



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

Last Modified 03/23/2007

Partner Information

Partner Name	Oracle
Web Site	www.oracle.com/siebel/index.html
Product Name	Siebel Analytics
Version & Platform	7.8.2 SIA (Windows Server, IA32)
Product Description	Siebel Business Analytics applications are comprehensive prebuilt solutions that deliver pervasive intelligence across an organization, empowering users at all levels — from front line operational users to senior management — with the key information they need to maximize effectiveness. Intuitive and role-based, these solutions transform and integrate data from a range of enterprise sources, including Siebel, Oracle, PeopleSoft, SAP, and corporate data warehouses — into actionable insight that enables more effective actions, decisions, and processes.
Product Category	Web-Based Application

Solution Summary

Feature	Details
Use UserID for SSO	Yes
Use UserID for Personalization	Yes
Username/Password Auth	Yes
SecurID Support	Yes, via web plug-in
Keon Support	Yes, via web plug-in
Authorization Support via Clear Trust API	No

Product Requirements

Please refer to the **Siebel 7.8.2 Supported Platforms** for details on the following Siebel client/server hardware and software requirement. See **Installing and Configuring Siebel Applications** for installation and configuration details.

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

Overview

RSA Access Manager can be configured to protect Siebel Analytics URIs, thus providing web access management and web single sign on to Siebel users. When a user tries to access a protected Analytics application via a web browser, the RSA Access Manager Web Server Agent intercepts the request, and redirects the user to the Access Manager logon page. After the user has been authenticated, the web server plug-in writes the authenticated username to an HTTP Header variable. The Siebel Analytics Web (SAW) ISAPI plug-in is configured to trust this variable's value and use it to create a session.

Prerequisites

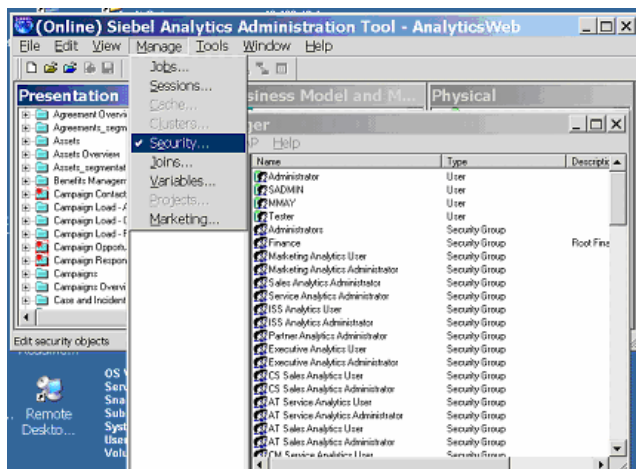
The next section provides instructions for integrating RSA Access Manager 6.0 and Siebel Analytics 7.8.2. Assure that the following requirements have been met before proceeding:

- 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.**

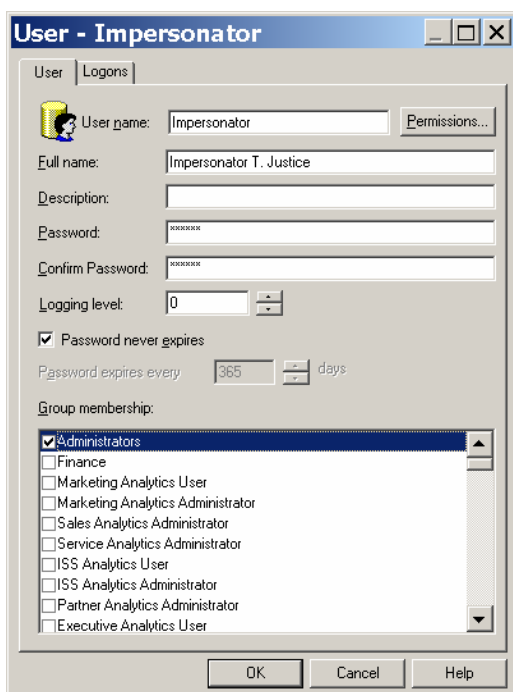
Product Configuration

1. Create an Analytics Server user for impersonation

- Log in to the Analytics Server Administrative Tool.
- Select **Security** from the **Manage** menu.



