Single Sign-On with
SAP BusinessObjects Access Control 5.3

Author:
Harleen Kaur
SAP GRC Regional Implementation Group

Applicable Releases:
SAP BusinessObjects Access Control 5.3

Topic Area:
Single Sign-On Version 2.0

Capability:
All

September 2009
## Typographic Conventions

<table>
<thead>
<tr>
<th>Type Style</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example Text</strong></td>
<td>Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation</td>
</tr>
<tr>
<td><strong>Example text</strong></td>
<td>Emphasized words or phrases in body text, graphic titles, and table titles</td>
</tr>
<tr>
<td><strong>Example text</strong></td>
<td>File and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools</td>
</tr>
<tr>
<td><strong>Example text</strong></td>
<td>User entry texts. These are words or characters that you enter in the system exactly as they appear in the documentation</td>
</tr>
<tr>
<td><strong>&lt;Example text&gt;</strong></td>
<td>Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system</td>
</tr>
<tr>
<td><strong>EXAMPLE TEXT</strong></td>
<td>Keys on the keyboard, for example, F2 or ENTER</td>
</tr>
</tbody>
</table>

## Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔴</td>
<td>Caution</td>
</tr>
<tr>
<td>📚</td>
<td>Note or Important</td>
</tr>
<tr>
<td>🌐</td>
<td>Example</td>
</tr>
<tr>
<td>🔴</td>
<td>Recommendation or Tip</td>
</tr>
</tbody>
</table>
# Table of Contents

1. Introduction .....................................................................................................................1

2. Prerequisites....................................................................................................................2

3. Setting up Single Sign-On for SAP BusinessObjects AC 5.3 ........................................2
   3.1 Single Sign-On with SAP BusinessObjects AC in a Portal environment: ............2
      3.1.1 Access Control and Portal on same server ....................................................3
      3.1.2 Access Control and Portal on different servers ..............................................3
      3.1.3 SSO Wizard ................................................................................................10
      3.1.4 Troubleshooting ..........................................................................................11
   3.2 SSL and X.509 Client Certificates ...........................................................................11
   3.3 Suppressing email Notifications with Passwords .....................................................12
   3.4 Kerberos based authentication with SPNEGO .........................................................13
      SSO in an SPNEGO Environment .........................................................................13
      3.4.1 How to achieve SSO for email links ............................................................15
      3.4.2 Single Sign-On with multiple LDAPs as authentication ...............................16

4. Related SAP Notes ........................................................................................................16

5. Further Reading .............................................................................................................17

6. Comments and Feedback .............................................................................................17
1. Introduction

Single Sign-On (SSO) is a mechanism whereby a single action of user authentication and authorization can permit a user to access all the systems where he has access permission, without the need to enter multiple passwords. It is a specialized form of authentication that enables you to authenticate once and gain access to the resources of multiple software systems.

Reasons for Single Sign-On

- In a complex system landscape, an employee has many user IDs with different passwords
- Different procedures for each system to roll-out, reset and change new / existing passwords
- Significant administration task is required to manage different user IDs and passwords

Single Sign-On Benefits

- Single Sign-On provides for an environment where users are allowed access to multiple systems based on an initial authentication.
- Centralized reporting for compliance adherence
- Administration costs and efforts are drastically reduced

SAP BusinessObjects AC 5.3 provides the ability to integrate with several different types of Single Sign-On mechanisms using SAP NetWeaver. So, SAP BusinessObjects AC depends on the capabilities of NetWeaver to provide SSO. This enables SAP BusinessObjects AC 5.3 to participate in SSO scenarios with a larger number of different applications. The three types of SSO services supported by SAP NetWeaver are:

- Windows integrated SSO
- Web based SSO
- Enterprise SSO

Windows integrated Single Sign-On:

These services enable you to connect to multiple applications within your network that use a common authentication mechanism. These services request and verify your credentials after you log into the network, and use your credentials to determine the actions that you can perform based on your user rights. For example, if applications integrate using Kerberos, then after the system authenticates your user credentials, you can access any resource in the network that is integrated with Kerberos. SAP BusinessObjects AC 5.3 can also be integrated with Kerberos and this document covers the configuration steps required for this integration.

