Oracle
Secure Global Desktop

RSA SecurID Ready Implementation Guide

Last Modified: December 9th, 2014

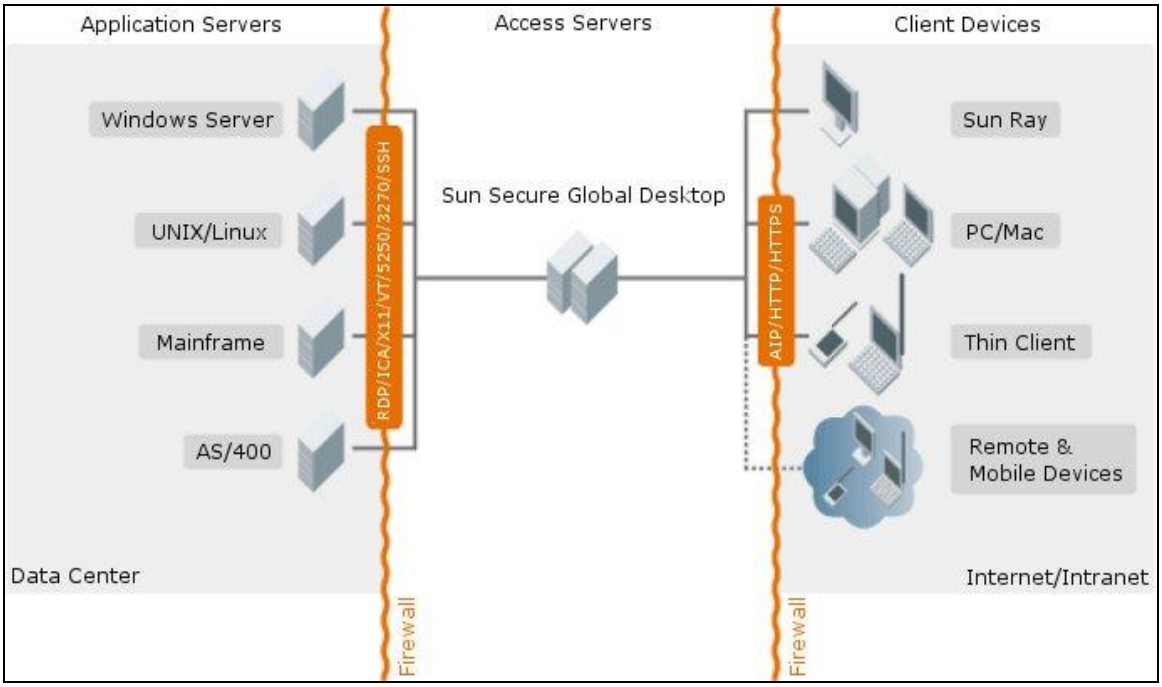
Partner Information

Product Information	
Partner Name	Oracle
Web Site	www.oracle.com
Product Name	Secure Global Desktop
Version & Platform	5.1
Product Description	Oracle Secure Global Desktop provides secure access to centralized, server-hosted Windows, UNIX, mainframe, and midrange applications from a wide variety of popular client devices, including Windows PCs, Mac OS X systems, Oracle Solaris workstations, Linux PCs, thin clients, and more. Additionally, Oracle Secure Global Desktop provides access to full-screen desktop environments, allowing administrators the freedom to use a single solution to provide access to both server-based applications and server-hosted desktop environments such as Microsoft Remote Desktop Services.

Solution Summary

SecurID authentication enables users with RSA SecurID tokens to log in to Secure Global Desktop. Secure Global Desktop authenticates users against an RSA Authentication Manager.

