Configuring AS J2EE and AS ABAP to Accept and Verify SSO Logon Tickets – Practical examples

Applies to:

SAP Enterprise Portal. For more information, visit the Portal & Collaboration homepage

Summary

You can prevent data from being written to the Portal Content Directory (PCD) by activating write-protect mode. This article presents all the different ways of activating the write protect mode.

Author: arthik Rajagopal

Company: Infosys Technologies Ltd.

Created on: 24 March 2009

Author Bio

Karthik Rajagopal is a SAP Certified Professional with a vast experience in SAP NetWeaver-Portal, Knowledge Management & Collaboration and WebDynpro technologies.

Table of Contents

SSO Functionality

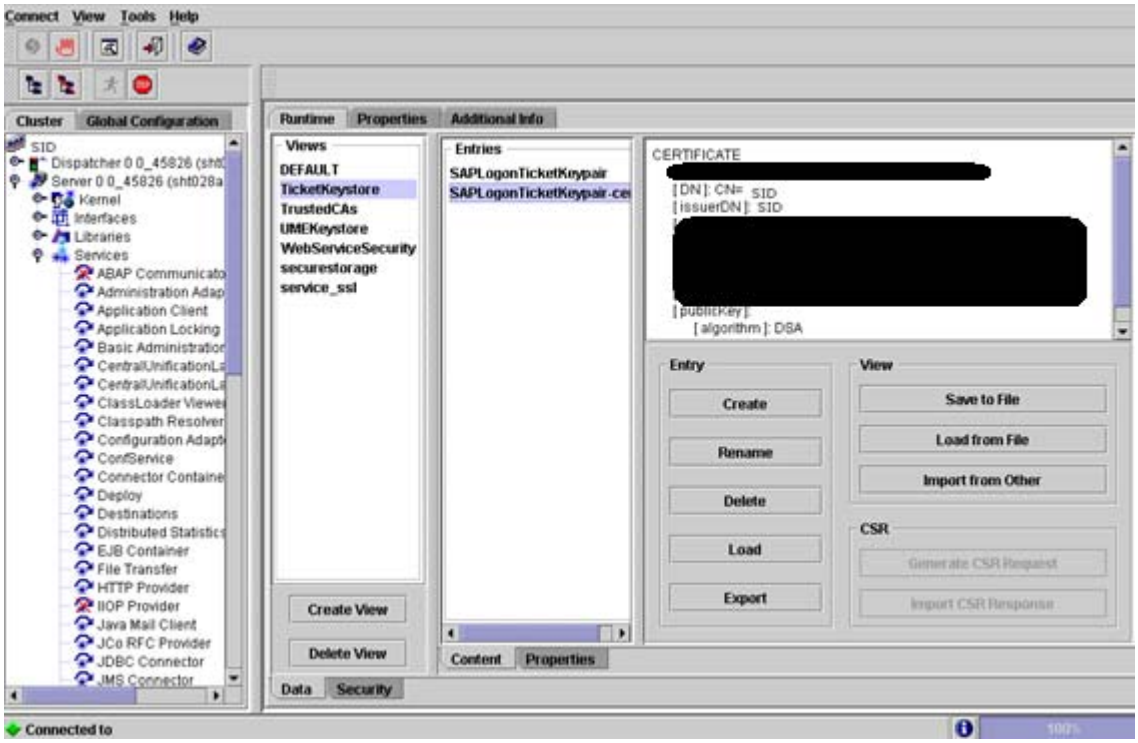
Single Sign On provides the flexibility to the user to just login once into the system and access all other SAP systems. When a user logs in to the EP system, a non–persistent HTTPcookie is generated, this holds the SAP logonticket in the user's browser. In order to accept this cookie in the browser, the internet options settings has to accept this cookie to reside in the browser. The backend needs to accept the logon ticket from the Portal. To enable the Internet browser to accept the SSO cookie, you must enter a fully qualified host name.

For Configuring EP as Ticket-Issuing System you will set up the logon ticket options as appropriate. Also, if non-SAP systems are included in the portal, you can set up a user mapping between the SAP user IDs and the external system's user IDs. To protect the logon ticket that will be issued to the users, the portal digitally signs the logon ticket. For this purpose, the portal possesses a public-key pair. The corresponding public key needs to be made available to the accepting systems for use in the next steps.

i.e. you will set up any AS-ABAP and AS-JAVA systems that are integrated into the portal to accept the portal's logon tickets i.e. Configuring AS-ABAP and AS-JAVA to Accept and Verify Logon Tickets