- In the Security Manager, select **New-> User** from the **Action** menu.
- Create a user who is a member of the group **Administrators**. In this example, the user's name is **Impersonator** and the password is **secret**.



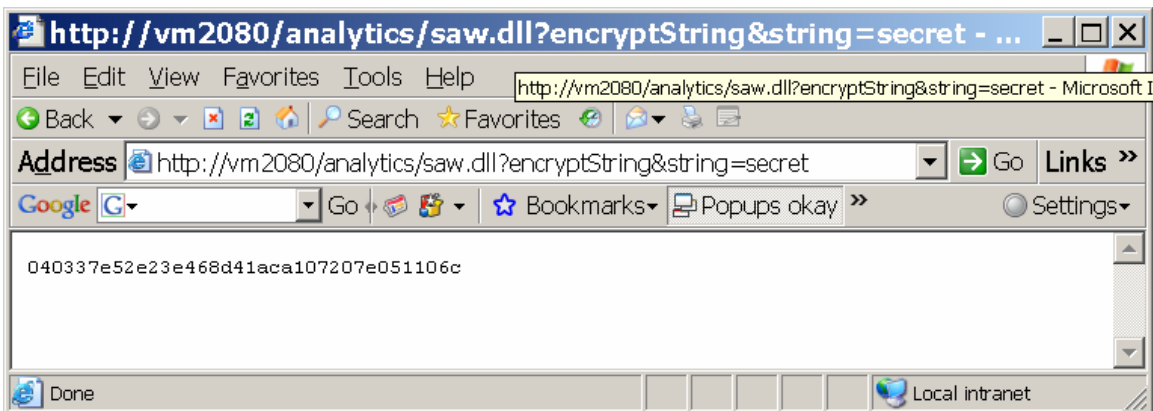
2. Generate an encrypted password

- For security purposes, ensure that HTTP logging is disabled.
- Log into Siebel Analytics Web as an administrator, and issue the following URL:

<http://server/analytics/saw.dll?encryptString&string=secret>

where **secret** is the password for the impersonator user created in step 1.

- The encrypted password will be displayed in the browser. Copy the string and save it to a temporary file.



3. Configure SAW

- Shut Siebel Analytics Web down.
- Open %SiebelAnalyticsDataHOME%\Web\configinstanceconfig.xml and add the following entries inside the <WebConfig><ServerInstance> tag:
 - RPC/PermittedClientList – A comma separated list all of the client IP addresses that will be allowed to communicate directly with SAW
 - Auth/Impersonator – the user created for impersonation in step 1
 - Auth/ImpersonatorPassword – the encrypted password created in step 2
 - Auth/SSOEnabled – **y** to enable SSO and **n** to disable it
 - Auth/SSOServerVariable – the name of the HTTP header variable that will contain the Access Manager –authenticated username. **HTTP_CT_REMOTE_USER**, for example.
 - Auth/SSOStripWindowsDomain- **y** to strip out a \ and the preceding domain name from the username and **n** otherwise
- See the example xml file below:

```
<?xml version="1.0"?>
  <WebConfig>
    <ServerInstance>
      <RPC>
        <PermittedClientList>127.0.0.1</PermittedClientList>
      </RPC>
```

```

<Auth>
  <Impersonator>Impersonator</Impersonator>
  <ImpersonatorPassword>040337e52e23e468d41aca107207e051106c
  </ImpersonatorPassword>
  <SSOEnabled>y</SSOEnabled>
  <SSOServerVariable>REMOTE_USER</SSOServerVariable>
  <SSOStripWindowsDomain>N</SSOStripWindowsDomain>
</Auth>
</ServerInstance>
</WebConfig>

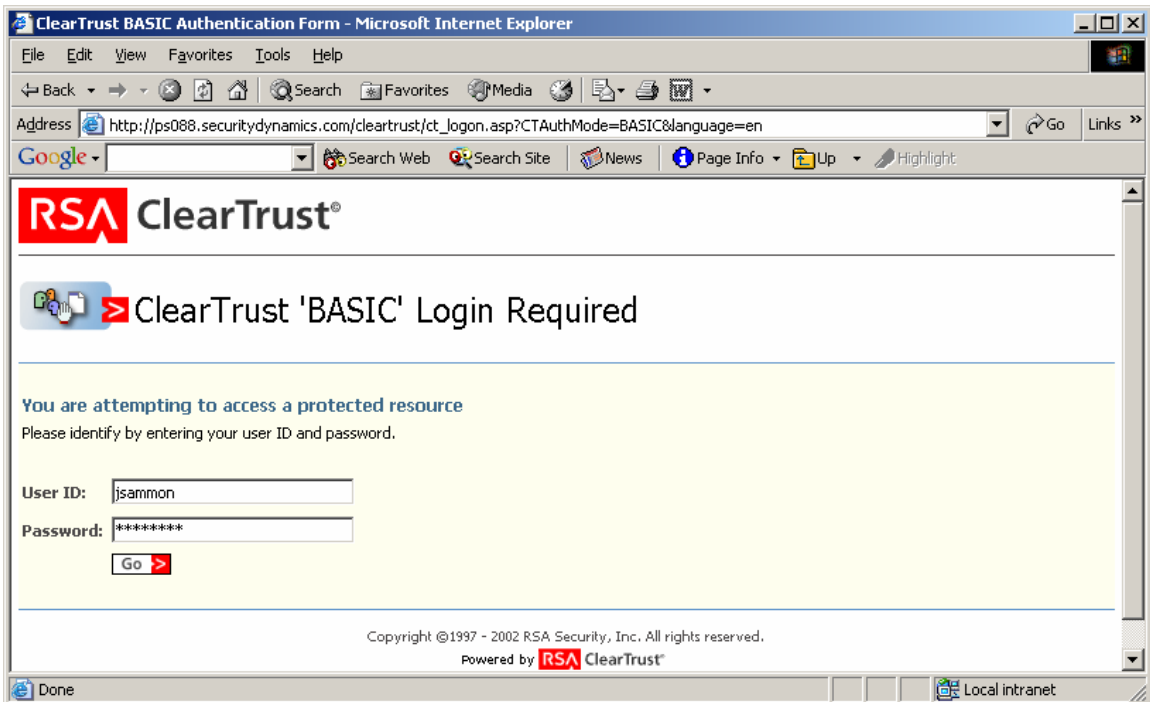
```