Web based Single Sign-On:

These services enable you to access resources over the Internet by using a single set of user credentials. The user provides a set of credentials to log on to different Web sites that belong to different organizations.

Enterprise Single Sign-On:

These services enable you to integrate multiple heterogeneous applications and systems in the enterprise environment.
2. Prerequisites

Single Sign-On for SAP BusinessObjects AC components is supported using the Single Sign-On Launch Pad. It can also be configured for individual components of SAP BusinessObjects AC using NetWeaver Portal iViews. This allows customers to provide Single Sign-On experience for both end users and administrators individually to each of the components of SAP BusinessObjects AC 5.3.

As SAP BusinessObjects AC 5.3 is deployed on the JAVA engine of Web AS, most of the configurations for SSO are the same as required for the underlying J2EE engine.

This document describes the options that are available in SAP BusinessObjects AC through which Single Sign-On can be configured for SAP BusinessObjects applications.

To do so, please ensure that the System Landscape should be configured for Single Sign-On and should have SAP BusinessObjects AC 5.3 installed on the J2EE engine.

3. Setting up Single Sign-On for SAP BusinessObjects AC 5.3

SAP BusinessObjects AC 5.3 application leverages the technical infrastructure of SAP NetWeaver. Hence for Single Sign-On to work for SAP BusinessObjects applications, Single Sign-On needs to be configured for the underlying J2EE engine.

The Web AS (also referred to as the J2EE Engine) implements the Java Authentication and Authorization Service (JAAS) standard to support various authentication methods. SAP BusinessObjects AC capabilities utilize UME to authenticate users.

**Portal Authentication:**

As portal runs on the J2EE Engine, so it supports the same authentication mechanisms and the configuration steps are the same as for the underlying J2EE Engine.

To log on to the portal, users must enter in the browser the full URL including the fully qualified domain name; otherwise the browser will not get the correct logon ticket. If the portal is running in the intranet only, you can configure your Web server to change a host name to a full URL.

3.1 Single Sign-On with SAP BusinessObjects AC in a Portal environment:

In most organizations, SAP NetWeaver Portal formerly known as Enterprise Portal (EP) is the single point of access for all users. The SAP BusinessObjects AC application can be completely integrated into SAP EP by creating iViews for SAP BusinessObjects AC capabilities in SAP EP.

**Authentication in Portal:**

Single Sign-On (SSO) is a key feature of the SAP NetWeaver Portal that eases user interaction with the component systems available to the user in a portal environment.
A user is granted access to the portal only after that user’s identity is verified against the Portal authentication mechanism. Once the user has been authenticated, he is issued an SAP logon ticket that allows him to access all the other applications, information and services in SAP NetWeaver Portal for which he is authorized using Single Sign-On.

The SAP logon ticket itself is stored as a cookie on the client and is sent with each request of that client. It can then be used by external applications, such as SAP systems, to authenticate the portal user to those external applications without any further user logons being required.

With Single Sign-On configured in the portal, the user can access different systems and applications without having to repeatedly enter his or her user information for authentication. SAP BusinessObjects AC application can also be configured for Single Sign-On with Log On tickets.

The SAP Enterprise Portal (or SAP EP) and the SAP BusinessObjects AC application can run on the same system or different systems depending on the landscape of the organization. The configurations required to configure Single Sign-On when SAP BusinessObjects AC and Portal reside on the same server are different from the configurations required when they are on different servers. Usually, Compliant User Provisioning (CUP) needs to be integrated with SAP EP so we will consider CUP as an example to explain the steps required for Single Sign-On. The same procedure would be true for all the other capabilities of SAP BusinessObjects AC, as well.

