

Single Sign-On Configuration



Applies to:

SAP NetWeaver Application Server, SAP NetWeaver Portal

For more information, visit the [Security homepage](#).

Summary

Single Sign-On (SSO) is a key feature of the SAP NetWeaver Portal that eases user interaction with the many component systems available to the user in a portal environment. This guide will give you step-by-step instructions in configuring Single Sign-On with the SAP NetWeaver Portal to the SAP Systems and vice versa. Single Sign-On uses SAP Logon Tickets and helps streamline the user logon process while implementing strong security settings for the systems and network.

Author: Karthik Vodela

Company: DELOITTE

Created on: 01 January 2009

Author Bio



SAP Basis Consultant with 2 years of consulting experience. Involved in different SAP Projects in Solution Network (SNET) Team in Deloitte. Experience with architecture and infrastructure related to SAP including SAP NetWeaver technologies.

Table of Contents

Section I- SSO from Portal to ABAP	3
1 Export Certificate from Portal System	3
2 Import Portal Certificate into ABAP system	3
3 Creating the system connector in the Portal	4
4 Check Profile Parameters in ABAP system	7
5 Test connections in Portal-	7
Section II- SSO from ABAP to Portal and Vice Versa	8
1 Export Certificate from Portal System	8
2 Export / Import Certificates from ABAP system	8
Import Portal Certificate into ABAP system	8
3 Creating the system connector in the Portal	9
5 Check Profile Parameters in ABAP system	12
6 Create a JCo RFC provider in the Portal system.....	13
7 Add ABAP System to Security providers list in Portal	14
8 Import ABAP system certificate to J2EE of portal system	15
9 Create RFC connection in the ABAP system to Portal	16
10 Maintain Portal Server Settings in ABAP	16
11 Test connections between ABAP and Portal system.....	17
Related Content	19
Disclaimer and Liability Notice	20

Section I- SSO from Portal to ABAP

1 Export Certificate from Portal System

1. Logon to the Portal and Navigate to below path
2. Go to *System Administration* → *System Configuration* → *Keystore Administration*

SAP NetWeaver Portal	<i>System Administration</i> → <i>System Configuration</i> → <i>Keystore Administration</i>
-----------------------------	---

3. Select *SAPLogonTicketKeypair-cert* from the drop list menu (default)
4. Choose Download verify.der

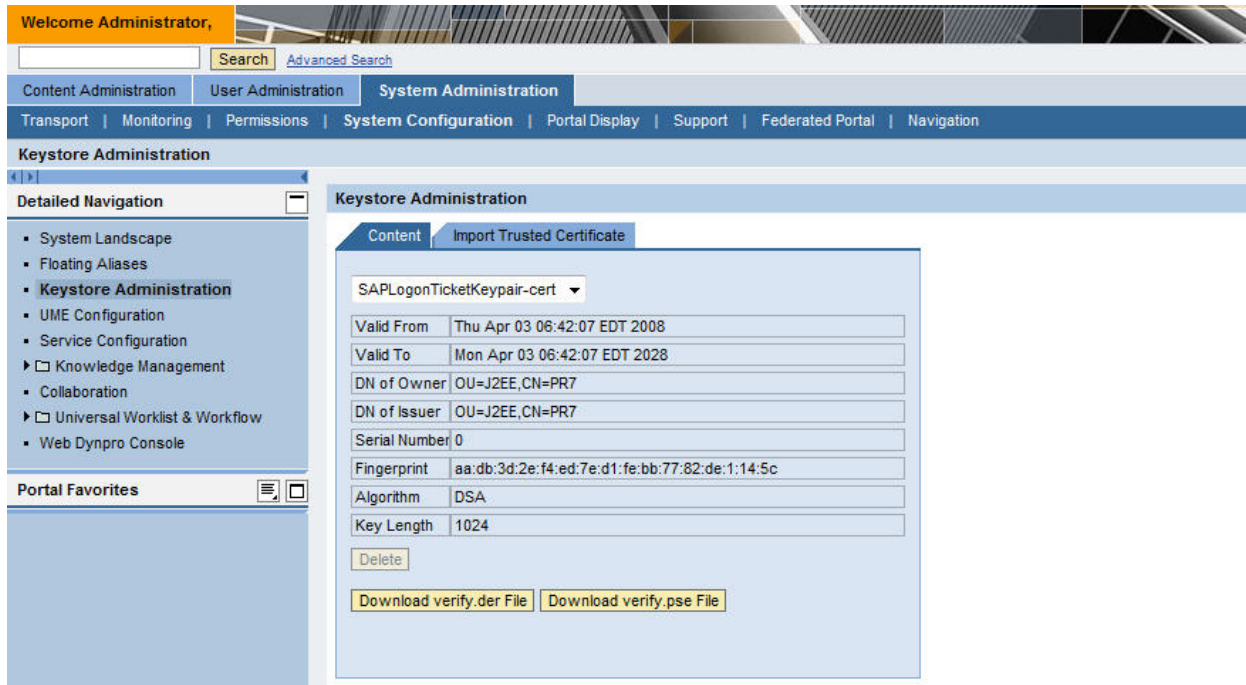


Figure 1 - *SAPLogonTicketKeypair-cert*

5. Save file to a folder on your hard drive (ex: D:\Best_Practices\verify.der.zip)
6. Extract the zip file and save the *verify.der* file to the hard drive (i.e. D:\Best_Practices\verify.der)

2 Import Portal Certificate into ABAP system

1. Logon to client 000 of ABAP system
2. Execute transaction '**STRUSTSSO2**'
3. Choose *Import certificate* button in the Certificate section.
Note: Choose binary as the format in the dialog box 'import certificate'
4. Choose the *Browse* button in the *File path* text field and select the *verify.der* you exported from the portal.
5. Choose *OK* button.
6. Choose *Add to Certificate List* button
7. Choose *Add to ACL* button
8. Add the *Portal Instance* name to the *System ID* text field.
9. Add **000** to the *Client* text field.
10. Choose *OK* button.
11. Choose *Save*.

