



RSA SecurID Ready Implementation Guide

Last Modified: September 29, 2004

1. Partner Information

Partner Name	Oracle Corporation
Web Site	www.oracle.com
Product Name	Oracle Net – Advanced Security Option
Version & Platform	10g (9.0.4.0.0)
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 Communications

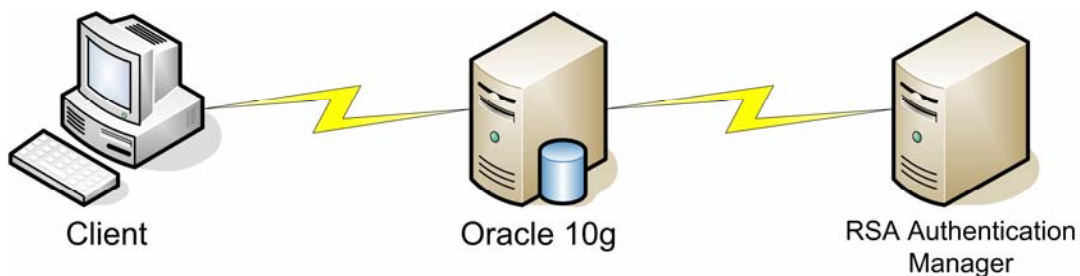


2. Contact Information

	Sales Contact	Support Contact
Phone	800-ORACLE1	800-223-1711
Web	www.oracle.com	www.oracle.com

3. Solution Summary

Feature	Details
Authentication Methods Supported	RADIUS
RSA Authentication Agent Library Version	N/A
RSA Authentication Manager Name Locking	No
RSA Authentication Manager Replica Support	No
Secondary RADIUS Server Support	Yes (1 backup supported)
Location of Node Secret on Client	None Stored
RSA Authentication Agent Host Type	Net OS
RSA SecurID User Specification	All Users
Support for Download of Offline Day Files	No
RSA SecurID Protection of Partner Product Administrators	Yes
RSA Software Token API Integration	No



The Oracle Net's Advanced Security Option allows for more secure authentication of Oracle clients. For this integration, the Advanced Security Option is configured for the RADIUS protocol. In this case, 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.

4. Product 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.

5. RSA Authentication Manager configuration

Perform the following steps to set up the Oracle client as an agent host within the RSA Authentication Manager's database.

- On the RSA Authentication Manager computer, go to **Start > Programs > RSA ACE Server**, and then **Database Administration - Host Mode**.
1. On the **Agent Host** menu, choose **Add Agent Host....**

The screenshot shows the 'Add Agent Host' dialog box with the following configuration:

- Name: ps057.pe.rsa.net
- Network address: 10.100.50.57
- Site: (empty)
- Agent type: Net OS Agent
- Encryption Type: DES
- Open to All Locally Known Users: checked
- Requires Name Lock: unchecked
- Enable Windows Password Integration: unchecked

- In **Name**, type the hostname of the Oracle client.
- In **Network address**, type the IP address of the Oracle client.
- For **Agent Type**, select Net OS.
- Under **Secondary Nodes**, define all other hostname/IP addresses that resolve to the Oracle client, if needed.
- Under **Assign/Change Encryption Key...**, enter the encryption key. This must match the encryption key you enter on the Oracle client. This should be 16 characters or less, see [known issue number one](#).
- Uncheck the **Requires Name Lock**, **Enable Offline Authentication**, **Enable Windows Password Integration**, and **Create Verifiable Authentications** options.

Note: It is important that all hostname and IP addresses resolve to each 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.

6. Partner RSA Authentication Agent configuration

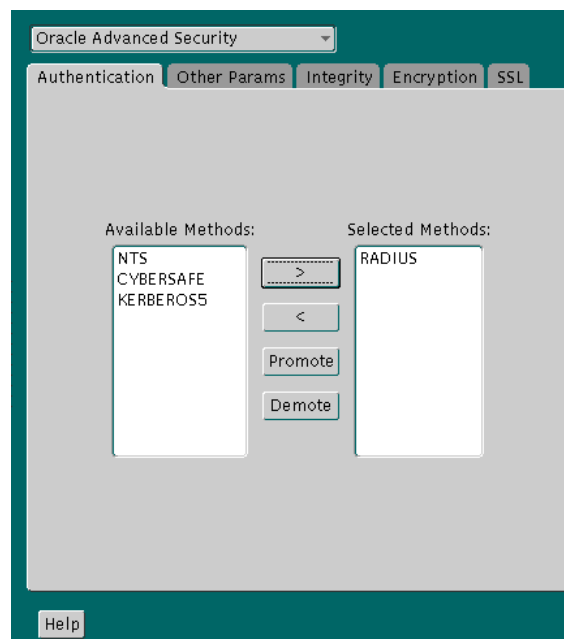
This section provides instructions for integrating the partners' product with RSA SecurID. This document is not intended to suggest optimum installations or configurations. It is assumed that the reader has both working knowledge of the two products to perform the tasks outlined in this section and access to the documentation for both in order to install the required software components. All products/components need to be installed and working prior to this integration. Perform the necessary tests to confirm that this is true before proceeding.

Create the RADIUS Secret Key File on the Oracle Server

1. Obtain the RADIUS shared secret key from the RSA Authentication Manager. In the **Edit Agent Host** dialog, select **Assign/Change Encryption Key...**, then either create or copy the value. For this integration, this shared secret must be exactly sixteen characters. See [known issues number one](#) for more details.
2. On the Oracle server, create a **network\security** directory under the Oracle home directory, if it does not already exist.
3. Create the file **radius.key** to hold the shared secret from the RADIUS server. Enter the shared secret, and only the shared secret, into the file, and save it in the **security** directory previously created.
4. For security purposes, change the file permission of **radius.key** to read-only, and make it accessible only by the Oracle owner, since Oracle relies on the file system to keep this file secret.