- **SSO will work for SAP BusinessObjects AC in an Enterprise Portal environment only when the authentication source and the user data source for SAP BusinessObjects AC applications are set to SAP UME. Users should also be assigned default roles in UME (Portal Authentication mechanism) to access the SAP BusinessObjects AC applications.**

### 3.1.1 Access Control and Portal on same server

If Access Control and SAP EP applications are residing on the same system, i.e. on the same J2EE server, then no configuration is required and, by default, all four capabilities of Access Control (integrated with SAP EP by creating iViews) will accept SAP EP’s user credentials and allow SSO.

- **Please refer** [SAP Help Portal](https://help.sap.com) **for more information on creating iViews in SAP EP.**

### 3.1.2 Access Control and Portal on different servers

If you have Access Control and SAP EP applications residing on different servers but both are in the same domain then here are the steps to configure SSO for AC applications for example CUP and SAP EP.

You can also configure all the other capabilities of Access Control Suite (e.g. RAR, ERM) by following the steps provided below:

**Enterprise Portal SSO mechanism**

Enterprise Portal SSO mechanism supports the following two variants depending on security requirements and the supported external applications:

- **SSO with SAP logon tickets**
- **SSO with user ID and password**
Both the variants eliminate the need for repeated logons to individual applications after the initial authentication at the Enterprise Portal whereas SSO with SAP logon tickets is based on a secure ticketing mechanism and hence we use this for achieving SSO with Compliant User Provisioning application.

SSO with user ID and password, on the other hand, forwards the user’s logon data (user ID and password) to the systems that a user wants to call.

**SSO with SAP Logon Tickets:**

**Configuring Portal Server for SSO with SAP Logon Tickets:**

The portal is the ticket-issuing system and by default, it is set up so that the underlying J2EE Engine issues SAP logon tickets. Therefore, you do not need to make any settings on the portal server.

**Configuring the CUP Capability’s J2EE Engine to Accept Logon Tickets:**

Step 1: Export the ticket-issuing server’s public-key certificate.

a. The server’s public-key certificate would be available in the Keystore View. Go to System Administration → System Configuration → Keystore Administration to download this certificate.

b. The certificate is the verify.der file in the file system. (See the screenshot below.)

c. Download the verify.der file.

d. Rename the file and change the extension of this file to "crt" (This step is optional.)

Step 2: Go to the visual admin tool of the J2EE engine which is supposed to accept the download certificate.

a. Import the certificate into the TicketKeystore view on the accepting J2EE Engine using the Key Storage service on the accepting server (see the screenshots below)
b. Select the *TicketKeystore* view.

c. Choose *Load*.

d. Select the file from the file system and choose *OK*.
e. The certificate is stored in the selected view as a CERTIFICATE entry.

f. The contents of the certificate can be viewed.
Step 3: Now, maintain the logon ticket access control list in the options for the login module EvaluateTicketLoginModule (or EvaluateAssertionTicketLoginModule):

- Using the Security Provider service, choose the User Management tab.
- Choose Manage Security Stores.
- Make sure the UME User Store is selected as the User Store.
- The Login modules shown in the screenshot are delivered for verifying logon tickets with the UME. Select the EvaluateTicketLoginModule (or EvaluateAssertionTicketLoginModule) entry and choose View / Change Properties.
e. Under **Options**, make entries for each ticket-issuing server from which the J2EE Engine should accept logon tickets as shown in the following screenshots.
f. Make note of the server’s Distinguished Name ([DN]) and the issuer’s Distinguished Name ([IssuerDN]). We need these two Distinguished Names for the access control list (ACL) entries.