RSA Authentication Manager supported features	
Oracle Secure Global Desktop	
RSA SecurID Authentication via Native RSA SecurID UDP Protocol	Yes
RSA SecurID Authentication via Native RSA SecurID TCP Protocol	No
RSA SecurID Authentication via RADIUS Protocol	No
RSA SecurID Authentication via IPv6	No
On-Demand Authentication via Native SecurID UDP Protocol	Yes
On-Demand Authentication via Native SecurID TCP Protocol	No
On-Demand Authentication via RADIUS Protocol	No
Risk-Based Authentication	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



Agent Host Configuration

To facilitate communication between the Secure Global Desktop system 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 Secure Global Desktop system and contains information about communication and encryption.

RSA Authentication Manager 8.0 introduced a new TCP-based authentication protocol and corresponding agent API. RSA Authentication Manager 8.0 and newer also maintains support for the existing UDP-based authentication protocol and agents. The agent host records for TCP and UDP agents are configured similarly, but there are some important differences.

Include the following information when configuring a UDP-based agent host record.

- Hostname
- IP addresses for network interfaces

> **Note: The UDP-based authentication agent's hostname must resolve to the IP address specified.**

Include the following information when configuring a TCP-based agent host record.

- RSA agent name (in the hostname field)

> **Note: The RSA agent name is specified in the rsa_api.properties file.**

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 the Secure Global Desktop system will occur.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Secure Global Desktop system 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 Secure Global Desktop components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configure Oracle Secure Global Desktop for SecurID Authentication

Complete the following steps to enable RSA SecurID authentication on Oracle Secure Global Desktop.

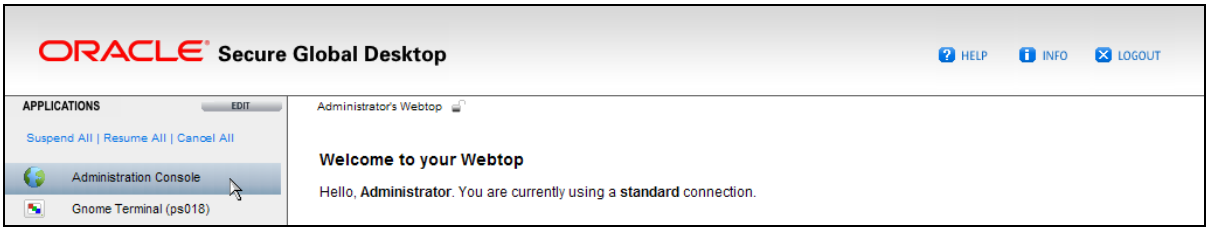
1. On the Oracle Secure Global Desktop server, create the file `/etc/sdace.txt` that contains the following line.

```
VAR_ACE=/opt/ace/data
```

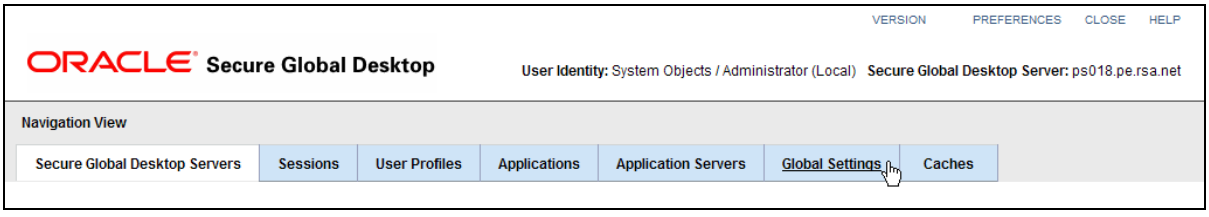
2. Create the directory `/opt/ace/data/` and copy the RSA Authentication Manager's `sdconf.rec` file to it.
3. Set the file permissions so that Oracle Secure Global Desktop can read and write the configuration files.

```
chmod 444 /etc/sdace.txt
chown -R ttasys:ttaserv /opt/ace
chmod -R 775 /opt/ace
```