3 Creating the system connector in the Portal

1. Log on to the Portal with a user id that has administrator rights.
2. Follow the menu path: System Administration → System Configuration → System Landscape → Portal Content. Click the arrow next to **Portal Content** as shown in Figure2.

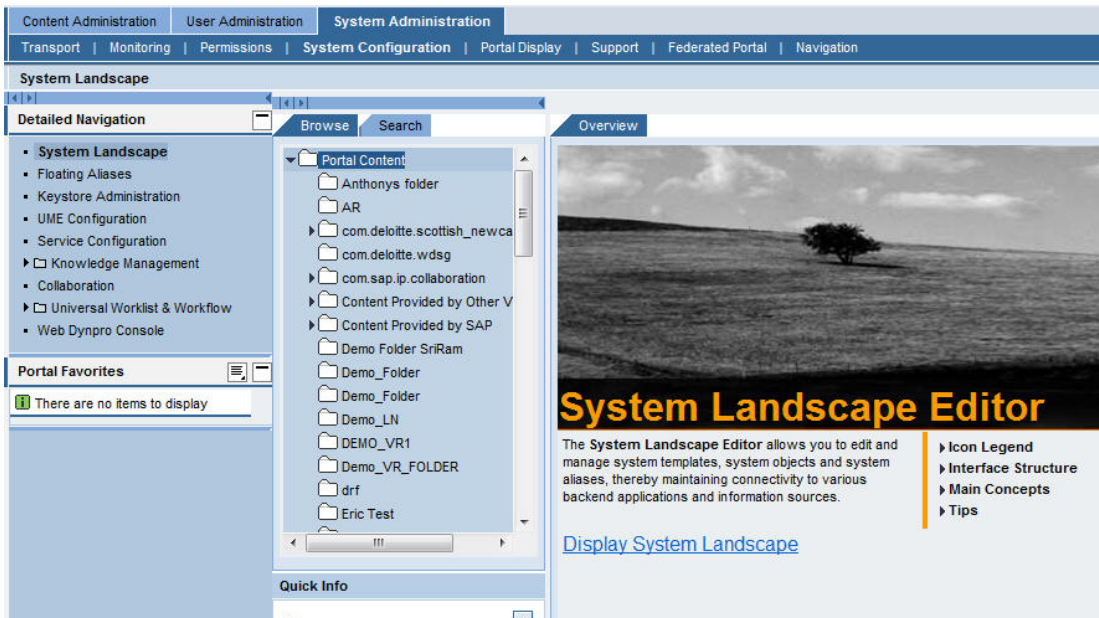


Figure 2 – System Landscape Editor

3. Under Portal Content, right-click on the Systems folder. Select **New** → **System** (from template) as shown in Figure 3.