g. Login Module Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>trustedsys&lt;x&gt;</td>
<td>&lt;SID&gt;, &lt;Client&gt;</td>
</tr>
<tr>
<td>trustediss&lt;x&gt;</td>
<td>&lt;Issuer’s Distinguished_Name&gt;</td>
</tr>
<tr>
<td></td>
<td>Distinguished Name of the issuer of the ticket-issuing system’s public-key certificate.</td>
</tr>
<tr>
<td>trusteddn&lt;x&gt;</td>
<td>&lt;System’s Distinguished_Name&gt;</td>
</tr>
<tr>
<td></td>
<td>Distinguished Name of the ticket-issuing system.</td>
</tr>
<tr>
<td></td>
<td>If the ticket-issuing system uses a self-signed certificate, then these two Distinguished Names are identical.</td>
</tr>
<tr>
<td></td>
<td>Also, the corresponding public-key certificate must exist in the SAPLogonTicket keystore view entry.</td>
</tr>
<tr>
<td>ume.configuration.active</td>
<td>true</td>
</tr>
</tbody>
</table>
Step 4: Check the login module stack for the ticket template (or any other applications that use the EvaluateTicketLoginModule).

- In the Security Provider service, choose Policy Configurations
- Position the login module at the top of the stack. Specify the Flag **SUFFICIENT**.

Creating iViews and roles:

- Now create a URL iView for the Compliant User Provisioning capability of the Access Control Suite on NetWeaver Portal and assign a role to it.
- Whenever we assign this role to some user, he will be able to see Compliant User Provisioning on EP and SSO will be enabled.

3.1.3 SSO Wizard

For configuring Single Sign On with SAP Logon tickets, SSO2 Wizard has been integrated with Netweaver Administrator for the following SP:

- For AS Java 640: SP 21
- For AS Java 700: SP 14
For AS Java lower than the above mentioned Support Pack levels, you need to deploy the following SDAs on the accepting system:
1. tc-sec-auth-jmx-ear.sda
2. tc-sec-auth-sso2-wizard.sda

and the following SDA on the ticket issuing system:
1. tc-sec-auth-jmx-ear.sda

Note: You will find these files attached in SAP Note Number: 1083421

Integration of SSO2 wizard makes it easier to configure and troubleshoot Single Sign On

When deployed, SSO2 wizard is accessible at:

http(s)://<host>:<port>/sso2

Please refer the SSO2_wizard.pdf attached in SAP Note: 1083421 for more detailed steps on how to configure Single Sign On using SSO wizard.

### 3.1.4 Troubleshooting

- Make sure that the user ID which is being used to log on exists on both the systems, i.e. in the UME of Compliant User Provisioning and EP.
- While creating the URL iView, make sure to give the fully qualified domain name of the Compliant User Provisioning capability.
- While accessing the portal application, use the fully qualified domain name.

⚠️ If you Log Off from CUP, then the SSO session will expire and you will have to open a new session for Portal to access CUP with SSO. If you will try to access CUP in the same session, then it will prompt for user id/password.

⚠️ You can also configure all the other capabilities of the Access Control Suite, (Risk Analysis and Remediation, Enterprise Role Management and Superuser Privilege Management) by following the steps provided above.

### 3.2 SSL and X.509 Client Certificates

An X.509 Client Certificate is a digital "Identification Card" for use in a multiple application environment.

A user who accesses the SAP NetWeaver Application Server and presents a valid certificate is authenticated on the server using the SSL protocol. The information contained in the certificate is passed to the server and the user is logged on to the server based on this information. User authentication takes place in the underlying protocols and no user ID and password entries are necessary.

Users need to receive their client certificates from a Certification Authority (CA) as part of a public-key infrastructure (PKI). If you do not have an established PKI, then you can alternatively use a Trust Center Service to obtain certificates. The CA you choose to use must be designated as a trusted CA on the Web server.
When using client certificates for user authentication, the user is re-authenticated with each request using the SSL protocol. However, no user intervention is necessary, which provides for a Single Sign-On environment for the end user.

Once you have SAP NetWeaver AS JAVA configured for Single Sign-On as per the SSL Protocol, SAP BusinessObjects AC will also work with this Single Sign-On as long as the authentication mechanism being used for SAP BusinessObjects AC is SAP UME.

