



RSA Secured Implementation Guide For Portal Servers and Web-Based Applications

Last Modified: November 29, 2006

Partner Information

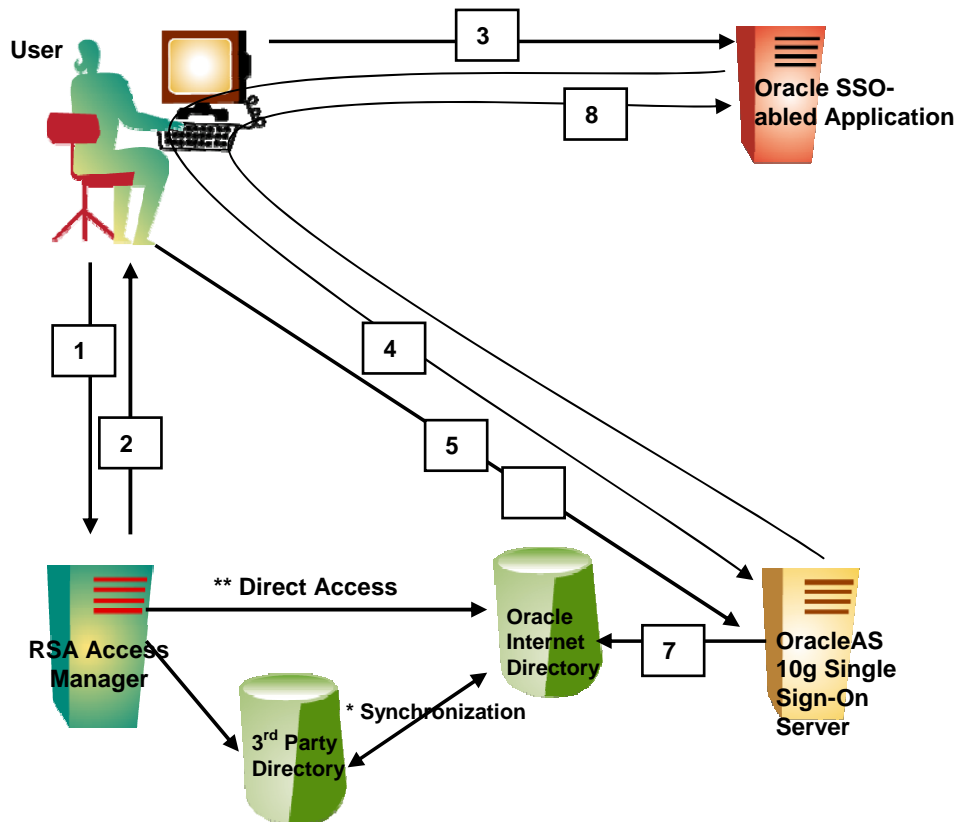
| Product Information | |
|---------------------|---|
| Partner Name | Oracle Corporation |
| Web Site | www.oracle.com |
| Product Name | Oracle 10g Application Server |
| Version & Platform | 10g (10.1.2.0.2) |
| Product Description | Oracle Application Server 10g offers full support for J2EE, enterprise 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 |

ORACLE

Solution Summary

To achieve Single-Sign-On with the Oracle 10g Portal Server, the RSA ClearTrust Apache Agent is installed on the Oracle infrastructure Web Server, and identical usernames are added to both products' repositories. The Agent is then configured to protect all portal-related pages. Oracle 10g Portal Server establishes the identity of the user by parsing the HTTP Headers and using the CT_REMOTE_USER variable to serve personalized content.

| Partner Integration Overview | |
|--|--|
| Use UserID for SSO | Yes |
| Use UserID for Personalization | Yes |
| Recognize Authentication Type | No |
| API-level Authorization Support (RuntimeAPI) | No |
| User Management (AdminAPI) | Yes Via Shared User Repository. See Oracle Internet Directory 10g Implementation guide for more details. |



Product Requirements

| Partner Product Requirements: Oracle 10g Portal Server | |
|--|------------------|
| Operating System | |
| Platform | Required Patches |
| Solaris | |
| Red Hat Linux | |

The integration requires an RSA ClearTrust Agent installed on the Oracle http web server which is currently Apache 1.3

Note: There are many different configuration options for Oracle 10g and thus many different requirements based on the options chosen. Please see the Oracle documentation for more detailed information on the requirements based on the Oracle environment chosen.

| Additional Software Requirements | |
|----------------------------------|--------------------|
| Application | Additional Patches |
| OracleAS | 10g |
| OracleAS Single-Sign-On | 10g |
| OracleAS Portal | 10g |
| Oracle Internet Directory | 10g |
| Oracle 10g Database | 10g |

| Integration Modules | |
|---------------------|---|
| File Name | Destination |
| SSOCTAuth.jar | ftp.rsasecurity.com/pub/partner_engineering/AccessManager/Oracle/10g |

Product Configuration

Before You Begin

This section provides instructions for integrating the partners' product with RSA Access Manager. 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.

