



## RSA Secured Implementation Guide

### For Portal Servers and Web-Based Applications

Last Modified 12/2/05

#### Partner Information

---

Product Information	
Partner Name	Business Objects
Web Site	<a href="http://www.businessobjects.com">www.businessobjects.com</a>
Product Name	InfoView
Version & Platform	X1r2 / BusinessObjects Enterprise
Product Description	<p>Business Objects is an integrated query, reporting and analysis solution for business professionals that allows you to access the data in your corporate databases directly from your desktop and present and analyze this information in a Business Objects document.</p> <p>InfoView is your personal gateway to your corporate information capital. It allows you to access documents generated from your corporate data storage, from your office, home, or around the world, using your intranet, extranet, or the World Wide Web.</p>
Product Category	Portal Server



## Solution Summary

To achieve Single-Sign-On (SSO) with BusinessObjects Enterprise Xlr2 InfoView, a web server proxy to the InfoView application server host must be configured. An RSA ClearTrust agent is installed on this web server and it is configured to protect BusinessObjects Enterprise resources. Pre-existing RSA ClearTrust (LDAP) groups can be imported into InfoView. These groups and their individual users can then be managed and maintained via the ClearTrust Entitlements Manager and servers. Each user is given a BusinessObjects Enterprise alias and an LDAP alias, each of which correspond to the RSA ClearTrust username. BusinessObjects Enterprise is then configured to trust RSA ClearTrust-authenticated users.

The ClearTrust Administrator creates BusinessObjects Enterprise users, groups, resources, and entitlements. When a user first requests a protected resource, the RSA ClearTrust web server agent prompts the user for authentication credentials. The agent communicates with the RSA ClearTrust servers to establish authentication and determine if the user is authorized to access the requested resource. Following successful authentication and authorization, the user is forwarded to a script within the BusinessObjects Enterprise web application. This script retrieves the identity of the user by parsing an HTTP header variable and creates a personalized BusinessObjects Enterprise session.

Figure 1 illustrates a high-level view of this deployment.

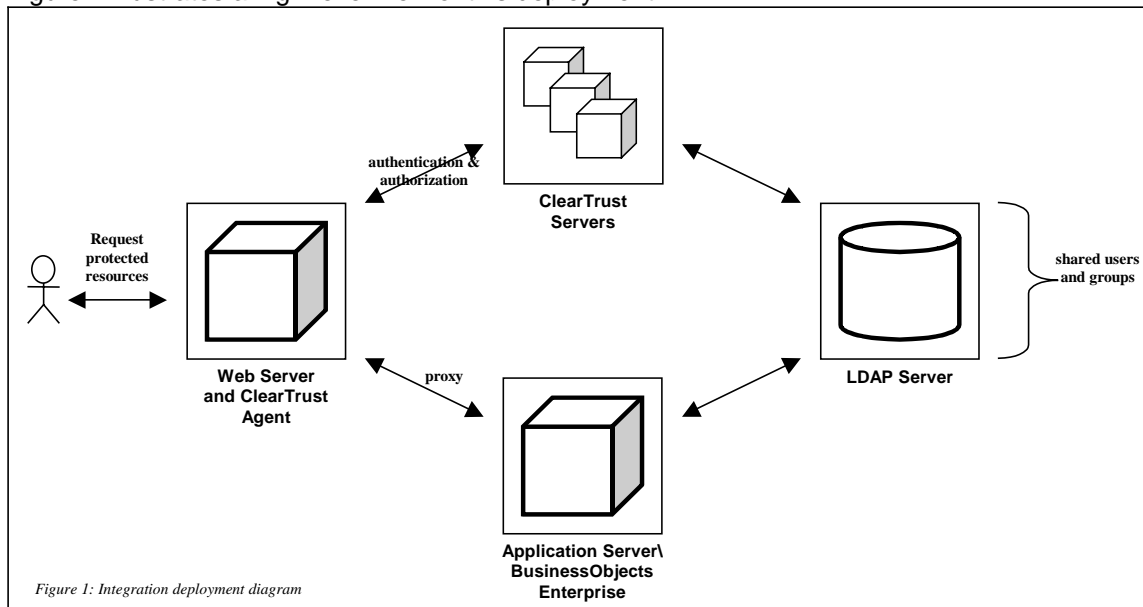


Figure 1: Integration deployment diagram

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

## Product Requirements

---

Partner Product Requirements: <Partner Product (Component)>	
<b>CPU</b>	Pentium 3 - 700 Mhz
<b>Memory</b>	1GB RAM
<b>Storage</b>	5 GB for BusinessObjects Enterprise and an additional 1.5 GB for Performance Management
<b>Optical Drives</b>	CD-ROM