### 3.3 Suppressing email Notifications with Passwords

Some organizations with SSO implemented may have passwords disabled in their environment. However, CUP sends passwords through email at the time of provisioning when a user ID is created in a target backend system and during password self service. There is presently no configuration in CUP for disabling this notification. To do so, please follow the steps below:

1. In the Initial System data for AC 5.3 CUP, you will find the `AE_init_clean_and_insert_data.xml` file. Make a backup copy of this file.
2. Open the `AE_init_clean_and_insert_data.xml` file in edit mode with a text editor that supports the UTF-8 characters.
3. Search for the following messages, one after another.
   - 1034, 1035, 1032, 1033, 1201, 1202, 1203
   - Example: Search term: MSGCODE="1034"
4. Delete the entire line.
   - Example line:
   ```xml
   <VIRSA_AE_MESSAGE MSGCODE="1034" MSGLOCALE="en" MSGTYPE="success" MSGDESC="This is to inform you that your password has been reset. Your ID:#{IPWD_RESET_USER_ID}! Your password in each system (Password/System):#{IPWD_RESET_USER_PASSWORD}!"/>
   ```
5) Repeat Steps 3 and 4 for each message code mentioned in step 3.

⚠ Please note that it is recommended that you delete these messages in all languages.

6) Search MSGCODE="2204". The contents of this message are:

   MSGDESC="Password reset for the system(s): #_!PSWD_RESET_SYSTEMS#_!, a notification email with new password has been sent to:#_!PSWD_RESET_EMAILS#_!".

7) Modify the message contents to suit the requirement, as this may be confusing to the user, because he/she will not receive any email as a result of this suppression process.

8) Save the file in UTF-8 format.

9) Import the modified file in “Clean and Insert” mode using Initial System Data Feature.

10) If you want to resume the email notifications, import the original AE_init_clean_and_insert_data.xml file.

⚠ Please refer to SAP Note: 12537270 for updated information on the script for suppressing emails in CUP.

⚠ Whenever CUP is upgraded, you will receive the new Initial data files with the upgrade package. Edit the “AE_init_clean_and_insert_data.xml” file, as per the SAP Note 1253720, and apply it as part of the post installation steps.

### 3.4 Kerberos based authentication with SPNEGO

Kerberos Single Sign-On (SSO) is a secure method of logging on to the SAP system that simplifies the logon procedure. It is suitable if you use Windows 2000 or later in your system landscape.

When your system is configured for SSO, an authorized user who has logged on to Windows can access an SAP system (Java or ABAP) directly. There is no need to enter a user ID and password every time that the user logs on to the SAP system. Therefore, SSO makes it easier for you to manage SAP system users.

The Microsoft Kerberos Security Service Provider (SSP) provides secure authentication plus encryption of the network communication.

**SSO in an SPNEGO Environment**

SAP NetWeaver supports Windows authentication. This allows users to achieve SSO to SAP BusinessObjects AC after logging into their machine. In this scenario, successful authentication to the NetWeaver Portal occurs via the SPNEGO protocol. After NetWeaver Portal authentication, an SAP logon ticket is created for SSO to SAP BusinessObjects AC.

⚠ RAR and SPM capabilities of SAP BusinessObjects Access Control would leverage SPNEGO for SSO and no additional configurations are required.
For CUP and ERM applications to leverage SSO with SPNEGO, the redirect application has to be deployed on the J2EE Engine and a redirect URL should be used to access these applications.

Perform the following steps below to configure CUP (and ERM) to retrieve the ticket from SPNEGO and for SSO to work for CUP (and ERM).

1) Deploy the redirect application which forwards the SPNEGO ticket and redirects the ticket to CUP capability.

   You may get the **redirect.ear** file from support by creating an OSS message.

   Deployment can be done using NetWeaver SDM.

2) After successful deployment, log into **NetWeaver Visual Administrator** as an administrator.
   
   a. Click on the **Cluster** tab on the left panel.
   b. Expand the tree node ‘Server’.
   c. Expand the tree node ‘Services’.
   d. Select the ‘Security Provider’ service.
   e. On the right panel, select the ‘Runtime’ tab.
   f. Select the **Policy Configurations tab** under the ‘Runtime’ tab.
   g. Select the **Redirect** application from the component tree.
   h. On the right panel select the ‘Security Roles’ tab.
   i. Select the ‘Default Security Role’ from Security Roles list box.
   j. Add the group ‘Everyone’ to the ‘Groups’ List box.

