



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

Last Modified 08/26/2008

Partner Information

Partner Name	Oracle
Web Site	www.oracle.com/siebel/index.html
Product Name	Siebel eBusiness Applications
Version & Platform	8.0 SIA (Windows Server, IA32)
Product Description	Oracle's Siebel eBusiness Applications provides the industry's most comprehensive family of multi-channel eBusiness applications and services. Siebel eBusiness Applications enable organizations to create a single source of customer information which facilitates selling to, marketing to, and servicing customers across multiple channels, including the Web, call centers, field, resellers, retail, and dealer networks. Siebel is a customer relation management system. The product is a set of applications that access a common, internal data repository. Included in Siebel are a custom web engine and a set of GUIs and tools for accessing data and configuring the system.
Product Category	Web-Based Application

ORACLE



Solution Summary

RSA Access Manager can be configured to protect Siebel eBusiness Application resources, thus providing web access management and Web Single Sign-On to Siebel users. When a user tries to access a protected Siebel eBusiness Application via a web browser, the RSA Access Manager Web Server Plug-in intercepts the request, and redirects the user to the Access Manager logon page. After the user has been authenticated, the Siebel Web Server Extension (SWSE) extracts the user's ID from the HTTP Header variable and passes it to the custom RSA Siebel Security Adapter to create a Siebel session.

Partner Integration Overview	
Use UserID for SSO	Yes
Use UserID for Personalization	Yes
Recognize Authentication Type	N/A
API-level Authorization Support (RuntimeAPI)	No
User Management (AdminAPI)	Via Shared User Repository (LDAP)



Product Requirements

Please refer to the Siebel 8.0 Supported Platforms for details on the following Siebel client/server hardware and software requirements:

- Siebel Gateway Server
- Siebel Enterprise Server
- Siebel Server
- Siebel Web Server Extensions

Integration Modules	
File Name	Destination
Access Manager custom Siebel Security Adaptor (axmSieb8.dll ¹)	%Siebel Root%\siebsrvr\bin
Seibel Web Server Extensions 8.0 (eapps.cfg)	%Siebel Root%\SWEapp\bin
Access Manager custom Siebel Security Adaptor support file (rsasso.txt)	C:\SiebINI

The RSA Access Manager custom Siebel Security Adaptor (axmSieb8.dll) file can be downloaded from the following URL:

ftp://ftp.rsasecurity.com/pub/partner_engineering/ClearTrust/Siebel/axmSieb8.zip

¹ NOTE: This DLL supports UTF8 encoding.



Product Configuration

Before You Begin

This section provides instructions for integrating Oracle Siebel 8.0 with RSA Access Manager 6.x. 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

Overview

RSA Access Manager can be configured to protect Siebel eBusiness Application resources, thus providing Web access management and Web Single Sign-On to Siebel users. When a user tries to access a protected Siebel eBusiness Application via a Web browser, the RSA Access Manager Agent intercepts the request and redirects the user to the Access Manager logon page. After the user has been authenticated, the Siebel Web Server Extension (SWSE) extracts the user's ID from the HTTP Header variable and passes it to the custom RSA Siebel Security Adapter to create a Siebel session.

Prerequisites

The next section provides instructions for integrating RSA Access Manager 6.0 and Siebel 8.0. Assure that the following requirements have been met before proceeding:

- It is assumed that the reader has working knowledge of both products.
- Siebel and RSA Access Manager should be installed and tested before following the instructions in this guide. This document is not intended to suggest optimum installations or configurations.
- Before beginning the integration, create matching RSA Access Manager User ids for all existing Siebel users. **If the products' UIDs don't match, the integration will not work.**

This section contains instructions for configuring Siebel 8.0 to use RSA Security's Custom Security Adapter. It is divided into three parts – the first lists pre-configuration tasks; the second, configuration file parameter settings; and the third, Siebel svrmgr parameter settings.

Some of the parameter values in the following sections are set to configure a specific Siebel deployment. For example, the deployment was configured to protect the Siebel "callcenter_enu" application. Each such deployment-specific value is explained in the beginning of its respective section and underlined in the instructions. These values should be changed appropriately, depending on the details and requirements of the current deployment. However, unless a parameter value has been underlined, please use the values as they appear in the document.



Section 1 – Pre-configuration Tasks

1. Confirm that your Siebel environment is running and that all necessary components including Siebel Gateway Server, Siebel Web Engine, Siebel Database Server, Siebel Application Server, and the appropriate Siebel 8.0 eBusiness Application(s) are installed and properly configured.
2. Confirm that your RSA Access Manager environment is running and that all necessary components are installed and properly configured. Run a simple authentication/authorization test.
3. Install the RSA Access Manager Web Server Agent on the web server that is hosting the Siebel Web Server Extension.
4. Download the RSA Access Manager Siebel Security Adapter module (axm-Sieb8.zip) from

ftp://ftp.rsasecurity.com/pub/partner_engineering/ClearTrust/Siebel/axm-Sieb8.zip

Extract the files contained in the ZIP archive to a temporary directory. The archive contains the following files:

- a. axmSieb8.dll – the RSA Access Manager Siebel Security Adapter
 - b. EncryptPWD.exe – an RSA command line utility for encrypting passwords
 - c. rsasso.txt – the security adapter’s configuration file
5. Install the RSA Access Manager custom Siebel Security Adapter by placing the axmSieb8.dll file in the %Siebel Root%\siebsrvr\bin directory.
 6. Create the appropriate Entitlements/Smart Rules within the RSA Access Manager Entitlement Server Manager to protect the Siebel application(s) URI(s).
 7. Ensure that the Siebel database user “LDAPUSER” and the Siebel user “SADMIN” exist in the current environment. (They both should have been created upon installation). Take note of their corresponding passwords.

