Integration of SAP BI 7.0 and SAP EP 7.0

Applies to:
SAP Enterprise Portal 7.0, SAP Business Intelligence 7.0

Summary
I have seen many people are searching for the Information in SDN about Integration of SAP EP 7.0 and SAP BI 7.0. So this blog is dedicated for them.

A number of settings need to be made in the BI system and SAP EP. Some settings depend on one another, and to achieve this, follow the given sequence when you maintain settings in the BI system and in the portal.

The portal communicates with BI using the Web protocol http or https. Communication is established based on the system object in the portal. BI uses an RFC connection to communicate with the portal. The portal is the RFC server and BI is the RFC client.

Author: Karthick Eswaran
Company: Satyam Computer Services ltd.
Created on: 28 November 2007

Author Bio
Karthick has 6+ of experience in IT industry of which 3 years in SAP NetWeaver Technologies. He has two plus years of domain expertise in Oil and Gas.

Worked extensively in SAP NetWeaver Administration and well versed with SAP EP 6.0 (NW04), EP 7.0 (NW04s) and SAP WebDynpro for Java applications.

Currently associated with Satyam Computer Services as a SAP Basis Administrator.
Table of Contents

Prerequisites ................................................................................................................................................. 3
Sequence of Steps .......................................................................................................................................... 3

Step 1: Create RFC Destination in J2EE Engine ...................................................................................... 4
Step 2: Create RFC Destination for the Portal .......................................................................................... 5
Step 3: Maintain Portal Server Settings for the Portal ............................................................................... 7
Step 4: Maintain Single Sign-On in the BI System .................................................................................... 8
Step 5: Export BI Certificate to the BI System .......................................................................................... 9
Step 6: Import BW Certificate to the Portal ............................................................................................. 10
Step 7: Create BI System in the Portal .................................................................................................... 12
Step 8: Configure User Management in the Portal .................................................................................. 15
Step 9: Export Portal Certificate to the Portal ........................................................................................ 16

Importing the Portal Certificate to the J2EE Engine .......................................................................... 17
Step 10: Import Portal Certificate to BI System ...................................................................................... 19
Step 11: Set up Repository Manager for BI Documents and BI Metadata ............................................. 21
Step 12: Maintain User Assignment in the Portal .................................................................................... 21
Step 13: Import SAP Basis Plug-In to BI System .................................................................................... 22

Related Content .......................................................................................................................................... 23

Disclaimer and Liability Notice ................................................................................................................... 24
Prerequisites

- BI administrators require authorization for transactions SM59, SMGW, RZ10, STRUSTSSO2, SM30 (table RSPOR_T_PORTAL) and, in some circumstances, STMS.
- Portal Administrators need to have the portal roles super_admin_role and com.sap.ip.bi.business_explorer_showcase assigned to them. They also need to have access to the Portal file system.

Sequence of Steps

SAP recommends that you perform the necessary steps in the following order:

1. Create RFC Destination in J2EE Engine
2. Create RFC Destination for the Portal
3. Maintain Portal Server Settings for the Portal
4. Maintain Single Sign-On in the BI System
5. Export BW Certificate to the BI System
6. Import BW Certificate to the Portal
7. Create BW System in the Portal
8. Configure User Management in the Portal
9. Export Portal Certificate to the Portal
10. Import Portal Certificate to the BI System
11. Set Up Repository Manager for BW in the Portal
12. Maintain User Mapping in the Portal
13. Import SAP Basis Plug-In to the BI System
Step 1: Create RFC Destination in J2EE Engine

Execute the following steps to create an RFC destination in the J2EE Engine:

1. Start the SAP J2EE Engine Administrator with `<PORTAL_DIRECTORY>\admin\go.bat`.
2. Connect to the portal server.
3. Select `<SID>/Server<#>/Services/Jco RFC Provider` from the hierarchy.
4. Maintain an RFC destination:
   - Program ID: `<PORTAL_HOSTNAME>_PORTAL_<SID>`
   - Gateway host: `<GATEWAY_HOST>`
   - Gateway service: `sapgw<SYSTEM_NUMBER>`
   - Number of processes (1..20): 20
   - Application server host: see gateway host
   - System number: `<SYSTEM_NUMBER>`
   - Client: `<BW_MANDANT>`
   - Language: EN
   - User: `<USER>` (user in the BW system)
   - Password: `<PASSWORD>`
5. Copy the RFC destination to the available RFC destinations by choosing Set.
6. Start the RFC server by choosing Start.