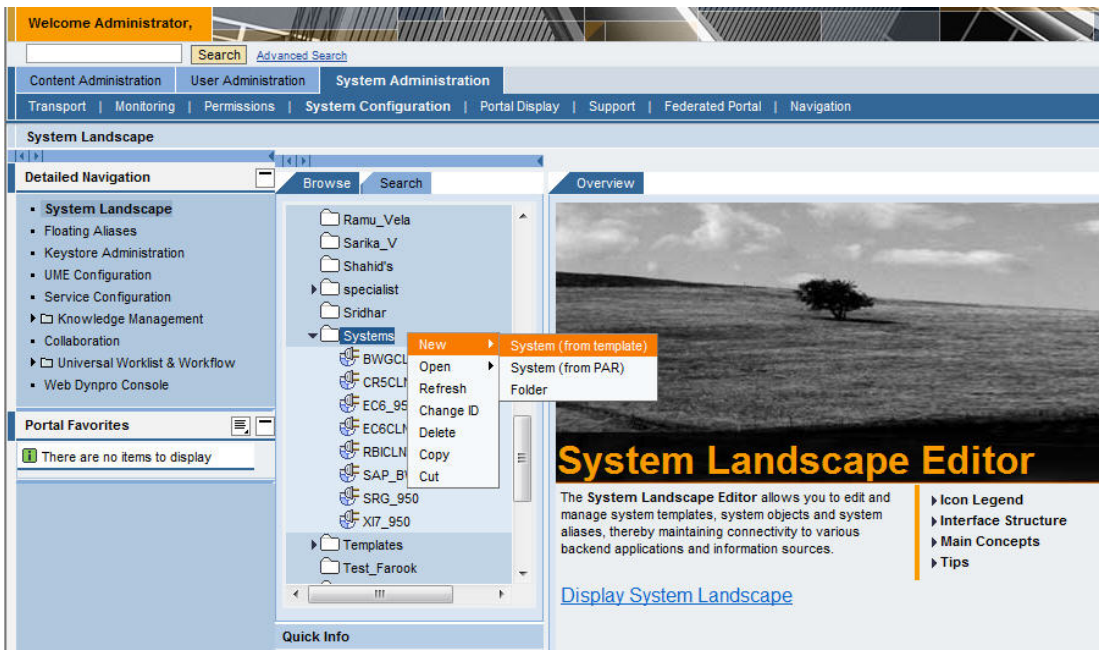


Figure 3 – Selecting the system folder

4. As shown in Figure 4, click **SAP system using dedicated application server**. Click **Next** to continue.

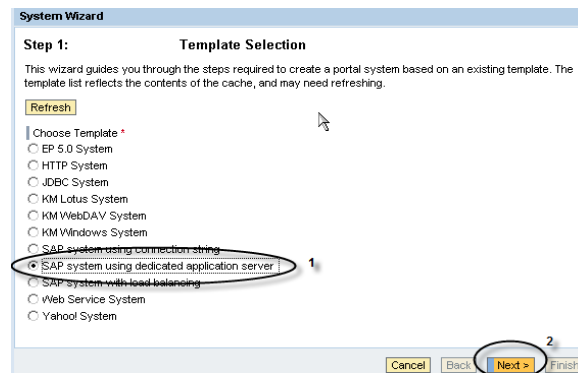


Figure 4 Selecting the template

5. As shown in Figure 5, enter the **System Name**, **System ID**, and **System ID Prefix**. Select a **Master Language** and enter a **Description**. Click **Next** to continue.

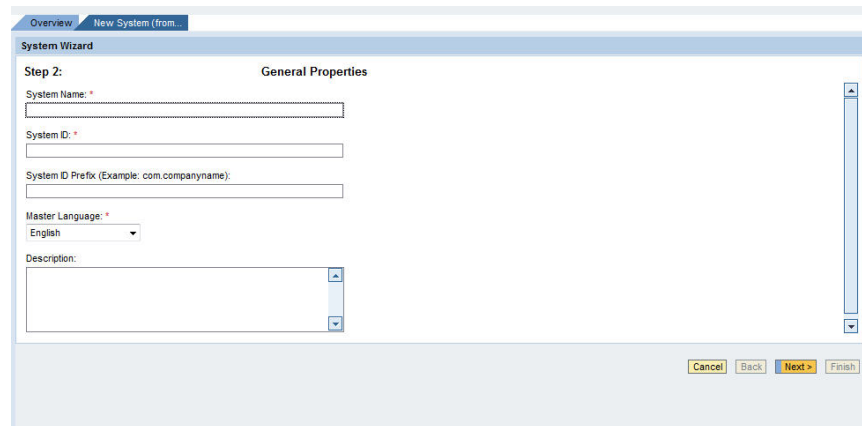


Figure 5 – Entering general properties

6. A summary screen appears. Click **Finish**.
 7. As shown in Figure 6, click **Open the object for editing**. Click **OK**.

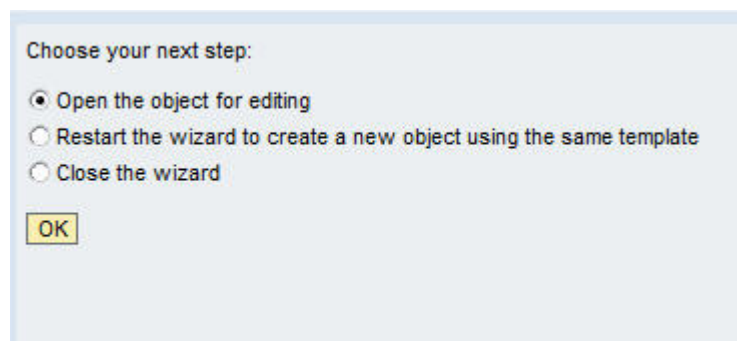


Figure 6 – Selecting the object for editing

8. On the Property Category menu, select **Show All**
9. Enter the following information:
- Application Host (Hostname of back-end R/3 system, ex: socw3s1er19.solnet.com)
 - ITS Host Name (<hostname>.<domain>.com:<port>)
 - ITS Path (/sap/bc/gui/sap/its/webgui)
 - ITS Protocol (http)
 - Logical System Name (same as the system you created and generally the same as the logical system you have created on the R/3 back-end ex:RE6CLNT800)
 - Logon Method (SAPLOGONTICKET)

- Remote Host Type (3)
 - SAP Client (i.e. 800)
 - SAP System ID (SID) (i.e. RE6)
 - SAP System Number (i.e. 00)
 - Server Port (Default 3200)
 - System Name (Same as Logical System i.e. RE6CLNT800)
 - System Type (SAP_R3)
 - User Mapping Type (admin,user)
 - WAS Hostname (<hostname>.<domain>.com:<port>)
 - WAS Protocol (http)
10. Click **Save**
 11. From the **Display** menu, select **System Aliases** to define a system alias.
 12. Create the following aliases (based on using ESS/MSS with WebDynpro).
 - <SID>CLNT<Client#> - (i.e. RE6CLNT800)
 - SAP_R3_HumanResources – Default Alias delivered with the ESS/MSS package that is loaded on the Java Stack.
 - SAP_WebDynpro_XSS – Default needed to use the WebDynpro after installing PCUI/XSS package that is loaded on the Java Stack.

