



RSA Secured Implementation Guide For User Management Products

Last Modified 10, 22 2007

Partner Information

Product Information	
Partner Name	Siebel
Web Site	www.siebel.com
Product Name	eBusiness Application
Version & Platform	7.8.2 – Solaris
Product Description	Siebel Systems 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

Solution Summary

RSA Access Manager can be configured to protect Siebel eBusiness Application URIs, 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 custom RSA Siebel Security Adapter extracts the user's ID from a HTTP header variable and creates a Siebel session.

Partner Integration Overview	
Use UserID for SSO	Yes
Use UserID for Personalization	Yes
Recognize Authentication Type	N/A
API-level Authentication Type	No
User Management (AdminAPI)	No

Product Requirements

Please refer to the Siebel 7.8.2 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

Operating System – Solaris 9/10	
Integration Modules	
File Name	Destination
Access Manager custom Siebel Security Adapter	%Siebel_Root%\siebsrv\bin

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

The next section provides instructions for integrating RSA Access Manager 5.5.3 and Siebel 7.8.2. 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.**

Configuring Siebel

This section contains instructions for configuring Siebel 7.8.2 to use RSA Security's Custom Security Adapter. It is divided into three sections – the first lists pre -configuration tasks; the second, configuration file parameter settings; and the third, Siebel srvmgr 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. Therefore, the "Configuration Files" section lists changes to parameters in "uagent.cfg" – the "callcenter_enu" application's configuration file. 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 7.8.2eBusiness 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 (ctsieb78UTF8_Solaris.zip) from:

ftp://ftp.rsasecurity.com/pub/partner_engineering/ClearTrust/Siebel/ctsieb78UTF8_Solaris.zip

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

- a. libctsieb78UTF8.so – the RSA Access Manager Siebel Security Adapter
 - b. rsasso.txt – the security adapter’s configuration file
5. Install the RSA Access Manager custom Siebel Security Adapter by placing the libctsieb78UTF8.so file in the <Siebel install>/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 7.8.2 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. However, the “uagent.cfg” file is used for an example in which RSA Access Manager is used to protect the Siebel “callcenter_enu” application resources. **The listed parameter settings for this file should be made to the configuration file of each Siebel application that will deploy the RSA Siebel Security Adapter.** This may or may not include “uagent.cfg”.

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 contains the following deployment-specific values:

A. EncryptedPassword = FALSE

- (eapps.cfg) set this value appropriately. 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 about the EncryptedPassword parameter as well as all other “eapps.cfg” settings. Please note that the value of this parameter affects the value of the AnonPassword variable. **It has no affect on the**

cleartrustbpassword and encrypt variables contained in the “rsasso.txt” file. For more information on the “rsasso.txt” variables, continue reading.

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.

C. [/callcenter_enu]

ProtectedVirtualDirectory = /callcenter_enu

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

D. uagent.cfg

- instead of (or in addition to) editing the parameter values in this file, choose the Appropriate Siebel application configuration file(s) (i.e. “auto_ct.cfg”, “eservice.cfg”, etc.)

E. 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.

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.

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

SingleSignOn = TRUE

[/callcenter_enu]

:: NOTE: The following variable = value pair may or may not need to be added.

ProtectedVirtualDirectory = /callcenter_enu

uagent.cfg

```
[InfraSecMgr]
SecAdptName = RSAsecadpt
SecAdptMode = Custom
```

;; NOTE: The following section needs to be added.

```
[RSAsecadpt]
SecAdptDllName = ctsieb78UTF8
SingleSignOn = TRUE
TrustToken = HELLO
```

rsasso.txt

```
[RSAsecadpt]
cleartrustdbuser = LDAPUSER
cleartrustdbpassword = LDAPUSER
```

SECTION 3 – Siebel svrmgr

This section describes Siebel Server configuration settings for the RSA Access Manager – Siebel 7.8 integration. These parameter values are set via the svrmgr utility. Please consult Siebel documentation for using the svrmgr 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 “Svrmgr Settings” section. Note that all values that are not underlined in the “Svrmgr 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. svrmgr /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 /tmp/svrmgr.txt
 - tmp/svrmgr.txt is a path to a “spool” file. The svrmgr 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=“/tmp/siebINI/rsasso.txt” for named subsystem RSAsecadpt
 - “/tmp/siebINI/rsasso.txt” is the absolute path to the “rsasso.txt” file created in the previous section.

- D. spool /tmp/svrmgr2.txt
 - See comment B.

- E. svrmgr /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).