** Gateway Host has to be name of server
Step 2: Create RFC Destination for the Portal

In this activity you create an RFC destination for the integration of a BI system and portal. You can specify this RFC destination in the activity Maintain Portal Server Settings for the Portal so that the RFC destination is recognized as the connected portal. The BI system uses the RFC destination to communicate with the portal.

Execute the following steps to create an RFC destination for the portal:

1. Start transaction Display and Maintenance of RFC Destinations (transaction code SM59).
2. Choose Create.
3. Maintain the RFC destination:

RFC destination: `<RFCDESTINATION>`: The name of the RFC destination for a portal should be selected carefully. The name of the RFC destination is saved in the settings for information broadcasting. This is necessary so that the portal that is connected and being used for integration with Knowledge Management can be clearly identified. The broadcast settings can be transported between BI systems. For this reason, the name of the RFC destination should be the same in the source system and in the target system. The name recommended by SAP for the RFC destination to the connected portal is `SAP_EP`
Connection type: T for TCP/IP connection

Description: <DESCRIPTION>: You can maintain the description of the RFC destination as language dependent. The language-dependent description is used when publishing iViews from the BEx Web Application Designer and the BEx Query Designer when multiple portals are connected to the BI system.

Technical settings - Activation type: Registered server program

Program ID: <PORTAL_HOSTNAME>_PORTAL_<SID>: The server program is set up under the program ID on the J2EE engine. The recommended naming convention is <PORTAL_HOSTNAME>_PORTAL

Gateway Options: Enter the Gateway host and the Gateway service that the J2EE engine uses to communicate with the BI system. The gateway host, which is an application server for the BI system, and the gateway service can be generated generically from sapgw<SYSTEM_NUMBER>. You can determine the parameters of the gateway in transaction Gateway Monitor (transaction code SMGW) by choosing Goto -> Parameter -> Display.

Send SAP logon ticket: activate: Activate option Send SAP Logon Ticket on the Logon & Security tab page.

Unicode: If the BI system is a Unicode system, you have to activate the Unicode option on the MDMP & Unicode tab page.

Save your entries. If the RFC destination is also set up on the J2EE Engine side you can test the connection by choosing the Test Connection.
Step 3: Maintain Portal Server Settings for the Portal

In this activity you designate a default portal. You can also make settings that are relevant to information broadcasting. If you do not maintain this table, the corresponding menu entries for publishing in the BEx Web Application Designer and BEx Query Designer are deactivated.

Execute the following steps to maintain the portal server settings for the portal:

1. Start table view maintenance (transaction code SM30).
2. Enter RSPOR_T_PORTAL as the table.
3. Choose **Maintain**.
4. Choose **New Entries** to create a new entry.
5. Maintain the connected portal:
   - RFC destination: `<RFC_DESTINATION>`
   - System name: `<SYSTEM_ALIAS>`
   - Default: `<DEFAULT>`
   - Portal-URLprefix: `<PORTAL_URL_PREFIX>`, for example, `http://<portalserver><domain>:<port>`
   - Prefix of RM for BW Metadata: `<KM_RM_METADATA_PREFIX>`, for example, `/bw_metadata`
   - KM service URL: `<blank>`
6. Save your entries.
Step 4: Maintain Single Sign-On in the BI System

In this activity you maintain Single-Sign-On settings in the BI system.

Execute the following steps to maintain the necessary settings for Single Sign-On in the BI system:

1. To use Single Sign-On (SSO), install SAPSECULIB on every application server for the BI system. It is not necessary to install SSO software on the client PC.

2. Use the maintain profile transaction (transaction RZ10) to set the following profile parameter:

   **login/create_sso2_ticket=2**: The profile parameter generates SSO tickets in the BI system. These are required for the communication between the BI system and the portal. The value 2 indicates that the certificate is self signed.