The screenshot shows the 'System Alias Editor' interface. At the top, there are buttons for 'Save', 'Close', 'Preview', 'Refresh', and 'Edit Mode', along with a 'Display' dropdown menu set to 'System Aliases'. Below this is a header 'System Alias Editor' and a text instruction: 'Create new aliases for this system or delete existing ones. A system alias can be any name you choose. The default alias represents'. There is an 'Alias Name:' input field with an 'Add' button. Below this is a table titled 'Defined Aliases' with columns 'Default' and 'Alias Name'. The table contains three rows: 'RE6CLNT800' (not selected), 'SAP_R3_HumanResources' (selected with a checkmark), and 'SAP_WebDynpro_XSS' (not selected). At the bottom of the table are 'Remove' and 'Set Default' buttons. Below the table, it shows 'User Mapping Status: ✓ (Ready for user mapping configuration)' and 'Alias name: SAP_R3_HumanResources'. The page number 'Page 1 / 1' is visible in the bottom right corner.

Default	Alias Name
<input type="radio"/>	RE6CLNT800
<input checked="" type="radio"/>	SAP_R3_HumanResources
<input type="radio"/>	SAP_WebDynpro_XSS

Figure 7 – Creating system aliases

13. Click **Add** after creating each alias. Click **Save** after creating the last alias.

4 Check Profile Parameters in ABAP system

1. Enter transaction **/nRZ10**.
2. Choose the *Profile Browse* button
3. Choose your *Instance Profile*.
4. Choose *Extended Maintenance* radio button.
5. Choose *Change* button
6. Make sure *login/create_sso2_ticket* = 2 and *login/accept_sso2_ticket* is set to 1 else choose the *Create Parameter* button and create the parameter with their respective values.

5 Test connections in Portal-

1. Goto System administration->System configuration->Systems->Select your system(HFD)
2. Goto Display connection tests and test below connections-

SAP Web AS Connection

ITS Connection

Test Connection with Connector

You should see all tests successful.

Test iView

1. *Switch* to the portal.
2. Go to *System Administration* → *Support* → *SAP Application*

SAP NetWeaver Portal	<i>System Administration</i> → <i>Support</i> → <i>SAP Application</i>
-----------------------------	--

3. Choose *SAP Transaction link*.
4. Choose your SAP system by *alias* in the drop list menu.
5. Enter a transaction in the *Transaction code* field (ie **su01**).
6. Choose the *Go* button.
You should see the transaction displayed as *WebGui iView*.

Result

You have Single Sign-On enabled from portal to ABAP system.

Section II- SSO from ABAP to Portal and Vice Versa

1 Export Certificate from Portal System

1. Logon to the Portal and Navigate to below path
2. Go to *System Administration* → *System Configuration* → *Keystore Administration*

SAP NetWeaver Portal	<i>System Administration</i> → <i>System Configuration</i> → <i>Keystore Administration</i>
-----------------------------	---

3. Select *SAPLogonTicketKeypair-cert* from the drop list menu (default)
4. Choose Download verify.der

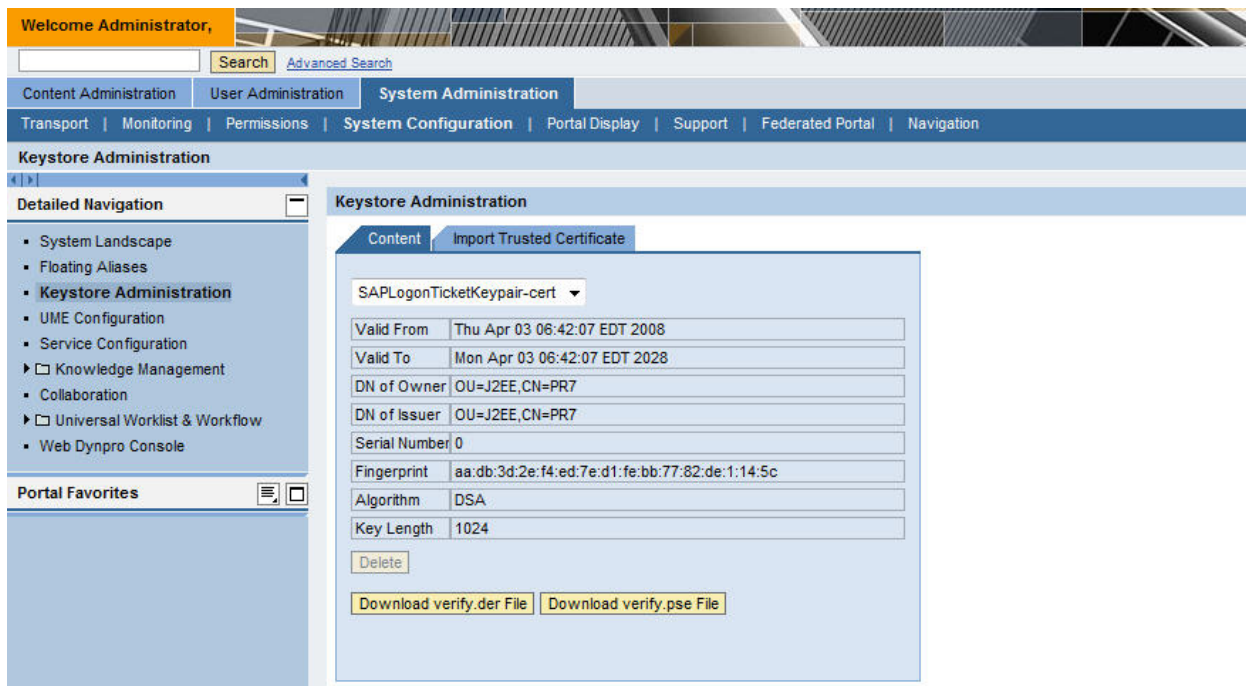


Figure 1- *SAPLogonTicketKeypair-cert*

5. Save file to a folder on your hard drive (ex: D:\Best_Practices\verify.der.zip)
6. Extract the zip file and save the *verify.der* file to the hard drive (i.e. D:\Best_Practices\verify.der)

2 Export / Import Certificates from ABAP system

Export SAP System Certificate

1. Enter `/nSTRUSTSSO2`.
2. Choose *Enter*.
3. Double-click “CN= in the Own Certif text field
4. The Certificate data will appear in the Certificate section.
5. Choose *Export certificate* button in the Certificate section and save to your hard drive (i.e. D:\Best_Practices\)

Note: choose binary as format in ‘Export Certificate’ dialog box

Import Portal Certificate into ABAP system

1. Logon to client 000 of ABAP system
2. Execute transaction ‘**STRUSTSSO2**’
3. Choose *Import certificate* button in the Certificate section.