SECTION 2 – Configuration Files

This section describes configuration file settings for the RSA Access Manager – Siebel 8.0 integration. The “File Settings” subsection contains a list of file names in bold type, followed by parameter = value pairs. The last configuration file in the list - rsasso.txt - was downloaded in the previous section. For this deployment, rsasso.txt has been copied to “C:\seib\INI”. The absolute path to rsasso.txt will be needed in the following section, so take note of it here. All other configuration files listed below are created as part of the standard Siebel and RSA Access Manager installations.

Unless otherwise noted, the listed parameters already exist – with or without values – in their respective files. The values for these existing parameters should be changed according to the following instructions. When a group of parameter = value pairs or an entire section needs to be added to a file, the group or section is preceded by a comment beginning with “; NOTE:” in the instructions. Please read the “Deployment-specific Values” section, make the appropriate configuration decisions and changes based on the current deployment, and apply the changes to the underlined values in the “File Settings” section. Note that all values that are not underlined in the “File Settings” section should be entered into their corresponding configuration files exactly as they appear.



Deployment-specific Values

This section should be used as a reference when reading the “File Settings” section that follows. Each list item begins with a variable name and an assigned value. The value is underlined (both here and in “File Settings”) to indicate that it’s used in the example but is subject to change in an actual deployment. The following lines in each item list the name of the containing configuration file in parenthesis followed by a description of the variable.

A. EncryptedPassword = FALSE

(eapps.cfg) - set this value to “TRUE” to encrypt all passwords that are stored in eapps.cfg. Since it is set to “False” in the example, all passwords listed in eapps.cfg are in clear text. See the Siebel Administration documentation for more information. Please note that the value of this parameter affects the value of the AnonPassword variable. **It has no effect on the cleartrustdbpassword and encrypt variables contained in the rsasso.txt file.** Continue reading for more information on the rsasso.txt variables.

B. AnonPassword = SADMIN

(eapps.cfg) - set this value to the SADMIN user’s password. See the Siebel Administration documentation for more information about the AnonUser and AnonPassword variables.

Note: The use of “SADMIN” as the anonymous user is only for non-production purposes. The Siebel SADMIN user should not be used as the anonymous user in an actual production environment.

C. [/callcenter_enu]

ProtectedVirtualDirectory = /callcenter_enu

(eapps.cfg) - instead of (or in addition to) editing the “callcenter_enu” section, choose the application section(s) that applies to the current deployment. As noted, the Siebel Sales application and the corresponding “callcenter_enu” section are used in this example.²

D. cleartrustdbpassword = LDAPUSER

(rsasso.txt) set this value to the LDAPUSER user’s password. Upon Siebel installation, this is initialized to “LDAPUSER”. Note that if the encrypt variable is set to “DecryptPWD”, the value of this variable should be the encrypted value of the LDAPUSER user’s password.

E. debug = off

(rsasso.txt) – set this value to “off”. The debug option is for internal use only.

F. encrypt = off

(rsasso.txt) - set this value to the “DecryptPWD” to enable password encryption/decryption.

In order to enable password encryption/decryption, take the following steps:

- a. Set the encrypt variable to “DecryptPWD”
- b. Run the EncryptPWD.exe utility – contained in axmSieb8.zip - on the clear text password currently assigned to the LDAPUSER:

EncryptPWD %Clear_text_pwd%

- c. The utility will echo the encrypted password to the command prompt screen. Copy it and paste it into rsasso.txt as the value for *cleartrustdbpassword*.

² Note that for every applicable Siebel application section in the current deployment, the ProtectedVirtualDirectory variable needs to be set to the section’s name (including the “/”).



File Settings

Below is a list of file names in bold type, followed by *parameter = value* pairs. For each file, replace all underlined parameters with their appropriate substitution and copy all other values exactly as they are listed. Please note that the following configuration settings cannot be delimited with tab characters. Refer to the preceding "Deployment-specific Values" section for information about

webagent.conf

```
cleartrust.agent.user_header_list=CTUSER
```

eapps.cfg

```
[defaults]
EncryptedPassword = FALSE
AnonUserName = SADMIN
AnonPassword = SADMIN
;; NOTE: The following four variable = value pairs need to be added.
TrustToken = HELLO
UserSpec = CTUSER
UserSpecSource = Header
SingleSignIn = TRUE
```

```
[/callcenter_enu]
```

```
;; NOTE: The following variable = value pair needs to be added.
ProtectedVirtualDirectory = /callcenter_enu
```

rsasso.txt

```
[RSAssecadpt]
cleartrustdbuser = LDAPUSER
cleartrustdbpassword = LDAPUSER
debug = off
encrypt = off
```



SECTION 3 – Siebel srvrmgr

This section describes Siebel Server configuration settings for the RSA Access Manager – Siebel 8.0 integration. These parameter values are set via the Siebel srvrmgr utility. Please consult Siebel documentation for using the srvrmgr utility.