Here is the screenshot of the above mentioned settings in Visual Administrator:
3) For the redirect application to pass SSO credentials to the SAP BusinessObjects AC application, access the SAP BusinessObjects AC capabilities using the following link:

https://<server_name>:5<instance>01/RedirectApp/?redirecturl=<put the Access Control URL* here >.

- The Access Control URL* to be inserted in the above mentioned link is the URL for CUP or ERM applications.
- Please refer SAP Note 1252589 for more updated details on configuration of SSO in SPNEGO set up.

### 3.4.1 How to achieve SSO for email links

CUP sends email notifications containing links to the application. After clicking on these links, the user is prompted for User ID / password to enter into the CUP capability. In a typical SPNEGO set up, this could be an undesirable scenario.

Users will be presented with an authentication form, prompting for the SAP BusinessObjects CUP User ID/ password because the proper prefix is not generated for system generated emails. In order to ensure that email links sent to users in CUP notifications function properly in an SPNEGO setup, please apply the script described below.

Make sure that the system generated emails are properly prefixed with the redirectURL.

Update the configuration with the URL to be prefixed in email links using the following script:

```sql
UPDATE VIRSA_AE_ERMCONFIG SET PARAMVALUE = 
'https://<server_name>:<port>/RedirectApp/?redirectURL= < put the Access Control URL* here >'
WHERE PARAM = '128'
```

- The Access Control URL* to be inserted in the above mentioned link is the URL for CUP application.
Make sure to modify the server name and port number to the correct server name and port number where the redirect application is deployed.

If SSO does not work with these configurations then, refresh the cache and restart the server.

### 3.4.2 Single Sign-On with multiple LDAPs as authentication

In an SPNEGO environment where multiple LDAPs are being used as the authentication mechanism, Single Sign-On can be implemented for SAP BusinessObjects Access Control by making changes to UME.

⚠️ This can only be done when UME is enabled for the use of multiple LDAP.

The code changes that need to be made to the "dataSourceConfiguration_ads_deep_readonly_db.xml" file to configure UME for multiple LDAPs are:

```xml
<ume.ldap.access.server_name>SERVER_HOSTNAME</ume.ldap.access.server_name>
<ume.ldap.access.server_port>SERVER_PORT</ume.ldap.access.server_port>
<ume.ldap.access.user>DS_USER_NAME</ume.ldap.access.user>
<ume.ldap.access.password>DS_PASSWORD</ume.ldap.access.password>
<ume.ldap.access.base_path.user>USER_ROOT_IN_DS</ume.ldap.access.base_path.user>
<ume.ldap.access.base_path.grup>GROUP_ROOT_IN_DS</ume.ldap.access.base_path.grup>
```

⚠️ Refer to SAP Notes 673824, 718383, and 736471 for updated information on configuring multiple LDAPs for UME.

⚠️ You may download the "dataSourceConfiguration_ads_deep_readonly_db.xml" file from the Configuration option in UME.

### 4. Related SAP Notes

Here are some of the related SAP Notes.

- 1253720 Compliant User Provisioning 5.3 Suppressing Password Emails
- 1252589 Compliant User Provisioning 5.3 – Redirection URL for SSO
- 994791 SPNEGO Wizard
- 701205 Single Sign-On using SAP Log On Tickets
- 968191 SPNEGO Central Note
- 138498 Single Sign-On Solutions
- 1083421 SSO2 Wizard
5. Further Reading

- SSO FAQs
- Authentication and Single Sign-On
- Integration of GRC AC 5.3 and EP
- Integration of Training and Verification System with CUP
- AC Accelerators
- SDN/BPX

6. Comments and Feedback

Please send your comments and feedback on grc_rig@sap.com.