Configuring SAP Web AS J2EE to Accept Logon Tickets from the J2EE Engine

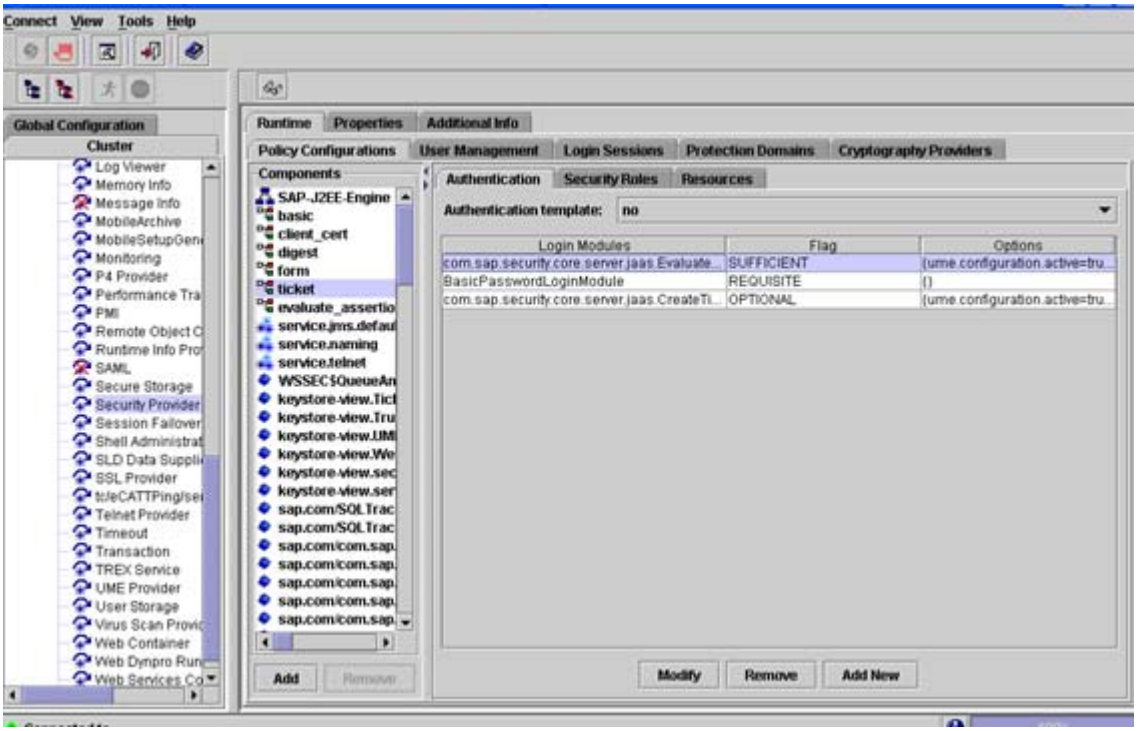
1. Start the *Visual Administrator.*
2. Choose *Cluster* → *Server* → *Services* → *Key Storage* → *TicketKeystore*.



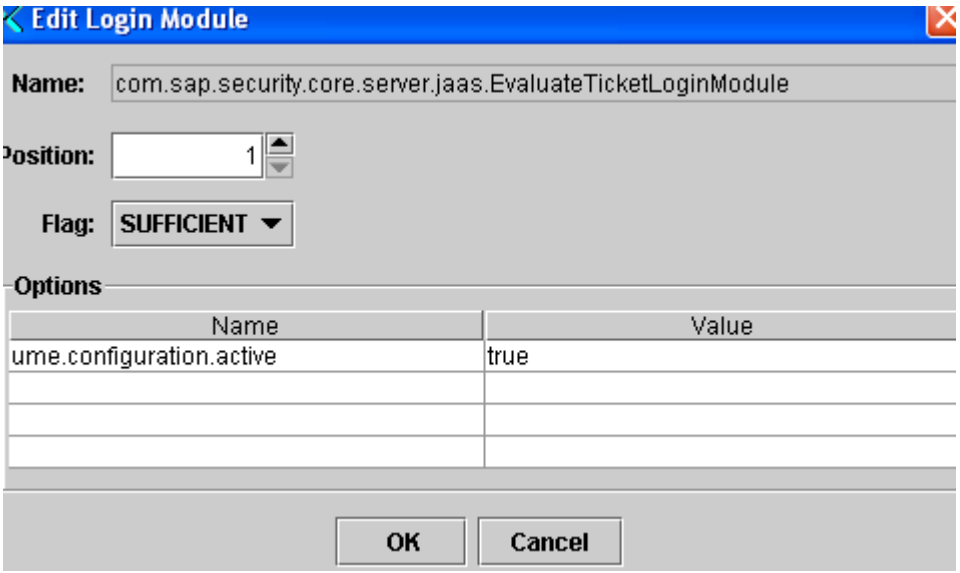
3. Click *Load* and then select the certificate and say OK.