   **login/accept_sso2_ticket=1**: The profile parameter means that the BI system SSO ticket is accepted by other systems (for example, the portal) when the appropriate certificate is imported (see, Importing Portal Certificates).
Step 5: Export BI Certificate to the BI System

Export Path and Export File Name: The BI certificate is saved under the specified path and file name and can then be imported into the portal. In this activity, you export the BI certificate from the BI system.

Execute the following steps in order to export the BI certificate to the BI system:


2. Select your own certificate. Your certificate is located in the system PSE area in the Your Certificate field. You display the certificate in the certificate area by double clicking on the field value.

   If you have not already created your own certificate, create one by choosing Create from the context menu in the system PSE and distribute it to all application servers for the BI system by choosing PSE -> Distribute. There may be a time delay when you distribute the certificate. If necessary, check more than once that the certificate has been distributed successfully.

3. Choose Certificate -> Export from the menu.

4. Enter file path <BW_SID>_certificate.crt ein (<BW_SID> is the system ID for the BI system).
5. Choose file format \textit{Binary}.

The file $<\text{SID}>_\text{certificate.crt}$ is used for step \textit{Importing BI Certificate} with the settings in the portal.

\textbf{Step 6: Import BW Certificate to the Portal}

In this activity you import the BI certificate into the portal. This is necessary before content from the portal can be displayed in the BI system, for example, before portal roles can be displayed in the BEx Web Application Designer. Before the BI certificate can be imported into the portal, it has to be exported from the BI system.

Perform the following steps to import the BI certificate into the J2EE engine:

1. Start the SAP J2EE Engine Administrator with \texttt{%INSTALLATION_ROOT\%\admin\go.bat}.
2. Connect to the portal server.
3. In the tree, select \texttt{<\text{SID}>/Server<#>/Services/Key Storage}.
4. Under Views, select the \texttt{TicketKeystore} view.
5. Under Entry, click \texttt{Load}.
6. Open the file $<\text{BW_SID}>_\text{certificate.crt}$.

In the \textit{Service Security Provider} under Ticket, perform the following steps to ensure that the SAP J2EE Engine accepts the SAP Logon Tickets from the BI system as an external system.

7. Start the SAP J2EE Engine Administrator with \texttt{%INSTALLATION_ROOT\%\admin\go}.
8. Connect to the portal server.
9. In the tree, choose \texttt{<\text{SID}>/Server<#>/Services/Security Provider}.
10. Under Component, choose Ticket.
11. Choose the \textit{Authentication} tab page.
12. Change the options for \texttt{com.sap.security.core.server.jaas.EvaluateTicketLoginModule} and enter the following values:

- $\text{trustedsys<Number>=<BW_SID>, <BW_CLIENT>}$ (for example, BWP, 000)
- $\text{trustediss<Number>=<ISSUER_DISTRIBUTED_NAME>}$ (z. B. \text{CN= BWP, OU=SAP Web AS, O=SAP Trust Community, C=DE})
- $\text{trusteddn<Number>=<SUBJECT_DISTRIBUTED_NAME>}$ (z. B. \text{CN= BWP, OU=SAP Web AS, O=SAP Trust Community, C=DE})
Explanations:

<Number> is a number for all three entries, but must be incremented by one for every external system.

<BW_SID> and <BW_CLIENT> are the system ID and the client of the BI system.

<ISSUER_DISTINGUISHED_NAME> and <SUBJECT_DISTINGUISHED_NAME> correspond to the Own Certificate value in transaction Trust Manager for Single Sign-On with Logon Ticket (transaction STRUSTSSO2). The value trustediss corresponds to the value Issuer; the value trusteddn corresponds to the value Owner.

In addition, you have to maintain the values under evaluate_assertion_ticket:

1. Start the SAP J2EE Engine Administrator with %INSTALLATION_ROOT%\admin\go.
2. Connect to the portal server.
3. In the tree, choose <SID>/Server<#>/Services/Security Provider.
4. Under Component, choose evaluate_assertion_ticket.
5. Choose the Authentication tab page.
6. Change the options for com.sap.security.core.server.jaas.EvaluateAssertionTicketLoginModule and enter the following values:
   - trustedsys<Number>=<BW_SID>, <BW_CLIENT> (for example, BWP, 000)
   - trustediss<Number>=<ISSUER_DISTINGUISHED_NAME> (z. B. CN= BWP, OU=SAP Web AS, O=SAP Trust Community, C=DE)
   - trusteddn<Number>=<SUBJECT_DISTINGUISHED_NAME> (z. B. CN= BWP, OU=SAP Web AS, O=SAP Trust Community, C=DE)
Step 7: Create BI System in the Portal