Configure RADIUS on the Oracle Client

1. First, start Oracle Net Manager. On UNIX, run **\$ORACLE_HOME/bin/netmgr**. On Windows, choose **Start → Programs → Oracle Product → Oracle Home → Configuration and Migration Tools → Oracle 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**; the tab control changes to reflect the advanced security options.



- From the **Available Methods** list in the **Authentication** tab, select **RADIUS**, and click the right arrow to move RADIUS to the **Selected Methods** list.
- If RADIUS should be the first service used, move it to the top of the selected methods.
- Then, choose **File → Save Network Configuration** to save your changes.
- Select the **Other Params** tab.

The screenshot shows the 'Oracle Advanced Security' configuration window with the 'Other Params' tab selected. The 'Authentication Service' is set to 'RADIUS'. The following fields are visible:

- Host Name: localhost
- Port Number: 1645
- Timeout (seconds): 15
- Number of Retries: 3
- Secret File: /vobs/oracle/network/s
- Send Accounting: OFF
- Challenge Response: OFF
- Default Keyword: challenge
- Interface Class Name: DefaultRadiusInterface

- From the **Authentication Service** drop-down list, select **RADIUS**, and complete the fields.

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

- Again, choose **File → Save Network Configuration** to save your changes.

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

```
SQLNET.AUTHENTICATION_SERVICES=RADIUS
SQLNET.RADIUS_AUTHENTICATION=radiusServerNameOrAddress
```

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:

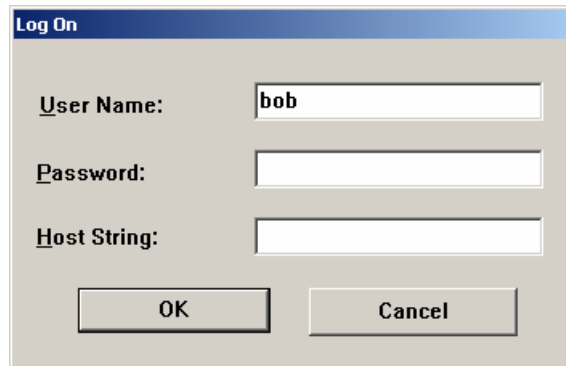
```
SQL> connect system/manager@dbname;
SQL> create user bob identified externally;
SQL> grant create session to user bob;
```

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

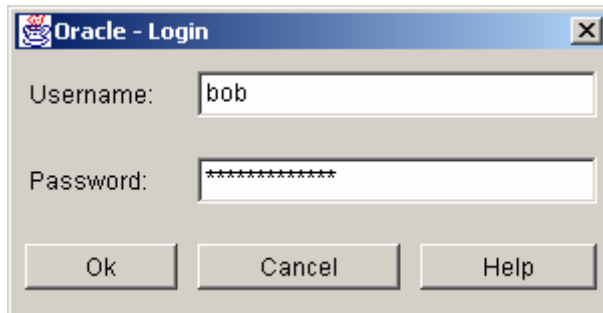
```
REMOTE_OS_AUTHENT=FALSE  
OS_AUTHENT_PREFIX=" "
```

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

In order to test the configuration, start SQL*Plus. When prompted to authenticate at the Oracle prompt, enter your username and password, and click **OK**. Note that some text is required in the password field for the dialog to be submitted, but it's not clear that this text is used for anything.



Once that dialog is submitted, the RADIUS challenge will be issued, and the user will be prompted by Oracle's RADIUS authentication dialog:



In this dialog, the user should enter their PASSCODE in the **Password** field. If the token is in a special mode, such as New PIN or Next Tokencode, the user may be prompted additional times for the necessary information.

7. Certification Checklist

Date Tested: September 15, 2004

Tested Certification Environment		
Product	Platform (OS)	Product Version
RSA Authentication Manager	Windows Server 2003, Enterprise	6.0
RSA Software Token	Windows Server 2003, Enterprise	3.0.3
Oracle Application Server	Windows Server 2003, Enterprise	10g (9.0.4.0.0)

Test	RSA Native Protocol	RADIUS Protocol
1st time auth. (node secret creation)	N/A	
New PIN mode:		
System-generated		
Non-PINPAD token	N/A	Pass
PINPAD token	N/A	Pass
User-defined (4-8 alphanumeric)		
Non-PINPAD token	N/A	Pass
Password	N/A	Pass
User-defined (5-7 numeric)		
Non-PINPAD token	N/A	Pass
PINPAD token	N/A	Pass
Software token	N/A	Pass
Deny 4 digit PIN	N/A	Pass
Deny Alphanumeric	N/A	Pass
User-selectable		
Non-PINPAD token	N/A	Pass
PINPAD token	N/A	Pass
PASSCODE		
16 Digit PASSCODE	N/A	Pass
4 Digit Password	N/A	Pass
"Pin-less" TokenCode	N/A	Pass
Next Tokencode mode		
Non-PINPAD token	N/A	Pass
PINPAD token	N/A	Pass
Software Token API Authentication		
New PIN mode	N/A	N/A
8 Digit PIN with 8 Digit TokenCode	N/A	N/A
Failover	N/A	Pass
User Lock Test (RSA Name Lock Function)	N/A	
No RSA Authentication Manager	N/A	Pass

ATB

Pass, Fail or N/A (N/A=Non-available function)



8. Known Issues

1. Oracle Net will silently truncate your RADIUS shared secret to 16 characters. Be sure to use only a 16 character shared secret, or you will not be able to authenticate with RSA Authentication Manager. This will show up in RSA Authentication Manager logs as “ACCESS DENIED – Syntax Error”.