Please read the “Deployment-specific Values” section, make the appropriate configuration decisions and changes based on the current deployment, and apply the changes to the underlined values in the “Srvrmgr Settings” section. Note that all values that are not underlined in the “Srvrmgr Settings” section should be entered into their corresponding configuration files exactly as they appear.

Deployment-specific Values

This section contains the following deployment-specific values:

- A. `srvrmgr /e RSA /g ps088 /u SADMIN /p SADMIN`
 - RSA is the enterprise name (“/e”)
 - ps088 is the gateway name server (“/g”)
 - SADMIN is the SADMIN user’s password (“/p”)

- B. `spool c:\srvrmgr.txt`
 - C:\srvrmgr.txt is a path to a “spool” file. The srvrmgr can pipe output to a file for easier reading. If the file doesn’t exist at the specified location, the utility will create it. Set this value to a valid path on the Siebel Server machine.

- C. `change param ConfigFileName=“C:\siebINI\rsasso.txt”` for named subsystem `RSAsecadpt`
 - “C:\siebINI\rsasso.txt” is the absolute path to the rsasso.txt file created in the previous section.

- D. `spool c:\srvrmgr2.txt`
 - See comment B.

- E. `srvrmgr /e RSA /g ps088 /u SADMIN /p SADMIN /s ps088`
 - See comment A for the first three values.
 - ps088 is the Siebel server name (“/s”)

- F. `change param secadptname=RSAsecadpt` for comp `SCCObjMgr_enu`
`change param secadptmode=CUSTOM` for comp `SCCObjMgr_enu`
 - SCCObjMgr_enu is the Object Manager for the Siebel “callcenter_enu” application. Change this value to the appropriate Object Manager(s) name(s).



Srvrmgr Settings

1. Log into srvrmgr:

```
srvrmgr /e RSA /g ps088 /u SADMIN /p SADMIN
```

2. Create a named subsystem for the RSA security adapter. In the example, the adapter is called "RSAsecadpt":

```
create named subsystem RSAsecadpt for subsystem InfraSecAdpt_CUSTOM
```

3. List the default parameters for the new named subsystem. Pipe it to a file for easier reading:

```
spool c:\srvrmgr.txt  
list param for named subsystem RSAsecadpt  
spool off
```

4. Modify the security adapter parameters:

```
change param SecAdptDllName=ctsieb77UTF8 for named subsystem RSAsecadpt  
change param ConfigSectionName=RSAsecadpt for named subsystem RSAsecadpt  
change param SingleSignOn=True for named subsystem RSAsecadpt  
change param TrustToken=HELLO for named subsystem RSAsecadpt  
change param ConfigFileName="C:\siebINI\rsasso.txt" for named subsystem  
RSAsecadpt
```

5. List the changes and ensure that the parameters have been set correctly.

```
spool c:\srvrmgr2.txt  
list param for named subsystem RSAsecadpt  
spool off
```

6. Log off:

```
quit
```

7. Log in to srvrmgr again, specifying the server name:

```
srvrmgr /e RSA /g ps088 /u SADMIN /p SADMIN /s ps088
```

8. Configure the Object Manager(s) to use the RSA Security Adapter:

```
change param secadptname=RSAsecadpt for comp SCCObjMgr_enu  
change param secadptmode=CUSTOM for comp SCCObjMgr_enu
```

9. Log off:

```
quit
```

10. Restart the Siebel servers.

11. Restart the web server.

Certification Checklist Portal Servers and Web-Based Apps

Date Tested: 08/25/2008

Certification Environment		
Product Name	Version Information	Operating System
RSA Access Manager	6.0	Windows Server 2003
RSA Access Manager Agent for IIS 6.0	4.6	Windows Server 2003
RSA Access Manager custom Siebel Security Adapter (axmSieb8.dll)	Supports Siebel SIA 7.5 through 8.0	Windows Server 2003
Siebel eBusiness Applications	8.0 SIA	Windows Server 2003
Siebel Web Server Extension (SWSE)	8.0 SIA	Windows Server 2003

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	✓
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	✓
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	✓

JGS

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



Notes

- **Logout.** Access Manager handles user log-out via its web plug-in. It parses all web requests for 'ct_logout.html'. When this page is found, the plug-in will then expire the users' cookie. Within the Siebel eBusiness Application, you will need to redirect the function of the logout button to the 'ct_logout.html' page instead of performing its regular function. Using Siebel Tools, locate the Siebel container web template for that application and configure the Siebel "Logout" control on that template to go to the "/ct_logoff.html" page instead of performing its regular operation. Please see Siebel Bookshelf for more information (Application Development > Tools Reference).