Installation Prerequisites

- Your RSA Access Manager infrastructure is properly installed and configured, and your web server agents are properly protecting web resources.
- Oracle 10g Portal is properly installed and configured, and users can successfully login via username and password to access their home page.

The integration requires an RSA ClearTrust Agent installed on the Oracle http web server which is currently Apache 1.3

Configuring OracleAS 10g Single-Sign-On

1. Stop the Oracle infrastructure services by running `opmnctl stopall`. Then install the RSA ClearTrust Apache Agent on the Oracle infrastructure web server and select the `modssl` version during the installation. For information regarding this installation, see the RSA Access Manager documentation.
2. Edit the `httpd.conf` file for the Oracle infrastructure web server located in the `<ORACLE_HOME>/Apache/Apache/conf` directory and move all the RSA ClearTrust configuration lines so they are located after the configuration line: `"include <ORACLE_HOME>/Apache/Apache/conf/oracle_apache.conf"`. This line is at the end of the file. Add one `</Directory>` directive and two `<Location>` directives. Then comment out two `<Directory>` directives so that your configuration looks similar to the example below.

```
include "/opt/oracle/infra/Apache/Apache/conf/oracle_apache.conf"
# moved Access Manager configuration lines.
LoadModule ct_auth_module /opt2/Apache/Apache/libexec/libct_apache_agent_mod_ssl.so
AddModule ct_apache_mod.c

<IfModule ct_apache_mod.c>
    CTAgentRoot /opt2/ctrust5/agent/apache
</IfModule>

<IfModule ct_apache_mod.c>
    <Location />                                     (Add)
        AuthType Basic
        Require valid-user
        AuthName CT
    </Location>                                       (Add)
</IfModule>

<IfModule ct_apache_mod.c>
    Alias /Access Manager/ "/opt2/ctrust5/agent/apache/htdocs/"
    <Directory "/opt2/ctrust5/agent/apache/htdocs">
        AuthType Basic
        Require valid-user
        AuthName CT
    </Directory>
</IfModule>
```

3. Copy SSOCTAuth.jar to <ORACLE_HOME>/j2ee/OC4J_SECURITY/applications/sso/web/WEB-INF/lib. See Section 5, Product Requirements on how to obtain this file.
4. Edit <ORACLE_HOME>/sso/conf/policy.properties. Change the appropriate Authentication plugin to correspond to the SSOCTAuth plugin.

```
#####
# Default tAuthLevel
# -----
# Default tAuthLevel entry must have a value assigned.

Default tAuthLevel = MediumSecurity

#####
# Authentication plugins
# -----
# Assign a class name that implements SSOServerAuthInterface
# for each auth level referenced.
#
# The Authentication level name must be appended with
# "_AuthPlugin" keyword.

#MediumSecurity_AuthPlugin = oracle.security.sso.server.auth.SSOServerAuth
#MediumSecurity_AuthPlugin = oracle.security.sso.server.auth.SSOCTAuth
```

5. Restart the Oracle infrastructure services.
6. Using the RSA Access Manager administration program, protect the logon button URI for the portal server or the <hostname>:7777/pls/orasso/* area of the infrastructure web server. See the RSA Access Manager documentation for more information on how to do this.

Once the RSA ClearTrust Apache Agent has been installed and configured, and the logon button has been added as a protected URI in the Entitlements Manager, users will be prompted to authenticate via RSA Access Manager when they click the logon button.