Execute the following steps to create a BI system in the portal:

1. Log on to the portal.
2. Start the iView System Administration -> System Configuration -> System Landscape.
3. The systems are maintained with the Portal Content Studio.
4. Choose New -> System from the portal catalog context menu.
5. Choose R/3 with Load Balancing (SAP_R3_LoadBalancing) or Dedicated Application Server for R/3 System (SAP_R3_Dedicated) as the template.
6. Maintain the most important properties with the property category Display All:
   - Logon methods: SAPLOGONTICKET or UIDPW
   - Type of user mapping: admin,user
   - Type of ticket authentication: SAP Assertion Ticket
   - Name of logical system: <SID>CLNT<MANDANT>
   - The recommended convention for logical system names consists of the system ID and client.
   - Remote host type: 3
   - SAP client: <CLIENT>
   - SAP system ID (SID) [R/3 Name]: <SID>
   - System type: SAP_BW
   - System name: <SID>CLNT<CLIENT>
   - WAS description: <DESCRIPTION>
   - WAS host name: <HOSTNAME>:<PORT>
   - WAS path: /sap/bw/bex
   - WAS protocol: http or https
All system information refers to the BI system.

You can determine the WAS host name, WAS path and WAS protocol settings using function module RSBB_URL_PREFIX_GET(transaction code SE37).
You must also maintain the following BI properties for SAP NetWeaver 2004s:

- **BI Directory Provider: true**
- If the indicator is set, the BI system is displayed in open dialog when selecting queries or InfoProviders. This property is usually activated.
- **BI Documents for InfoProvider**: `<KM_REPOSITORY_PATH>`
- **BI Documents for Master Data**: `<KM_REPOSITORY_PATH>`
- **BI Documents for Metadata**: `<KM_REPOSITORY_PATH>`
- The properties *BI Documents for InfoProvider, master data and metadata* contain the paths to Knowledge Management
- **BI Master System: true**
  - The property *BI Master System* means that the BI system is the central persistence storage for the portal. The BI master system is used to read and execute Web templates. The running BI Web runtime requires exactly one BI master system within a portal.

**Report** *Maintain Settings for Integration into the Portal* (RSPOR_SETUP) determines most of the mandatory values for the above properties automatically.

1. In the *System Aliases* view, maintain an alias for the system.
2. Save your entries.
Step 8: Configure User Management in the Portal

In this activity you configure user management for the portal.

In portal user management, some settings are necessary in order to support Single Sign-On between the BI system and the portal. The SAP reference system is required for the communication of the BEx tools in the portal.

The login.ticket_client parameter only has to be maintained if more than one portal is connected and these portals have the same system ID. Normally however, you should install the portals with different system IDs.

Execute the following steps to configure user management in the portal.

1. Log on to the portal.
2. Start the iView System Administration -> System Configuration -> Configuration for User Management.
4. Under SAP Reference System, enter the system alias of the BW system (see Creating BI Systems in the Portal). The default system alias of the BI system has to be entered.
5. Only one system can be specified as the SAP reference system. The SAP reference system cannot be the BI system. However, as it is not the BI system, the technical user name of the BI system has to be identical to the technical user name of the SAP reference system.
6. Save your entries.

If you want to connect more than one portal to a BI system and these portals have the same system ID, you have to maintain parameter login.ticket_client:

1. Start the SAP J2EE Configuration Tool.
2. Use the standard database settings.

You can choose any value between 000 and 999 as the <CLIENT>. The client is needed if more than one portal is connected and these portals have identical portal SIDs. The client has to be entered when the portal certificate is imported to the BI system.

5. Save your entries.

If changes are made in portal user management, the SAP J2EE has to be restarted with the portal.
**Step 9: Export Portal Certificate to the Portal**

In this activity you export the portal certificate. The portal certificate is required for displaying content from the BI system in the portal and has to be imported after the export to the BW system.