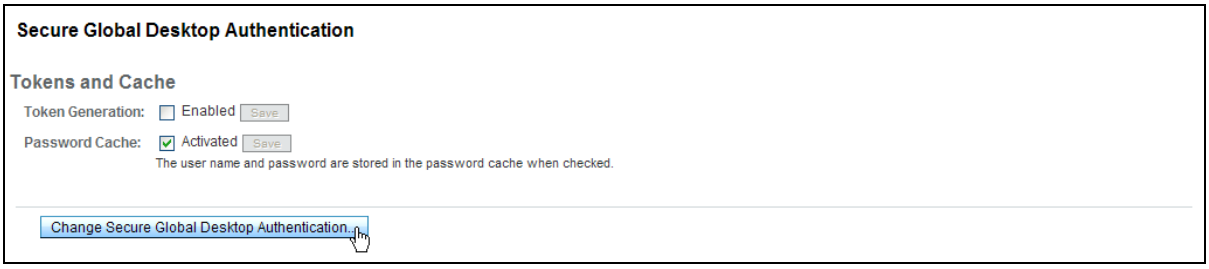
4. Log in to Oracle Secure Global Desktop and launch the **Administration Console** from the Applications list.



5. Click **Global Settings** from the Navigation View menu.

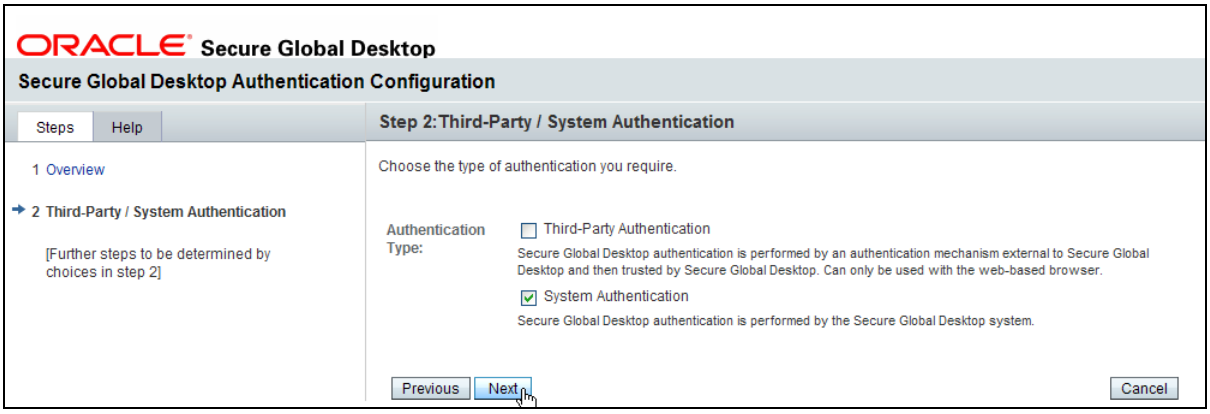


6. Click the **Change Secure Global Desktop Authentication** link.

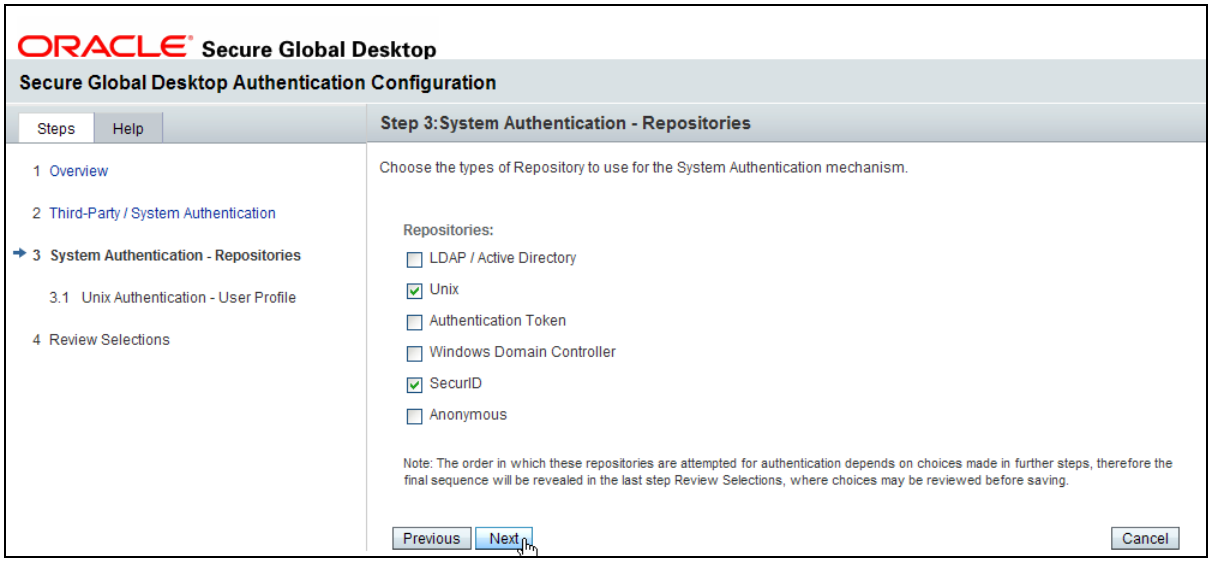


7. Click **Next**.

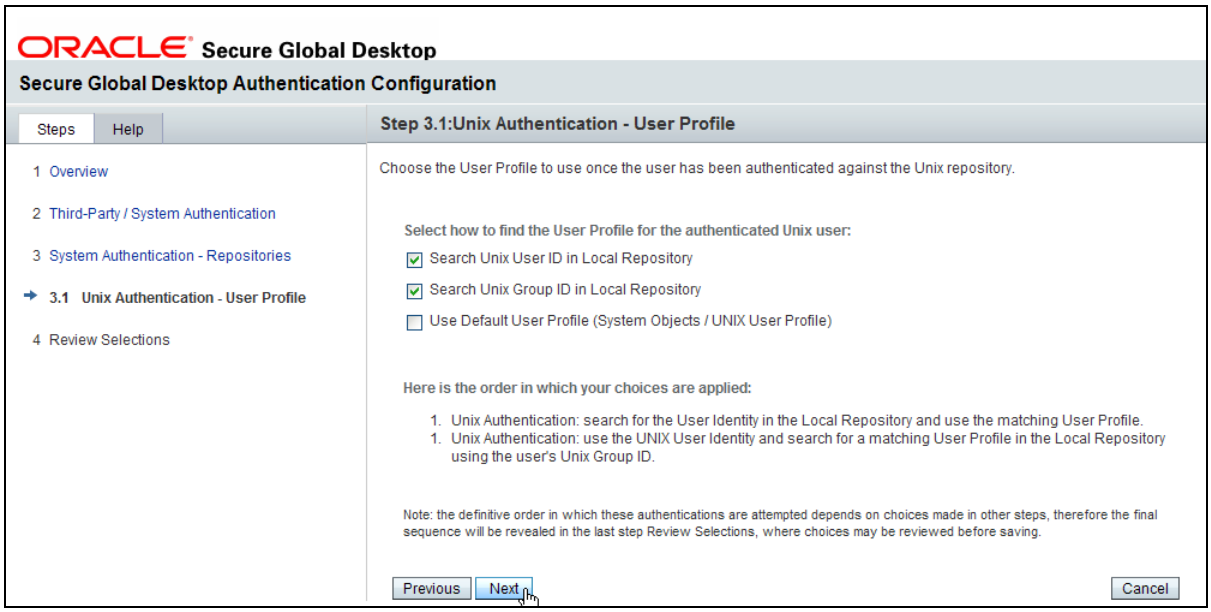
8. Click **Next**.