Configuring RSA Access Manager

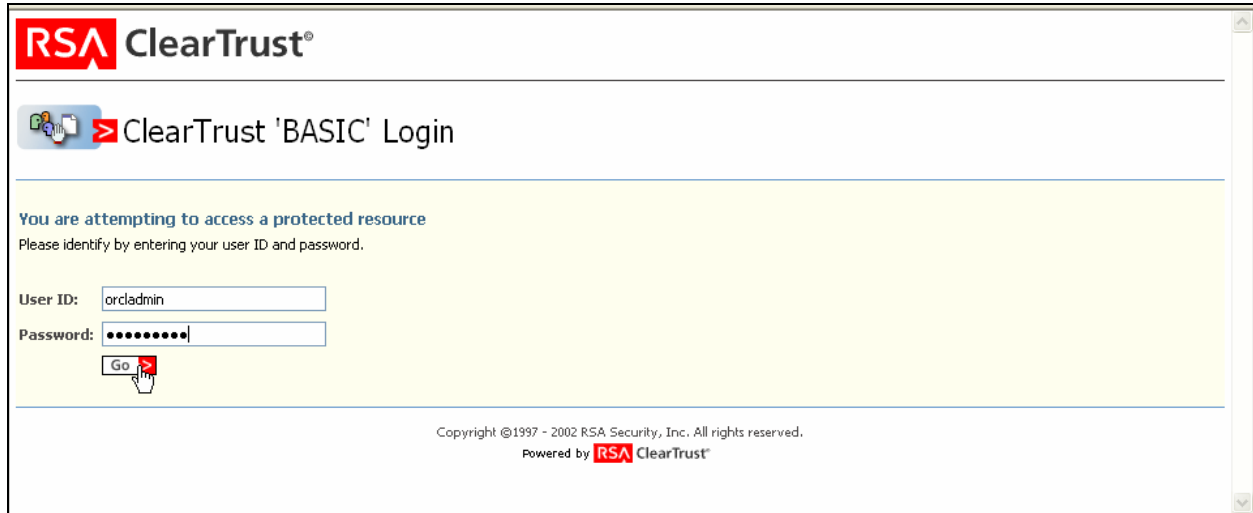
To achieve single-sign on compatibility between the RSA ClearTrust 3.5 and the RSA Access Manager 4.7 agents a configuration change must be made to the Access Manager 6.0 server.

1. Edit the *aserver.conf* file located for a default installation at *C:\Program Files\RSA\ClearTrust Servers 6.0\conf* to add the following line of configuration:

```
cleartrust.aserver.token_version=1
```

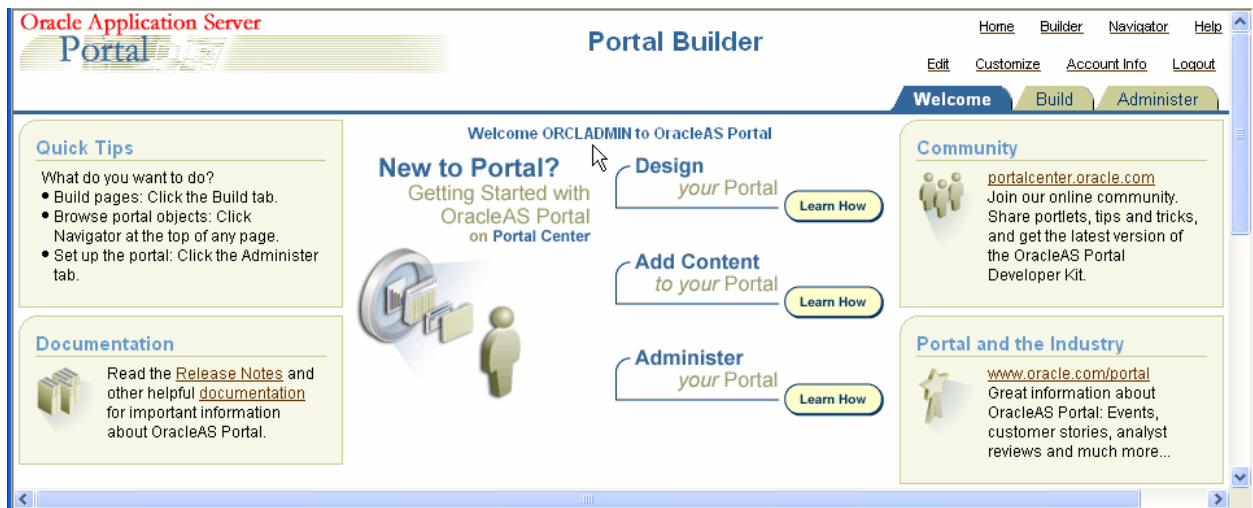
2. Restart the RSA Access Manager Authorization Server service.
3. Restart the RSA Access Manager Dispatch Server service.