Operating System <sup>1</sup>	
Platform	Required Patches
Windows 2000	SP4 Advanced Server, SP4 Datacenter Server or SP4 Server
Windows Server 2003	Datacenter Edition, Enterprise Edition, Standard Edition or Web Edition <sup>2</sup>

Integration Modules	
File Name	Destination
<a href="ftp://ftp.rsasecurity.com/pub/partner_engine/ClearTrust/BusinessObjects/BOXI_CT5_53_SSO.zip">ftp://ftp.rsasecurity.com/pub/partner_engine/ClearTrust/BusinessObjects/BOXI_CT5_53_SSO.zip</a>	Download the file and unzip it into a directory on the BusinessObjects Enterprises host.

<sup>1</sup> Business Objects supports and recommends the installation of all MSFT critical patches for the listed operating systems.

<sup>2</sup> Each of these editions is supported with or without SP1.

# Product Configuration

---

## ***Before You Begin***

This section provides instructions for integrating the partners' product with RSA ClearTrust. 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***

Before beginning the RSA ClearTrust – BusinessObjects Enterprise InfoView configuration, make sure that:

- The RSA ClearTrust servers have been installed.
- BusinessObjects Enterprise Xlr2 has been installed, including:
  - The Java-based Administrative console
  - InfoView
- A web server proxy to the application server that hosts BusinessObjects Enterprise has been installed and configured.<sup>3</sup>
- An RSA ClearTrust Web Server Agent has been installed and tested on the web server proxy.

## ***Configuring BusinessObjects Enterprise Xlr2***

You can configure InfoView to use RSA ClearTrust for user authentication and Single-Sign-On (SSO). There are five basic steps in this configuration process:

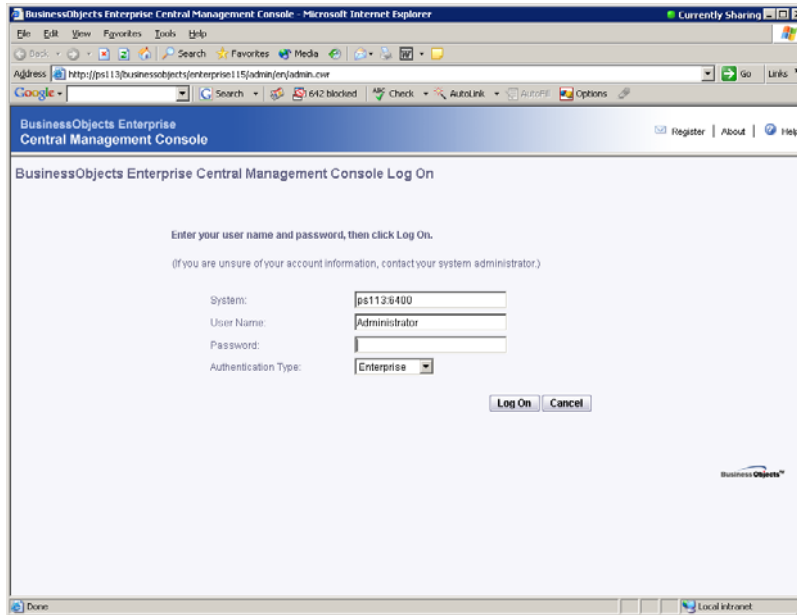
1. [Configure the LDAP plug-in](#)
2. [Build LDAP user accounts](#)
3. [Configure the Trusted Authentication shared secret](#)
4. [Add an Enterprise alias to each user account](#)
5. [Install the SSO and exit scripts](#)