Note: Choose binary as the format in the dialog box 'import certificate'

4. Choose the *Browse* button in the *File path* text field and select the *verify.der* you exported from the portal.
5. Choose *OK* button.
6. Choose *Add to Certificate List* button
7. Choose *Add to ACL* button
8. Add the *Portal Instance* name to the *System ID* text field.
9. Add **000** to the *Client* text field.
10. Choose *OK* button.
11. Choose *Save*.

3 Creating the system connector in the Portal

1. Log on to the Portal with a user id that has administrator rights.
2. Follow the menu path: **System Administration** → System Configuration → System Landscape → Portal Content. Click the arrow next to **Portal Content** as shown in Figure2.

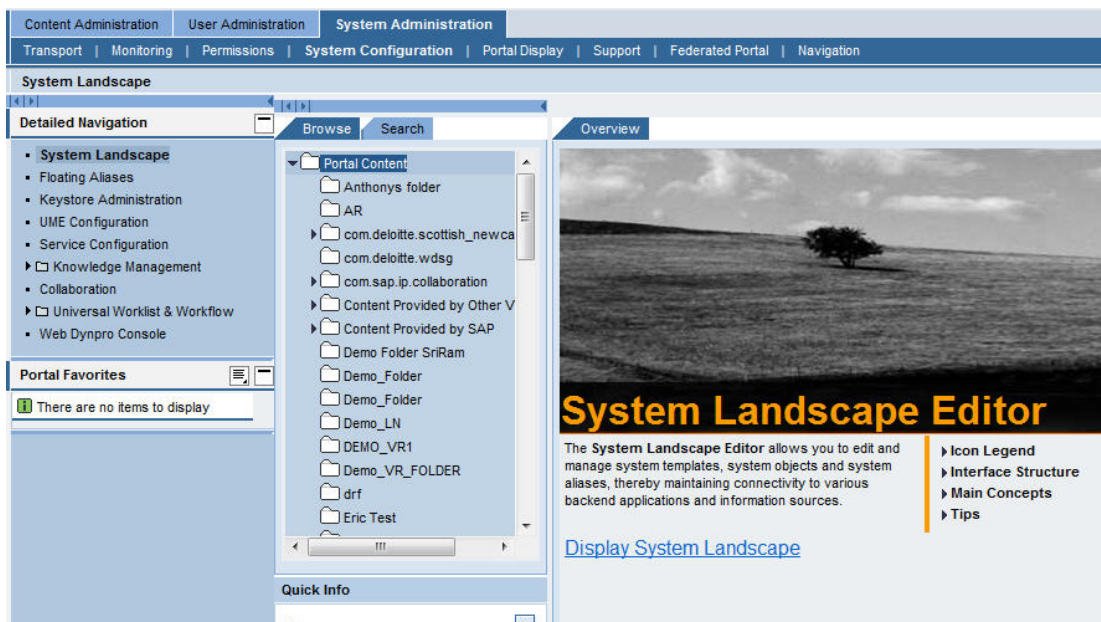


Figure 3 – System Landscape Editor

3. Under Portal Content, right-click on the Systems folder. Select **New** → **System** (from template) as shown in Figure



Figure 3 – Selecting the system folder

4. As shown in Figure 4, click **SAP system using dedicated application server**. Click **Next** to continue.

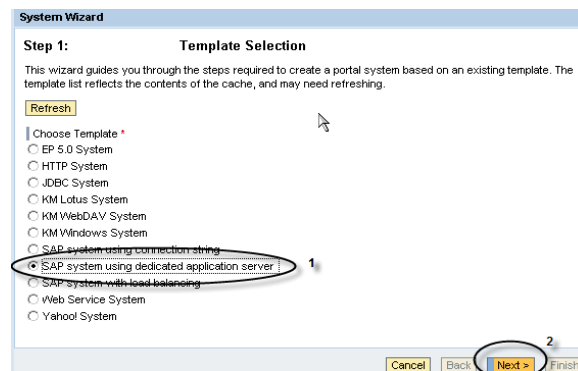


Figure 4 – Selecting the template

5. As shown in Figure 5, enter the **System Name**, **System ID**, and **System ID Prefix**. Select a **Master Language** and enter a **Description**. Click **Next** to continue.