**Execute the following steps to export the portal certificate from the J2EE Engine:**

1. Start the SAP J2EE Engine Administrator with `<PORTAL_DIRECTORY>\admin\go.bat.`
2. Connect to the Portal Server.
3. Select `<SID>/Server<#>/Services/Key Storage` from the hierarchy.
4. Under Views, select the `TicketKeystore` view.
5. If SAPLogonTicketKeypair-cert is not available under Entries, generate a portal certificate as instructed in the following steps. Otherwise you can continue with the export from step 9.
6. Choose Create under Entry. Enter the following values for Key and Certificate Generation:
   - Subject Properties: Each key has to have one value under Value.
   - The value CN=Common Name is the first value that is displayed in transaction STRUSTSSO2. Therefore it can be seen as the name of the certificate. The recommendation `<HOSTNAME_PORT>` from the portal server is also valid.
   - Entry Name: SAPLogonTicketKeypair (the entry SAPLogonTicketKeypair-cert is generated automatically)
   - Store Certificate: X
   - Algorithm: DSA
7. Choose Generate to generate the certificate.
10. Export the portal certificate as `<PORTAL_SID>_certificate.crt` in file format X.509 certificate (*.crt).
Importing the Portal Certificate to the J2EE Engine

1. Start the SAP J2EE Engine Administrator with %INSTALLATION_ROOT%\admin\go.bat.
2. Connect to the portal server.
3. Choose <SID> → Server<#> → Services → Key → Storage.
4. iViews: Select the view TicketKeystore.
5. Entry: Choose Load.
6. Open the file <PORTAL_SID>_certificate.crt.

In the Service Security Provider, under Ticket, perform the following steps to ensure that the SAP J2EE Engine accepts SAP logon tickets from the SAP NetWeaver 2004s portal as an external system.

7. Start the SAP J2EE Engine Administrator with %INSTALLATION_ROOT%\admin\go.
8. Connect to the portal server.
10. Components: Choose Ticket.
11. Choose the Authentication tab page.
12. Add the following values for com.sap.security.core.server.jaas.EvaluateTicketLoginModule:

   • trustedsys<Number>=<PORTAL_SID>, <PORTAL_CLIENT> (for example, J2E, 000)
   • trustediss<Number>=<ISSUER_DISTINGUISHED_NAME> (for example, CN=J2E)
   • trusteddn<Number>=<SUBJECT_DISTINGUISHED_NAME> (for example, CN=J2E)

   <Number> is an identical number for all three entries, but must be incremented by one for each external system.

   <PORTAL_SID> and <PORTAL_CLIENT> are the system ID and client of the SAP NetWeaver 2004s portal. The client is the value of the parameter login.ticket_client. The default value is 000.

   <ISSUER_DISTINGUISHED_NAME> and <SUBJECT_DISTINGUISHED_NAME> are the values of [issuerDN] and [DN] of certificate SAPLogonTicketKeypair-cert (see above).
You also have to add these values under `evaluate_assertion_ticket`:

13. Start the SAP J2EE Engine Administrator with `%INSTALLATION_ROOT%\admin\go`.
14. Connect to the portal server.
15. Choose `<SID> → Server<#> → Services → Security → Provider`.
17. Choose the `Authentication` tab page.
18. Add the following values for `com.sap.security.core.server.jaas.EvaluateAssertionTicketLoginModule`:

   - `trustedsys<Number>=<PORTAL_SID>, <PORTAL_CLIENT>` (for example, J2E, 000)
   - `trustediss<Number>=<ISSUER_DISTINGUISHED_NAME>` (for example, CN= J2E)
   - `trusteddn<Number>=<SUBJECT_DISTINGUISHED_NAME>` (for example, CN=J2E)

The values are the same as the above values under `Ticket`. 
Step 10: Import Portal Certificate to BI System

Firstly export the verify.der file as shown below and extract certificate from the same.

In this activity you import the portal certificate. You need this setting to call content from the BI system in the portal. Execute the following steps to import the portal certificate into the BI system:

1. In transaction STRUSTSSO2, choose Certificate -> Import and import file `<PORTAL_SID>_certificate.crt` in binary format.
2. To include the certificate in the SSO Access Control List (ACL), choose Edit -> Certificate in ACL from the menu.