End User Experience

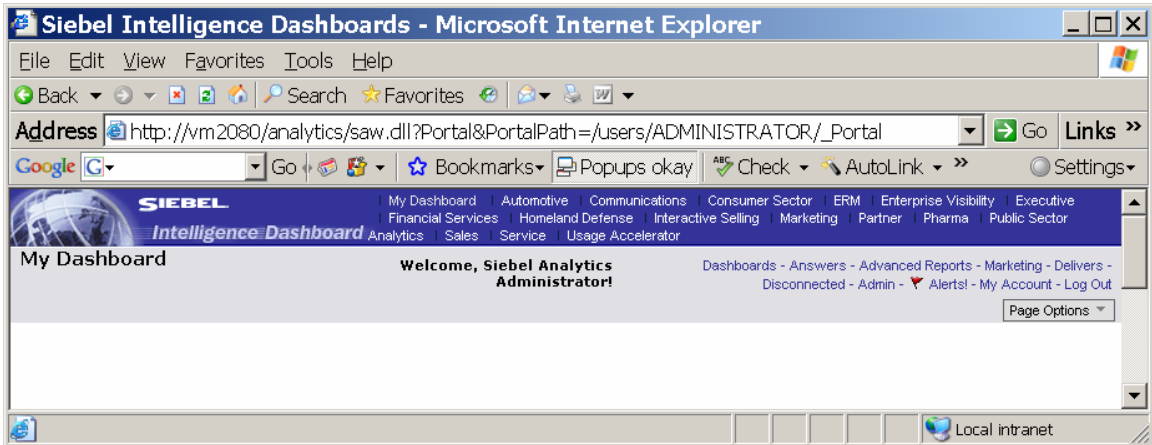
A login example:

The user opens a browser and types in a protected Siebel resource (*/Analytics* 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 */Analytics* application.)



The user is authenticated and redirected to the Siebel application.



Certification Checklist Portal Servers and Web-Based Apps

Date Tested: 03/12/2007

Certification Environment		
Product Name	Version Information	Operating System
RSA Access Manager	6.0	Windows Server 2003
RSA Access Manager Agent for IIS	4.6	Windows Server 2003
Oracle Database	9.0.2.4	Windows Server 2003
Siebel Analytics	7.8.2	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