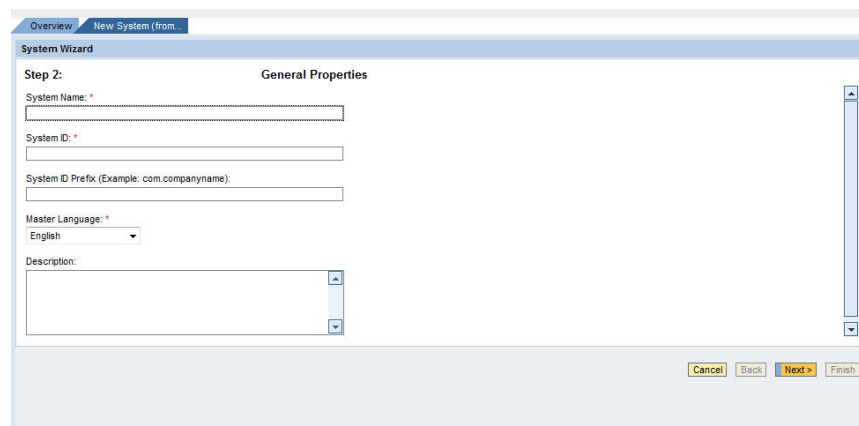


Figure 5 – Entering general properties

6. A summary screen appears. Click **Finish**.

7. As shown in Figure 6, click **Open the object for editing**. Click **OK**.

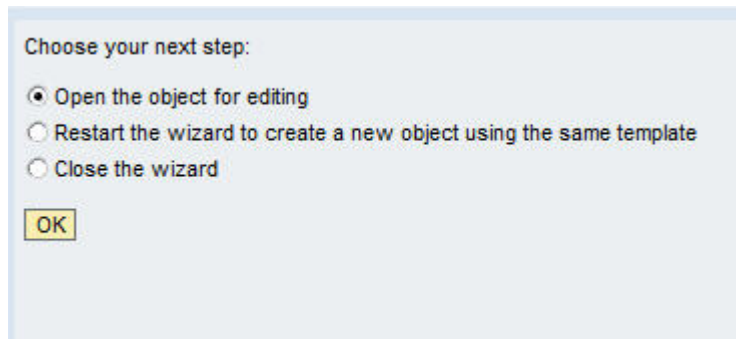


Figure 6 – Selecting the object for editing

8. On the Property Category menu, select **Show All**
9. Enter the following information:
- Application Host (Hostname of back-end R/3 system, ex: socw3s1er19.solnet.com)
 - ITS Host Name (<hostname>.<domain>.com:<port>)
 - ITS Path (/sap/bc/gui/sap/its/webgui)
 - ITS Protocol (http)
 - Logical System Name (same as the system you created and generally the same as the logical system you have created on the R/3 back-end ex:RE6CLNT800)
 - Logon Method (SAPLOGONTICKET)
 - Remote Host Type (3)
 - SAP Client (i.e. 800)
 - SAP System ID (SID) (i.e. RE6)
 - SAP System Number (i.e. 00)
 - Server Port (Default 3200)
 - System Name (Same as Logical System i.e. RE6CLNT800)
 - System Type (SAP_R3)
 - User Mapping Type (admin,user)
 - WAS Hostname (<hostname>.<domain>.com:<port>)
 - WAS Protocol (http)
10. Click **Save**
11. From the **Display** menu, select **System Aliases** to define a system alias.

12. Create the following aliases (based on using ESS/MSS with WebDynpro).
- <SID>CLNT<Client#> - (i.e. RE6CLNT800)
 - SAP_R3_HumanResources – Default Alias delivered with the ESS/MSS package that is loaded on the Java Stack.
 - SAP_WebDynpro_XSS – Default needed to use the WebDynpro after installing CUI/XSS package that is loaded on the Java Stack.

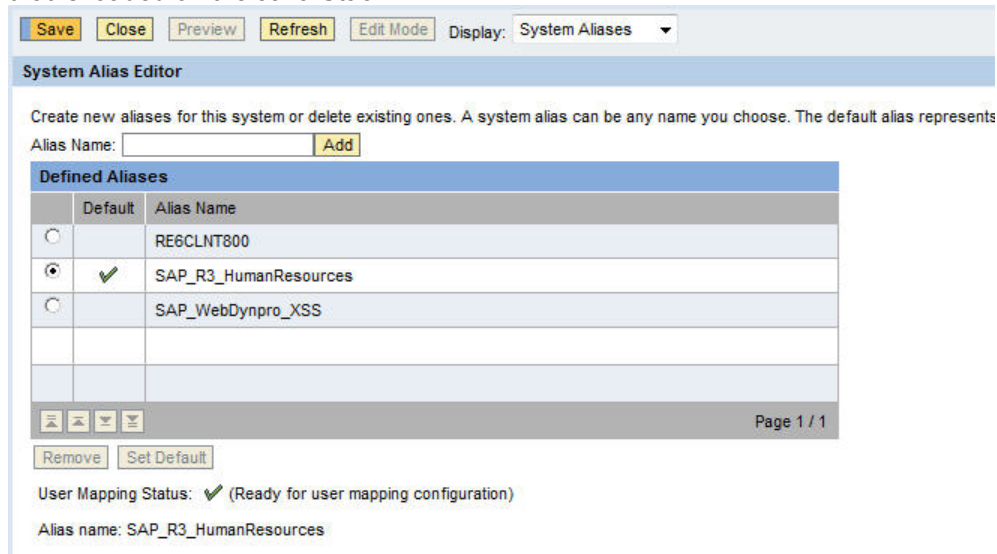


Figure 7 – Creating system aliases

13. Click **Add** after creating each alias. Click **Save** after creating the last alias.

4 Create a System user in ABAP system with Required Roles

Check the SAP system for the SAPJSP and required roles

1. Enter transaction **SU01**.
2. Choose *Enter*.
3. Enter **SAPJSF** in the *User* text field.
4. Choose *Create* button
5. Enter a *Last Name* in the required *Last Name* text field.
6. Enter initial password under Initial password and Repeat password
7. Choose *Roles* tab.
8. Enter SAP_BC_JSF_COMMUNICATION in the Roles table.
9. Choose *Save* button.