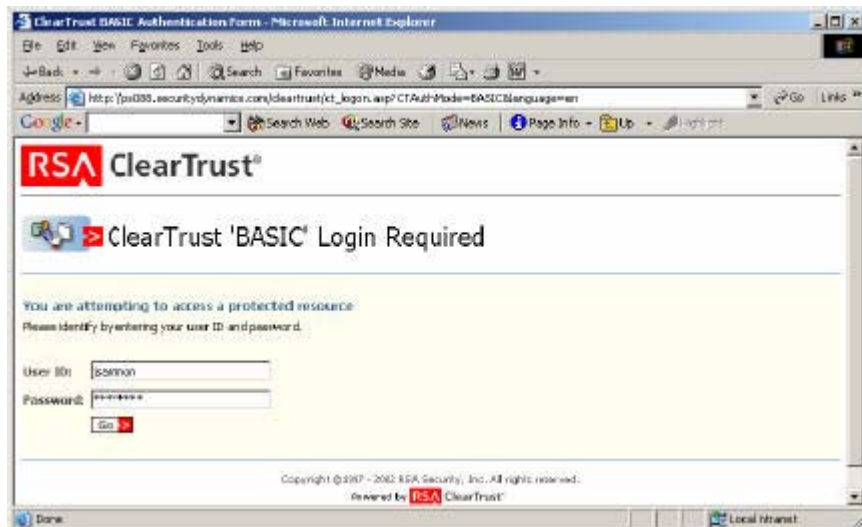
Srvrmgr Settings

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 /tmp/srvrmgr.txt***
 - ***list param for named subsystem RSAsecadpt***
 - ***spool off***
4. Modify the security adapter parameters:
 - ***change param CustomSecAdpt_SecAdptDllName=ctsieb77UTF8 for named subsystem RSAsecadpt***
 - ***change param ConfigSectionName= RSAsecadpt for named subsystem RSAsecadpt***
 - ***change param CustomSecAdpt_SingleSignOn=True for named subsystem RSAsecadpt***
 - ***change param CustomSecAdpt_TrustToken=HELLO for named subsystem RSAsecadpt***
 - ***change param ConfigFileName="/tmp/siebINI/rsasso.txt" for named subsystem RSAsecadpt***
5. List the changes and ensure that the parameters have been set correctly.
 - ***spool /tmp/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.

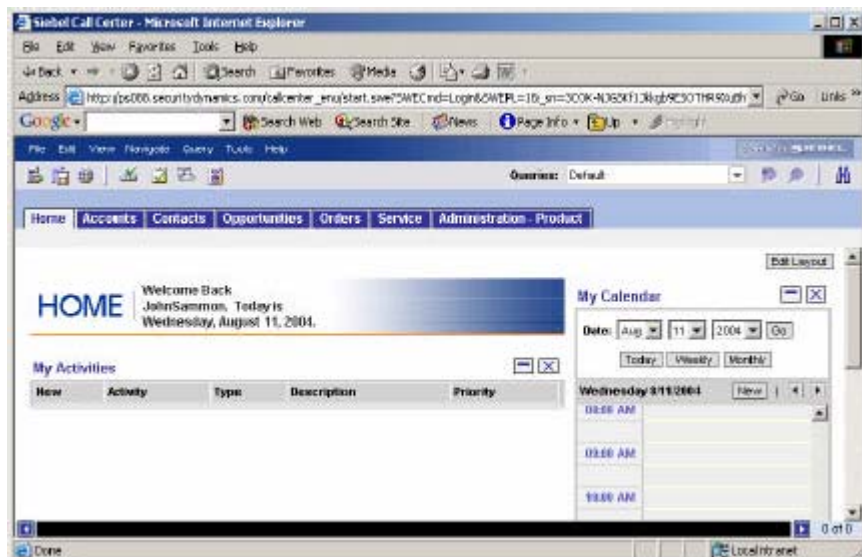
End User Experience

A login example:

The user opens a browser and types in a Siebel resource (“/callcenter_enu” in this case). The user is redirected to the RSA Access Manager Login page. (Note that in this example the jsammon user exists in both Siebel and RSA Access Manager environments, and has been given access to the /callcenter_enu application.)



The user is authenticated and redirected to the Siebel application.



Certification Checklist for User Management Products

Date Tested: 01/17/2007


Certification Environment		
Product Name	Version Information	Operating System
RSA Access Manager	6.0	Windows Server 2003
RSA Access Manager Agent for IIS	4.6	Solaris 9
RSA Access Manager custom Siebel Security Adapter (ctsieb77UTF8.so)	Supports Siebel 7.5, 7.7, 7.8 Applications.	Solaris 9
Siebel eBusiness Applications	7.8.2 SIA	Solaris 9
Siebel Web Server Extension (SWSE) (IIS 6.0)	7.8.2 SIA	Solaris 9

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

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).