---

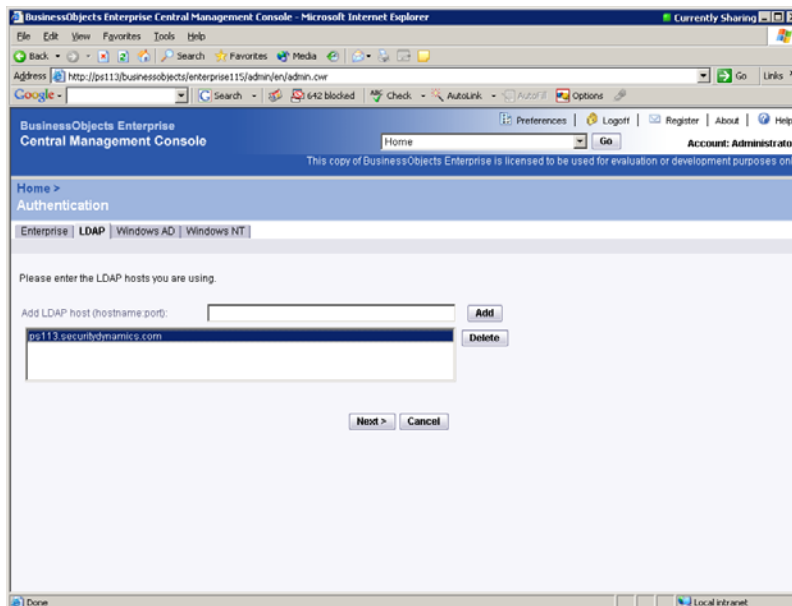
<sup>3</sup> Web server proxy configuration is outside of the scope of this documentation. Please refer to the appropriate application server documentation.

## Configure the LDAP plug-in

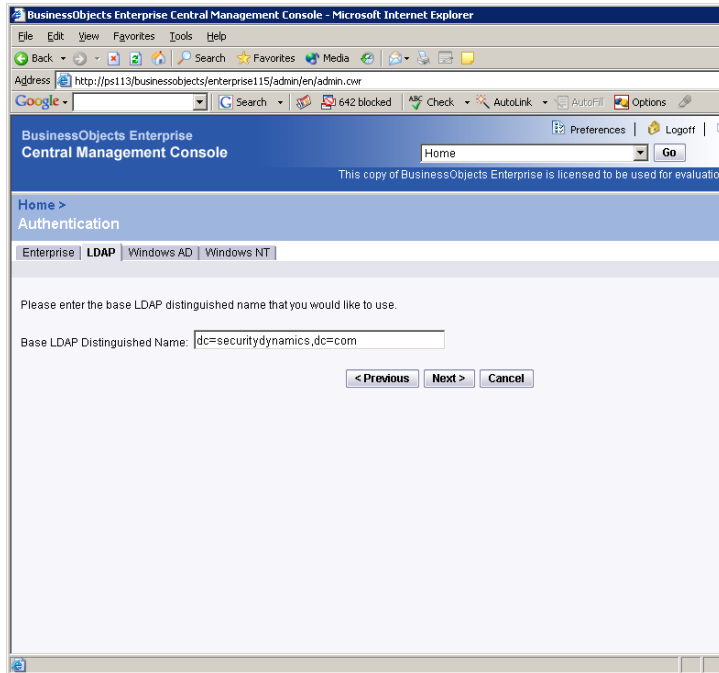
1. Launch and log into the BusinessObjects Enterprise Central Management Console (CMC).



2. Select **Authentication** from the **Manage** frame and then chose the **LDAP** tab.
3. Enter the LDAP hostname and port, click the **Add** button and then click **Next**.