5 Check Profile Parameters in ABAP system

1. Enter transaction **/nRZ10**.
2. Choose the *Profile Browse* button
3. Choose your *Instance Profile*.
4. Choose *Extended Maintenance* radio button.
5. Choose *Change* button
6. Make sure *login/create_sso2_ticket* = 2 and *login/accept_sso2_ticket* is set to 1 else choose the *Create Parameter* button and create the parameter with their respective values.

6 Create a JCo RFC provider in the Portal system

1. Logon to the operating system level in your portal
2. Launch the *J2EE Visual Administrator*
3. Double-click the *go.bat* file for the J2EE Visual Administrator (i.e. C:\usr\sap\J2E\JC00\j2ee\admin\go.bat)
4. Logon to Visual admin with *Administrator password*.
5. Choose *Connect*.
6. Navigate to *Server* → *Services* → *JCo RFC provider* node.
7. Choose *JCo RFC* provider node.
8. Enter values in the following tables:

Field name	Field Entry
<i>Program Id</i>	<Name of Program> (for example, sapj2ee_port . You will need it later)>
<i>Gateway host</i>	< (for example, server.domain.com)>
<i>Gateway service</i>	< (for example, sapgw00)>
<i>Server Count (1..20)</i>	Enter a <i>number from 1 to 20</i>
<i>Application server host</i>	< (for example, server.domain.com)>
<i>System number</i>	<(for example, 00)>
<i>Client</i>	<(for example, 050)>
<i>Language</i>	
<i>User</i>	< <i>user from step 2</i> >
<i>Password</i>	< password from step 2 >

9. Choose *Set* button.

7 Add ABAP System to Security providers list in Portal

1. Logon to Visual admin Choose Server ## -> Services -> Security Provider
2. Choose *ticket* in the Components menu.
3. Choose *Edit* mode button

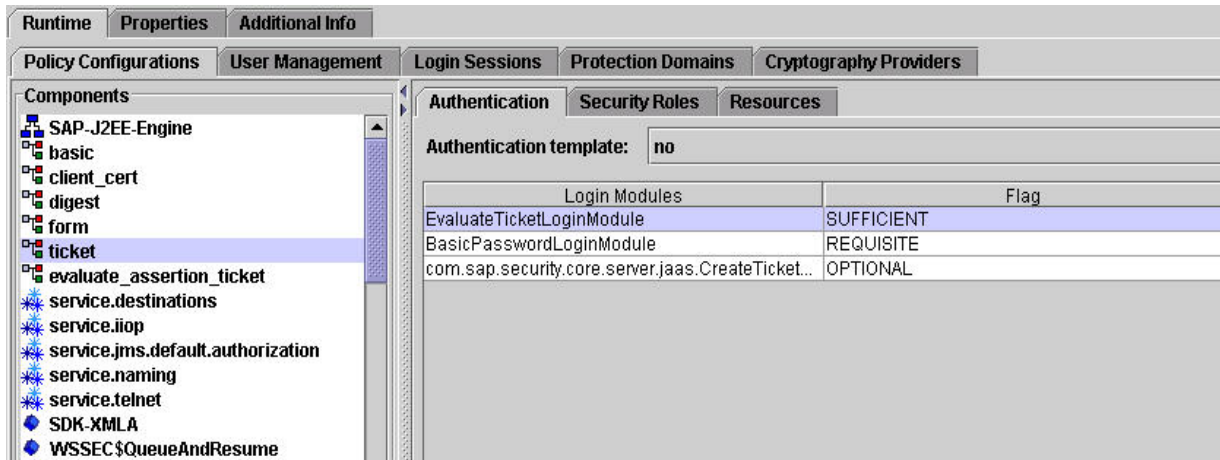


Figure 8- Visual Admin

4. Choose *com.sap.security.core.server.jaas.EvaluateTicketLoginModule* in the Login Modules table.
5. Choose *Modify* button. An *Edit Login Module* dialog box displays.
6. Enter the following information:

Name	Value
ume.configuration.active	<true (default)>
trustedsys# (change # to a number, for example trustedys1)	<SID>, <client> (for example, RE6, 800)>
trustediss# (change # to a number, for example trustediss1)	CN=<SID> (for example CN=RE6)
trustedn# (change # to a number, for example trustedn1)	CN=<SID> (for example CN=RE6)