With the portal, you can specify the portal system ID as the system and the value of parameter logon.ticket_client as the client. (see step Configuring User Management in the Portal). If the logon.ticket_client parameter is not maintained, you can use client 000.

The system ID for the portal is determined when you install the portal and can be found in portal file path: #/<PORTAL_SID>/JC<Instance Number>/j2ee/cluster/server<Number>/#

3. To include the certificate in the list of certificates, choose Edit -> Include Certificate from the menu.

4. If you want to distribute the settings for more than one application server, choose Distribute from the context menu for the tree on the left-hand side of the screen.

There may be a time delay when you distribute the certificate. If necessary, check more than once that the certificate has been distributed successfully.

5. Save your entries.

When changes are made in user management in the portal, a new certificate may have to be generated and imported into the BI system. The portal certificate is generated automatically when the J2EE server is restarted and can then be exported again.
Step 11: Set up Repository Manager for BI Documents and BI Metadata

In this activity you can set up the BI Document and BI Metadata Repository Manager.

Execute the following steps to set up a Repository Manager for BI in the portal:

1. Log on to the portal.
2. Start iView System Administration -> System Configuration -> Knowledge Management -> Content Management.
5. Create a new instance of the BI Document Repository.
6. Enter the most important settings:
   - Name: Unique name of Repository Manager
   - Prefix (must start with /): <BI_DOCUMENT_PREFIX> (for example, /bi_documents)
   - Active: X
   - Security Manager: BWDocumentSecurityManager
7. Choose OK to save the settings.
8. Under Classes, choose BI Metadata Repository.
9. Create a new instance of the BI Metadata Repository.
10. Enter the most important settings:
    - Name: Unique name of Repository Manager
    - Prefix (must start with /): <BI_META_DATA_PREFIX> (for example, /bi_metadata)
    - Active: X
    - Security Manager: BIMetadataSecurityManager
11. Choose OK to save the settings.

Step 12: Maintain User Assignment in the Portal

In this activity you assign a user in the BI system to a user in the portal.

Ensure that all users have at least read access to the BI system created in step 7. Start the iView System Administration -> System Configuration -> System Landscape. Navigate to the system you have created, open the context menu and choose Open -> Authorizations. Search by user, user group or role, add these and allocate the authorization Read.

Execute the following steps to maintain user mapping in the portal:

1. Logon to the portal.
3. Choose User from the dropdown box.
4. Enter a user or choose Start for all users.
5. Choose Start.
6. Choose a user and choose Edit.
7. Choose the system alias of the BI system (see step Creating BI Systems in the Portal).
8. Enter the technical user name in the BI system.
9. Enter the password.
10. Save your entries.
Step 13: Import SAP Basis Plug-In to BI System

In this activity you import the SAP Basis Plug-In into the BI system.

The SAP Basis Plug-In (PI_BASIS) is required for the integration of the BI system and the portal.

Execute the following steps to import the SAP Basis Plug-In into the BI system:

1. Download the SAP Basis Plug-In (PI_BASIS) from http://service.sap.com/swdc.
2. Start the Transport Management System (transaction code STMS).
3. Import the SAP Basis Plug-In into the BI system.

Check

You can perform a check when you load BI roles into the portal.
Related Content

Please include at least three references to SDN documents or web pages.

- [http://help.sap.com/saphelp_nw04/helpdata/en/7f/5bfc3f8fc2c542e10000000a1550b0/frameset.htm](http://help.sap.com/saphelp_nw04/helpdata/en/7f/5bfc3f8fc2c542e10000000a1550b0/frameset.htm)
Disclaimer and Liability Notice

This document may discuss sample coding or other information that does not include SAP official interfaces and therefore is not supported by SAP. Changes made based on this information are not supported and can be overwritten during an upgrade.

SAP will not be held liable for any damages caused by using or misusing the information, code or methods suggested in this document, and anyone using these methods does so at his/her own risk.

SAP offers no guarantees and assumes no responsibility or liability of any type with respect to the content of this technical article or code sample, including any liability resulting from incompatibility between the content within this document and the materials and services offered by SAP. You agree that you will not hold, or seek to hold, SAP responsible or liable with respect to the content of this document.