4. Enter the base LDAP distinguished name, and click **Next**.

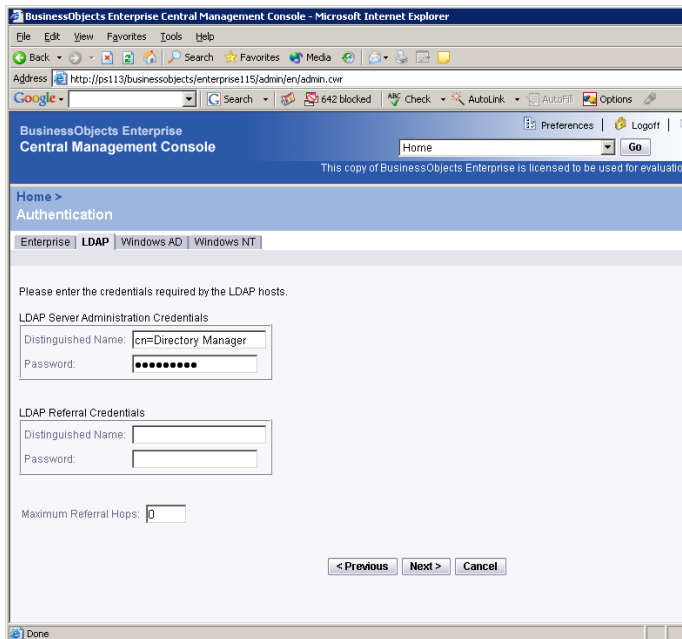


5. Enter LDAP log-on credentials and click **Next**.

---

 **Note:** The credentials do not need to be those of an LDAP server administrator. The user only needs read access to the server.

---

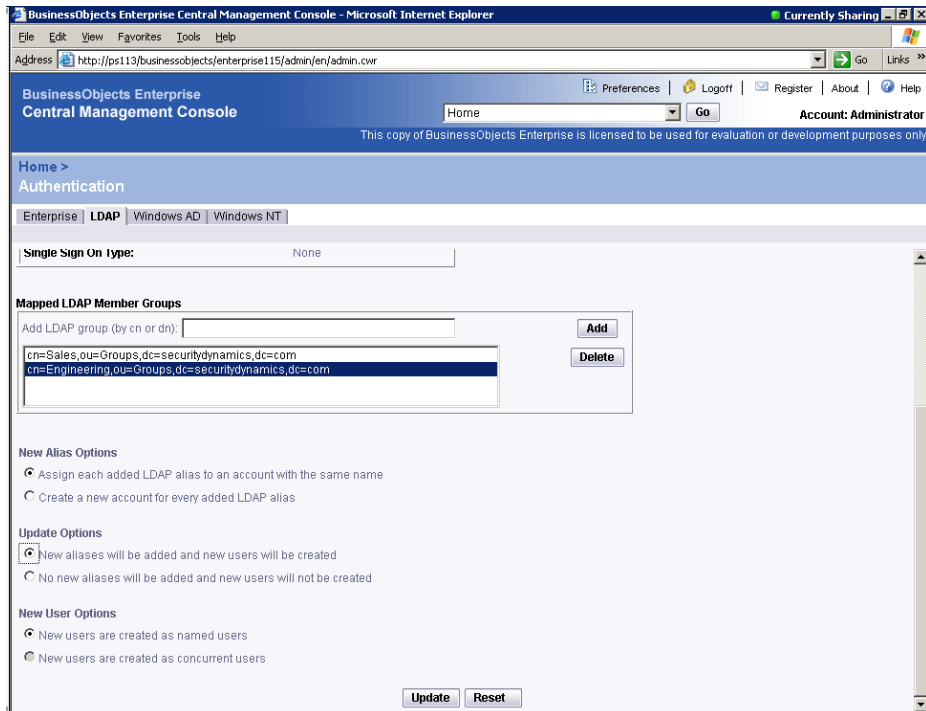


6. Select **Basic (no SSO)** for LDAP authentication and click **Next**.

7. Select the following radio buttons:
  1. Assign each added LDAP alias to an account with the same name
  2. No new aliases will be added and new users will not be created
  3. New users are created as concurrent users
8. Click **Next** and **Finish**.

## Build LDAP user accounts

1. Launch and log into the BusinessObjects Enterprise Central Management Console (CMC).
2. Select **Authentication** from the **Manage** frame and then chose the **LDAP** tab.
3. Enter and add all ClearTrust/LDAP groups to be imported.
9. Select the following radio buttons:
  1. Assign each added LDAP alias to an account with the same name
  2. New aliases will be added and new users will not be created
  3. New users are created as named users
10. Click **Update**.



## Configure the Trusted Authentication shared secret

1. Launch and log into the CMC.
2. Select **Authentication** from the **Manage** frame and then chose the **Enterprise** tab.
3. Select the **Trusted Authentication is enabled** checkbox and chose and enter a passkey in the **Shared secret** field.
4. Click **Update**.