7. Choose *OK* button.
8. Choose *com.sap.security.core.server.jaas.CreateTicketLoginModule*.



9. Choose *Modify* button. An *Edit Login Module* dialog box displays.

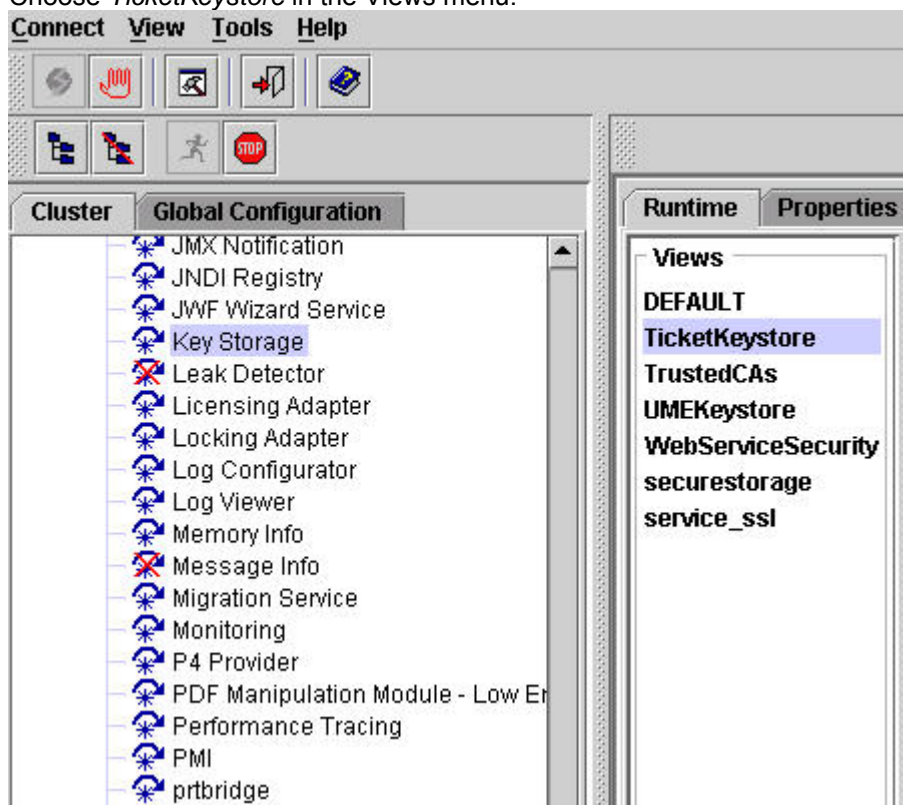
10. Enter the following information:

Name	Value
ume.configuration.active	<true (default)>
trustedsys# (change # to a number, for example trustedsys1)	<SID>, <client> (for example, RE6,800)>
trustediss# (change # to a number, for example trustediss1)	CN=<SID> (for example CN=RE6)
trustedn# (change # to a number, for example trustedn1)	CN=<SID> (for example CN=RE6)

11. Choose *OK* button.

8 Import ABAP system certificate to J2EE of portal system

1. Logon to Visual Admin and Navigate to *Server* → *Services* → *Key storage*
2. Choose *TicketKeystore* in the Views menu.



3. Choose the *Load* button.
4. Choose the *certificate* of the SAP system from step 2.

9 Create RFC connection in the ABAP system to Portal

1. Switch to the *SAP system*.
2. Enter transaction **SM59**.
3. Right-click *TCP/IP* connections and choose *Create*.
4. Enter the following values:

Name	Value
<i>RFC Destination</i>	<Name (for example, RFC_to_portal)>
<i>Connection Type</i>	T
<i>Description</i>	< <i>description of connection</i> >

5. Choose *Save* button.
6. Enter the following values into the Technical settings:

Name	Value
<i>Gateway host</i>	< (for example, server.domain.com)>
<i>Gateway service</i>	< (for example, sapgw00)>

7. Once you create the RFC connection in step 10 test the connection.

10 Maintain Portal Server Settings in ABAP

1. Execute transaction SM30 in ABAP system
2. Enter RSPOR_T_PORTAL as the table
3. Choose *Maintain*
4. Choose *New Entries*
5. Maintain following
 - RFC Destination
 - System name
 - Portal URL Prefix
 - Prefix for RM for BW metadata
 - KM service URL

Restart the J2EE instance

If you have changed parameters in RZ10, right-click the *Server ##* and choose *Reboot*.

11 Test connections between ABAP and Portal system

Test Connections in ABAP-

1. Create a *test user* in the SAP system with transaction *SU01*.
2. Create a test user in the portal system with the same user name.
3. Switch to the portal.
4. Navigate to *User Administration* → *Create User*.
5. Enter the following information:

Name	Value
<i>Name</i>	Username of logon for both portal and SAP System
<i>Last Name</i>	
<i>First Name</i>	
<i>Email address</i>	

6. Choose *Create* (scroll to the bottom of the iView)
7. Choose *Registered* server program under Technical settings.
8. Enter the *Application Name* in the Program ID field
9. Enter *Gateway host*
10. Enter *Gateway service*
11. Choose *Save*.
12. Test Connection.

Test connections in Portal -

1. Goto System administration->System configuration->Systems->Select your system
2. Goto Display connection tests and test below connections-

SAP Web AS Connection

ITS Connection

Test Connection with Connector

You should see all tests successful.

Test iView

1. *Switch* to the portal.
2. Go to *System Administration* → *Support* → *SAP Application*

SAP NetWeaver Portal

<i>System Administration</i> → <i>Support</i> → <i>SAP Application</i>
--

3. Choose *SAP Transaction link*.
4. Choose your SAP system by *alias* in the drop list menu.
5. Enter a transaction in the *Transaction code* field (ie **su01**).
6. Choose the *Go* button.
You should see the transaction displayed as *WebGui iView*.

Result

You have enabled Single Sign-On from portal to ABAP and vice versa.

Related Content

http://help.sap.com/saphelp_nw04s/helpdata/en/53/695b3ebd564644e10000000a114084/frameset.htm

<https://www.sdn.sap.com/irj/servlet/prt/portal/prtroot/docs/library/uuid/ec82ec90□0201□0010□72bc□88ef150211ff>

<https://www.sdn.sap.com/irj/scn/go/portal/prtroot/docs/library/uuid/0077873d-0b01-0010-1abb-cbf21d1aa43>

For more information, visit the [Security homepage](#).

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.