9. Mark the checkbox for **SecurID** from the System Authentication mechanism checklist and click **Next**.



10. Click **Next**.

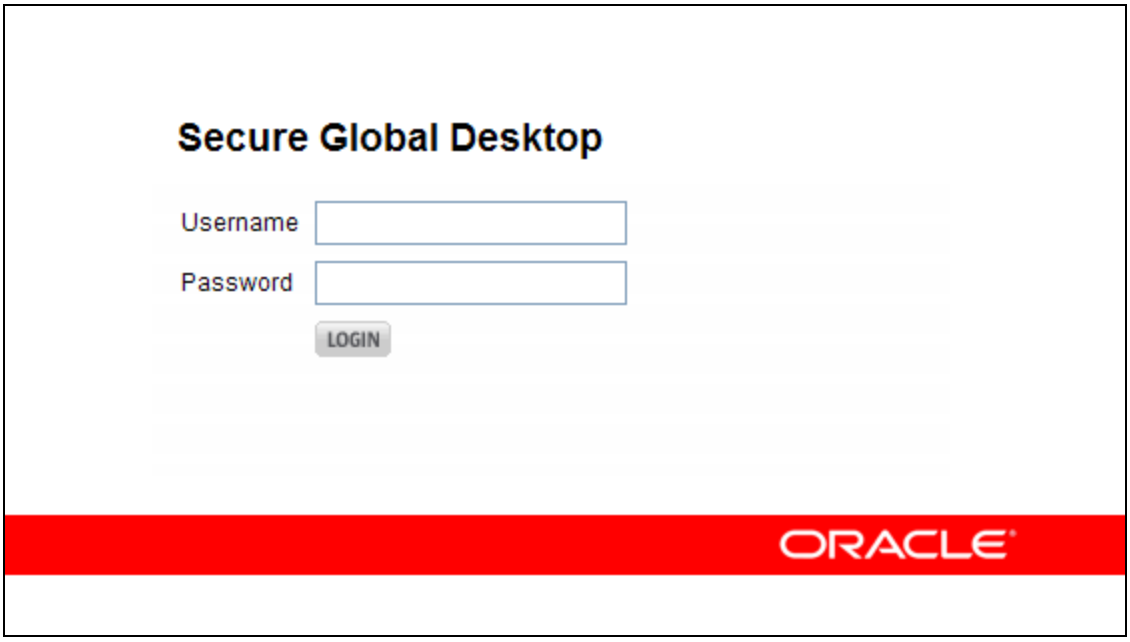


11. Click **Finish**.

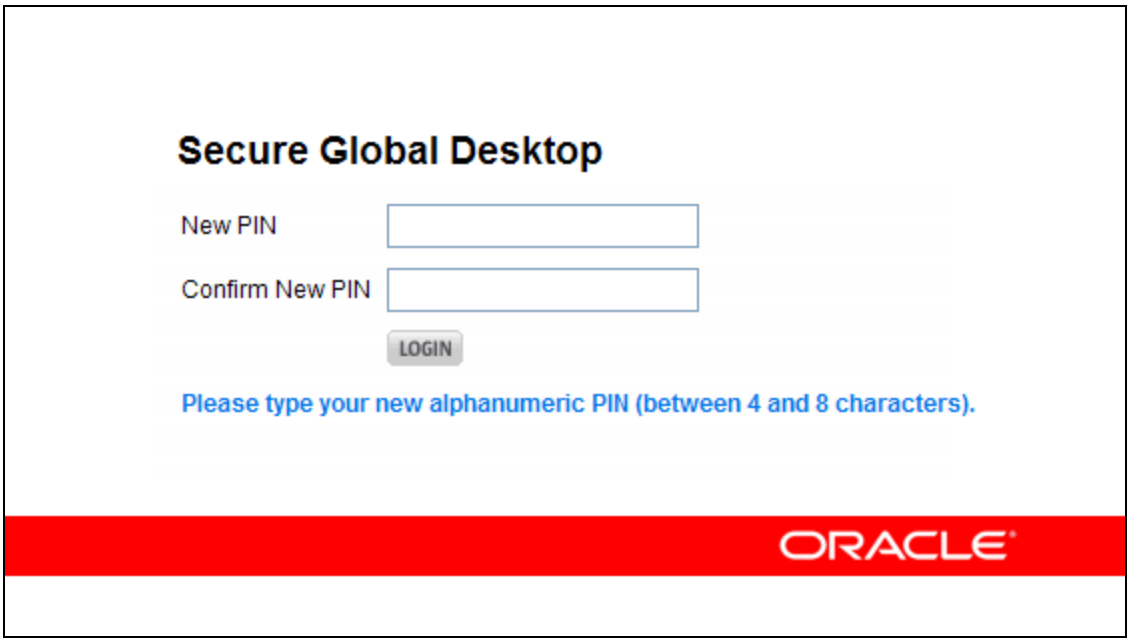
12. Reboot the Oracle Secure Global Desktop system to complete the configuration.