End User Experience



The screenshot shows the RSA ClearTrust 'BASIC' Login page. At the top left is the RSA ClearTrust logo. Below it is a heading 'ClearTrust 'BASIC' Login' with a small icon. A yellow background area contains the text: 'You are attempting to access a protected resource. Please identify by entering your user ID and password.' There are two input fields: 'User ID:' with the text 'orcladmin' and 'Password:' with masked characters. A 'Go' button with a red arrow is below the password field. At the bottom, there is a copyright notice: 'Copyright ©1997 - 2002 RSA Security, Inc. All rights reserved. Powered by RSA ClearTrust'.

After the user authenticates, they are presented with their portal page.



The screenshot shows the Oracle Application Server Portal Builder page. The top left has the 'Oracle Application Server Portal' logo. The top right has navigation links: 'Home', 'Builder', 'Navigator', 'Help'. Below these are 'Edit', 'Customize', 'Account Info', and 'Logout'. The main content area has a 'Welcome' tab selected, with 'Build' and 'Administer' tabs also visible. The main heading is 'Welcome ORCLADMIN to OracleAS Portal'. Below this is a 'New to Portal?' section with the text 'Getting Started with OracleAS Portal on Portal Center' and an illustration of a person and a folder. To the right of this are three 'Learn How' buttons: 'Design your Portal', 'Add Content to your Portal', and 'Administer your Portal'. On the left side, there are two boxes: 'Quick Tips' with three bullet points and 'Documentation' with a link to 'Release Notes'. On the right side, there are two boxes: 'Community' with a link to 'portalcenter.oracle.com' and 'Portal and the Industry' with a link to 'www.oracle.com/portal'.

URL: http://vm3078.pe.rsa.net:7778/portal/page?_pageid=6,1,6_13&_dad=portal&_schema=PORTAL

Certification Checklist Portal Servers and Web-Based Apps

Date Tested: November 29, 2006

| Certification Environment | | |
|---------------------------------|---------------------|---|
| Product Name | Version Information | Operating System |
| RSA Access Manager | 6.0 | Windows 2003 Enterprise Server R2 |
| RSA ClearTrust Agent for Apache | 3.5.0.4 | Red Hat Enterprise Linux ES 3.0 Update4 |
| Oracle Application Server | 10g (10.1.2.0.2) | Red Hat Enterprise Linux ES 3.0 Update4 |
| | | |

| Test Case | Result |
|---|--------|
| Product Characteristics for SSO Support | |
| Application/Portal is web-based, and supports access by a standard HTTP-based browser | ✓ |
| Application/Portal runs on Web Server Platform supported by RSA Access Manager | ✓ |
| Application/Portal login interface can be modified or replaced | ✓ |
| Application/Portal can extract user information from RSA Access Manager session cookie | N/A |
| Application/Portal can extract user information from HTTP Headers | ✓ |
| Application/Portal can extract authentication type from RSA Access Manager session cookie | N/A |
| Application/Portal can extract authentication type from HTTP Headers | N/A |
| Application/Portal can perform SSO with other RSA Access Manager-supported Web Server | ✓ |
| Login - General | |
| HTTP basic authentication | ✓ |
| Forms based | ✓ |
| Forms based w/ URI retention | ✓ |
| Login – Basic Authentication | |
| Access Denied for unauthorized user | ✓ |
| Successful login for authorized user | ✓ |
| Successful recognition of identity/personalization in 3 rd Party Product | ✓ |
| Successful recognition of identity/personalization after SSO with other RSA Access Manager-supported Web Server | ✓ |
| Login –Graded Authentication | |
| Access Denied for unauthorized user | N/A |
| Successful login for authorized user | N/A |
| Successful recognition of identity/personalization in 3 rd Party Product | N/A |
| Successful recognition of identity/personalization after SSO with other RSA Access Manager-supported Web Server | N/A |

SWA

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

Known Issues

1. Out of the box the RSA ClearTrust Apache Agent 3.5 is unable to protect the /pls/orasso area on the Oracle Infrastructure Web Server. You need to change some of the RSA ClearTrust Apache Agent configuration lines in the httpd.conf file. See the Configuring OracleAS 10g Single-Sign-On section, step 2 of this guide for detailed instructions.