The screenshot displays the BusinessObjects Enterprise Central Management Console (CMC) interface. The top navigation bar includes links for Preferences, Logoff, Register, About, and Help. The main content area is titled "Authentication" and features a tabbed interface with "Enterprise" selected. The configuration page includes several sections:

- Must wait N minute(s) to change password:** A checkbox is unchecked, and the value "0" is entered in the adjacent text box.
- Logon Restrictions:**
  - Disable account after N failed attempts to log on:** A checkbox is unchecked, and the value "3" is entered in the "N is:" text box.
  - Reset failed logon count after N minute(s):** The value "5" is entered in the text box.
  - Re-enable account after N minute(s):** A checkbox is unchecked, and the value "0" is entered in the text box.
- Trusted Authentication:**
  - Trusted Authentication is enabled:** A checkbox is checked.
  - Shared secret:** A text box contains a series of black dots representing a masked password.
  - Trusted logon request is timeout after N millisecond(s) (0 means no limit):** The value "0" is entered in the text box.

At the bottom of the configuration area, there are "Update" and "Reset" buttons. The status bar at the bottom of the window shows "Done" and "Local Intranet".



5. Navigate to `%BUSINESSOBJECTS_HOME%\BusinessObjects Enterprise 11.5\win32_x86\plugins\auth\secEnterprise` and create a new text file named ***TrustedPrincipal.conf***. Type the following line at the beginning of this file:

***SharedSecret=%SHARED\_SECRET%***

where `%SHARED_SECRET%` matches the passkey entered in step 3.

6. Save changes to ***TrustedPrincipal.conf*** and close it.

## Add an Enterprise alias to each user account

1. Launch and log into the CMC.
2. Select ***Authentication*** from the ***Manage*** frame and then chose the ***Enterprise*** tab.
3. Deselect every checkbox except ***Trusted Authentication is enabled***.
4. Click ***Update***.
5. Return to CMC ***Home*** and select ***Users*** from the ***Organize*** frame.
6. For each user, open the user account, scroll to the end of the page, and click ***New Alias***.
7. Select ***Enterprise*** as the Authentication type and enter a password.<sup>5</sup>
8. Deselect the ***User must change password at next logon*** checkbox.
9. Click ***OK***.

Home > Users > Anita >  
New Alias

Authentication Type: Enterprise

Account Name: Anita

Enterprise Password Settings:

Password: [masked]  Password never expires

Confirm: [masked]  User must change password at next logon

User cannot change password

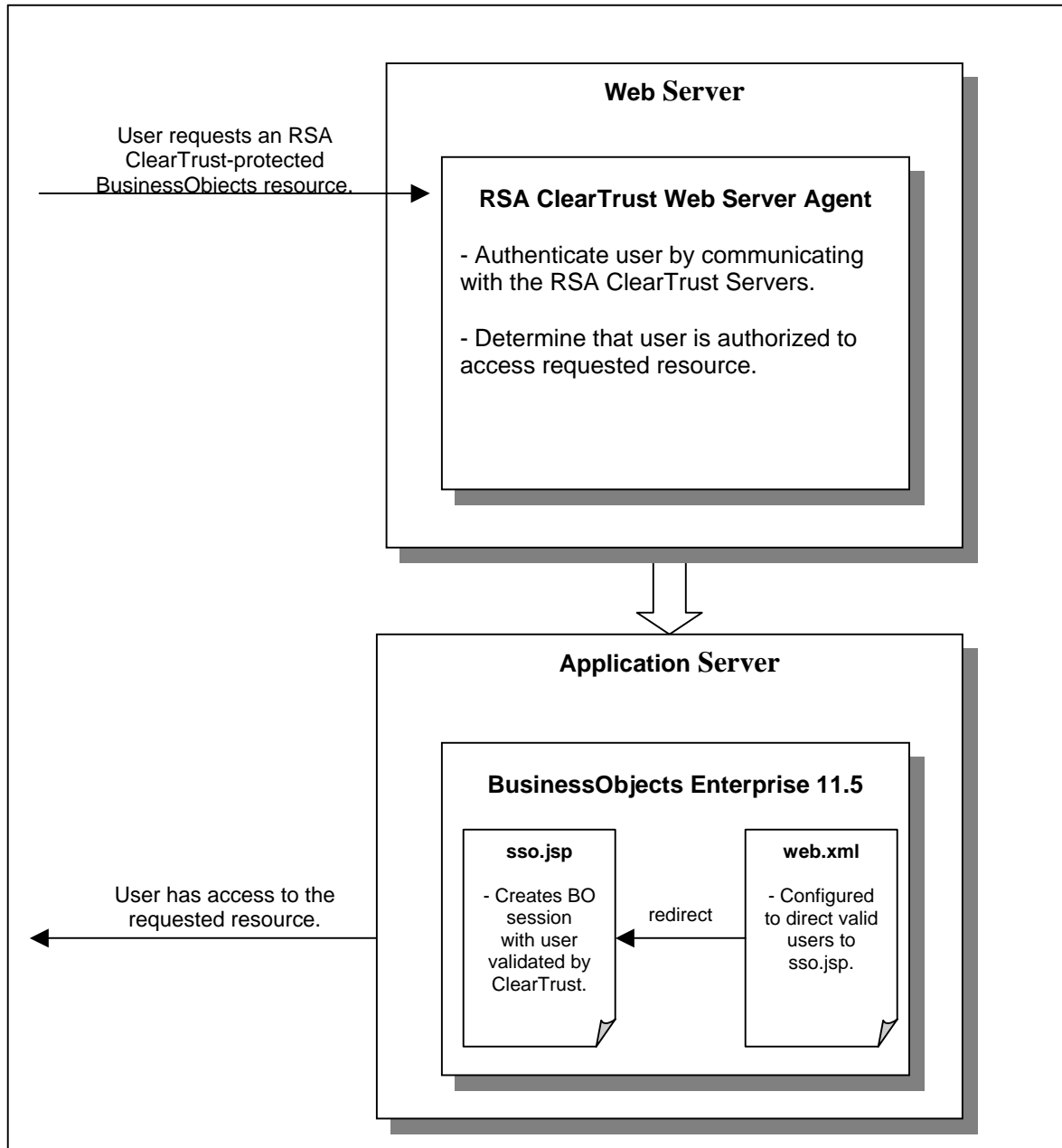
OK Cancel

<sup>4</sup> Replace `%BUSINESSOBJECTS_HOME%` with BusinessObjects Enterprise's installation directory. The default value for this directory is `C:\Program Files\Business Objects`.

<sup>5</sup> Note that this password doesn't have to match the user's RSA ClearTrust password. It is the latter password the user must remember and use to authenticate.


## Install the SSO and exit scripts

The SSO script – sso.jsp – is contained in the BOXI\_CT553.zip file (previously downloaded). This file is responsible for creating a BusinessObjects Enterprise session for the ClearTrust-authenticated user. After a successful ClearTrust authentication, the user will be redirected to this JSP. The BusinessObjects Enterprise web application's web.xml file must be configured in order for this redirection to take place.



The exit script – `exit.jsp` – is also contained in the `BOXI_CT553.zip` file. This script will be called when a user clicks the Logoff button on the CMC. It is responsible for destroying the BusinessObjects Enterprise session and closing the browser window (thus destroying the RSA ClearTrust SSO token).

---

 **Note: The `sso.jsp` and `exit.jsp` files are provided as examples. They may be used in a production environment, but they can also be modified to meet a specific customer's requirements.**

---

In order to install and configure the scripts:

1. Navigate to `%BUSINESSOBJECTS_HOME%\Tomcat\webapps\businessobjects\enterprise115\desktoplaunch\WEB-INF` and open the `web.xml` file. Find the `welcome-file-list` tag, and change the value of the `welcome-file` to `exit.jsp`<sup>6</sup>:

```
<!-- The welcome file list -->
<welcome-file-list>
  <welcome-file>exit.jsp</welcome-file>
</welcome-file-list>
```

2. Copy the `sso.jsp` and `exit.jsp` files to the `%BUSINESSOBJECTS_HOME%\Tomcat\webapps\businessobjects\enterprise115\desktoplaunch\` directory.

---

<sup>6</sup> The default `welcome-file` value is `default.htm`.

# Certification Checklist Portal Servers and Web-Based Apps

Date Tested 11/18/2005

Certification Environment		
Product Name	Version Information	Operating System
RSA ClearTrust	5.5.3	Windows 2003 Server Enterprise
RSA ClearTrust IIS Agent	6.0	Windows 2003 Server Enterprise
BusinessObjects Enterprise Xlr2 InfoView	Xlr2	Windows 2003 Server Enterprise

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

JGS

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