RSA SecurID Login Screens

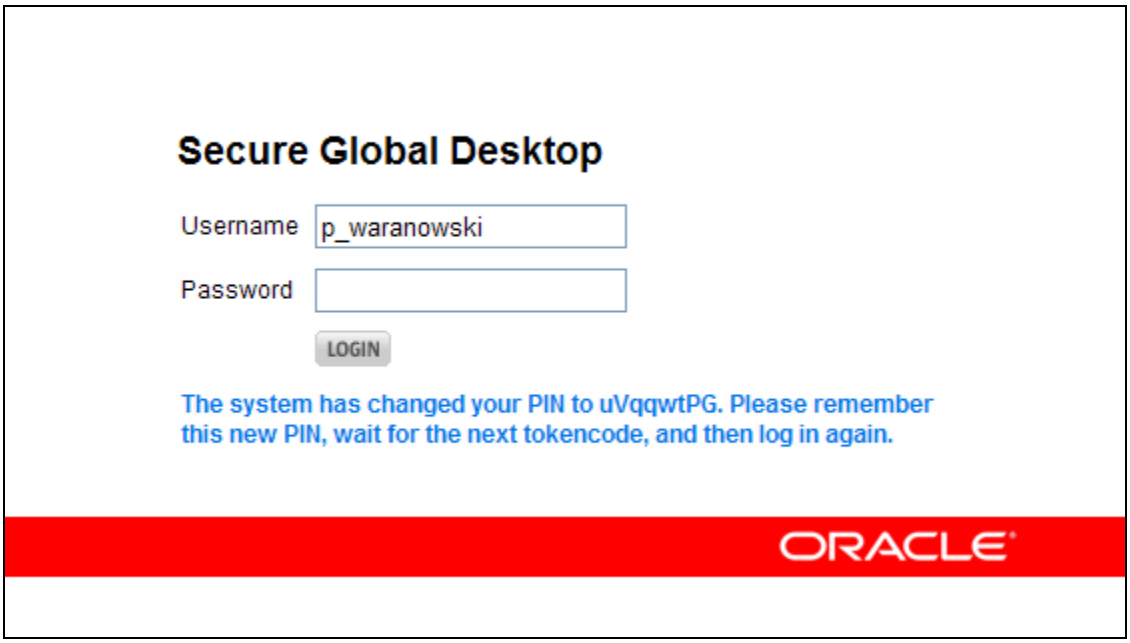
Login screen:



