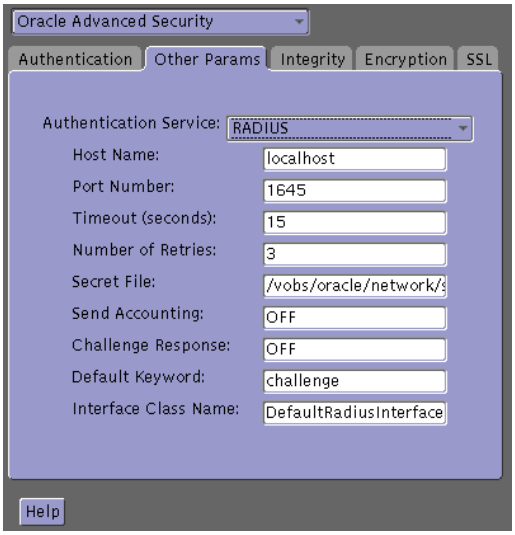


4. From the **Available Methods** list in the **Authentication** tab, select "*RADIUS*" and click the right arrow to move it to the **Selected Methods** list. If you have more than one security method in the list, you can change their respective priorities with the **Promote** and **Demote** buttons.
5. Choose **File → Save Network Configuration**.

---

* For security purposes, change the file permission of **radius.key** to read-only and make it accessible only by the Oracle owner.

6. Select the **Other Params** tab.



7. Select "*RADIUS*" from the **Authentication Service** dropdown list and enter the following data:

Field	Value
Host Name	Primary RADIUS server's host name or IP address
Port Number	Primary RADIUS server's port number
Secret File	Point to radius.key file location
Challenge Response	Set to 'ON'
Default Keyword	Accept default, or enter a keyword to request a challenge
Interface Class Name	Accept default, or enter your custom challenge-response class

8. Choose **File → Save Network Configuration** to save your changes.

Once these changes have been saved, your sqlnet.ora file should include lines which resemble the following:

```
SQLNET.AUTHENTICATION_SERVICES=RADIUS
SQLNET.RADIUS_AUTHENTICATION=radiusServerNam
eOrAddress
```

Create a User & Test Configuration

In order to use RADIUS authentication, users must be identified in the Oracle database for external authentication. For full instructions on how to accomplish this, refer to the Oracle documentation. As an example, using SQL*Plus, this process should resemble:

```
SQL> connect system/manager@dbname;
SQL> create user bob identified externally;
SQL> grant create session to user bob;
```

You may also need to modify the database initialization parameters. These are read from **$ORACLE_BASE/admin/*db_name*/pfile**. The specific parameters are:

```
REMOTE_OS_AUTHENT=FALSE
OS_AUTHENT_PREFIX=""
```

Important: Setting REMOTE_OS_AUTHENT to "TRUE" will allow remote users to access the system over non-secure protocols using operating system authentication rather than SecurID. See the Oracle Database Administrator's guide for more information.

If these parameters are changed, the database will need to be restarted.

Certification Checklist For RSA Authentication Manager v6.x

Date Tested:12/08/2008

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	6.1	Windows 2003 Server
Oracle Database Server 11g	11g	Windows 2003 Server

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	N/A	Force Authentication After New PIN	✓
System Generated PIN	N/A	System Generated PIN	✓
User Defined (4-8 Alphanumeric)	N/A	User Defined (4-8 Alphanumeric)	✓
User Defined (5-7 Numeric)	N/A	User Defined (5-7 Numeric)	✓
User Selectable	N/A	User Selectable	✓
Deny 4 and 8 Digit PIN	N/A	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	N/A	Deny Alphanumeric PIN	✓
Passcode			
16 Digit Passcode	N/A	16 Digit Passcode	✓
4 Digit Password	N/A	4 Digit Password	✓
Next Tokencode Mode			
Next Tokencode Mode	N/A	Next Tokencode Mode	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	Failover	✓
Name Locking Enabled	N/A	Name Locking Enabled	
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓

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	

INIT / PAR

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

Certification Checklist For RSA Authentication Manager 7.1

Date Tested: 05/18/2009

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1	Windows 2003 Server
Oracle Database Server 11g	11g	Windows 2003 Server

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	N/A	Force Authentication After New PIN	✓
System Generated PIN	N/A	System Generated PIN	✓
User Defined (4-8 Alphanumeric)	N/A	User Defined (4-8 Alphanumeric)	✓
User Defined (5-7 Numeric)	N/A	User Defined (5-7 Numeric)	✓
Deny 4 and 8 Digit PIN	N/A	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	N/A	Deny Alphanumeric PIN	✓
Deny Numeric PIN	N/A	Deny Numeric PIN	✓
PIN Reuse	N/A	PIN Reuse	✓
Passcode			
16 Digit Passcode	N/A	16 Digit Passcode	✓
4 Digit Fixed Passcode	N/A	4 Digit Fixed Passcode	✓
Next Tokencode Mode			
Next Tokencode Mode	N/A	Next Tokencode Mode	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	Failover	✓
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓

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

JGS

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