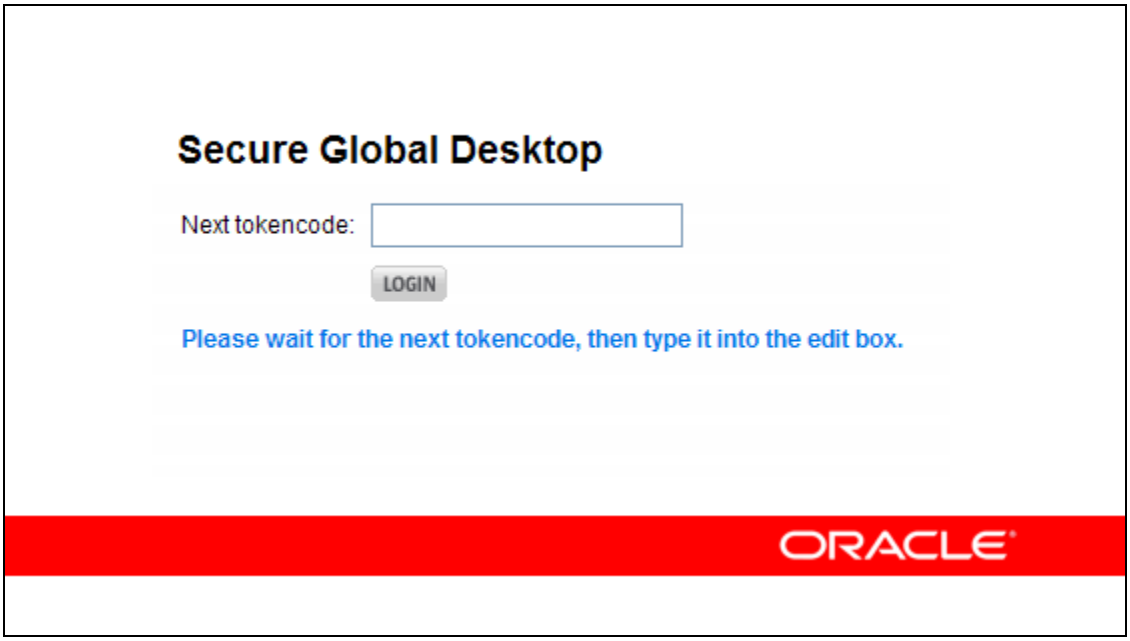
User-defined New PIN:



System-generated New PIN:



Next Tokencode:



Certification Test Checklist for RSA Authentication Manager

Certification Environment

Product Name	Version Information	Operating System
RSA Authentication Manager	8.1	Virtual Appliance
Oracle Secure Global Desktop	5.1	Solaris 11.6 x86_64

RSA SecurID Authentication

Date Tested: December 5th, 2014

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

PEW

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

Appendix

RSA SecurID Authentication Files

RSA SecurID Authentication Files	
UDP Agent Files	**Location**
sdconf.rec	/opt/ace/data/sdconf.rec
sdopts.rec	/opt/ace/data/sdopts.rec
Node secret	/opt/ace/data/securid
sdstatus.12 / jastatus.12	/opt/ace/data/sdstatus.12
TCP Agent Files	**Location**
rsa_api.properties	N/A
sdconf.rec	N/A
sdopts.rec	N/A
Node secret	N/A

Partner Integration Details

Partner Integration Details	
RSA SecurID UDP API	5.0.3.2
RSA SecurID TCP API	N/A
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	All Users
Display RSA Server Info	No
Perform Test Authentication	Yes
Agent Tracing	Yes

Node Secret:

The node secret is stored in the following file. Delete the file to reset the node secret.

```
/opt/ace/data/securid
```

sdconf.rec:

The RSA server configuration is stored in the following file. Delete or overwrite the file to update the configuration.

```
/opt/ace/data/sdconf.rec
```

sdopts.rec:

If you are using an sdopts.rec file, it needs to be located in the following directory.

```
/opt/ace/data/
```

sdstatus.12:

The RSA server list is stored in the following file.

```
/opt/ace/data/sdstatus.12
```

Agent Tracing:

Set the following global variables to enable agent tracing.

```
RSATRACELEVEL=<0-15>
RSATRACEDEST=<log file name>
```

Test Authentication:

Open a terminal and enter the following commands to perform a SecurID test authentication.

```
cd /opt/tarantella/bin/bin
./ttasecurid test
cmd=authenticate id=<userid> username=<userid> passcode=<passcode>
```