   For the certificate extract EP's .der file, and then browse to the file on Windows.
4. Take note of the [DN] and [issuer DN], as shown below.

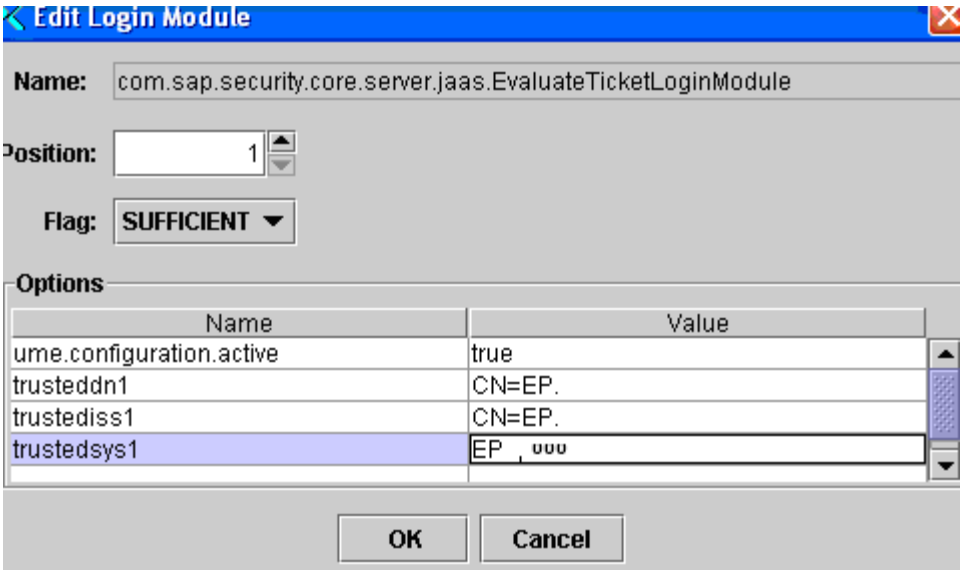
5. Choose *Cluster* → *Server* → *Services* → *Security Provider* → *ticket* as shown below.



6. Select Login Module that ends with “EvaluateTicketLoginModule as shown selected above and click *Modify*



7. Make the following entries below. In the "Value" field, the value for the DN and IssuerDN **must exactly match** what is in the cert in the Key Storage area in the step 4 above i.e. trusteddn1 (DN) and trustediss1 (IssuerDN). The trustedsys1 will most likely use 000 for a J2EE certificate.



Note: Login Module Options i.e. Name/Value pairs are as below

Name	**Value**
trustedsys<x>	**<SID>, <Client>** .
trustediss<x>	**<Issuer's_Distinguished_Name>** Distinguished Name of the **issuer** of the ticket-issuing system's public-key certificate.

trusteddn<x>	**<System's_Distinguished_Name>** Distinguished Name of the **ticket-issuing system**. If the ticket-issuing system uses a self-signed certificate, then these two Distinguished Names are identical. Also, the corresponding public-key certificate must exist in the SAPLogonTicket keystore view entry.
tenant<x>	Mulititenant portal only: **<Tenant name>** This entry is necessary if the accepting J2EE Engine is part of a multitenant portal environment, but the ticket issuer is not. In this case, you need to specify the tenant name as defined in the multitenant portal. For more information, see
ume.configuration.active	**true**

Note: the table above is available in standard sap help document.

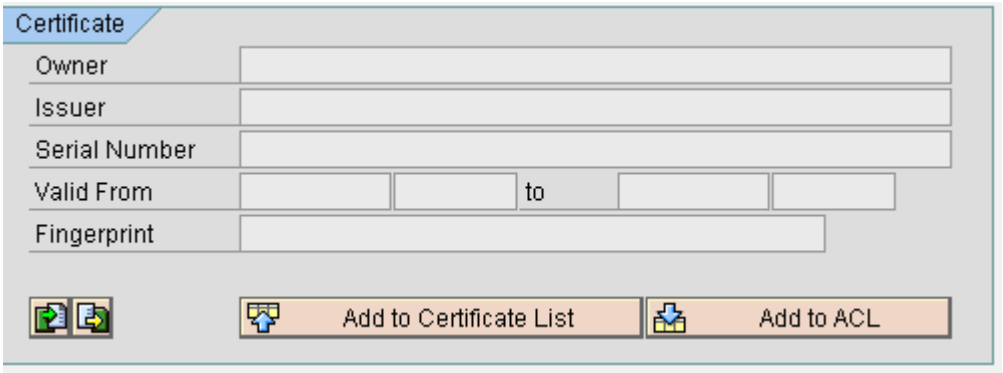
Result for WAS J2EE

The WAS J2EE Engine accepts logon tickets that have been issued by the server.

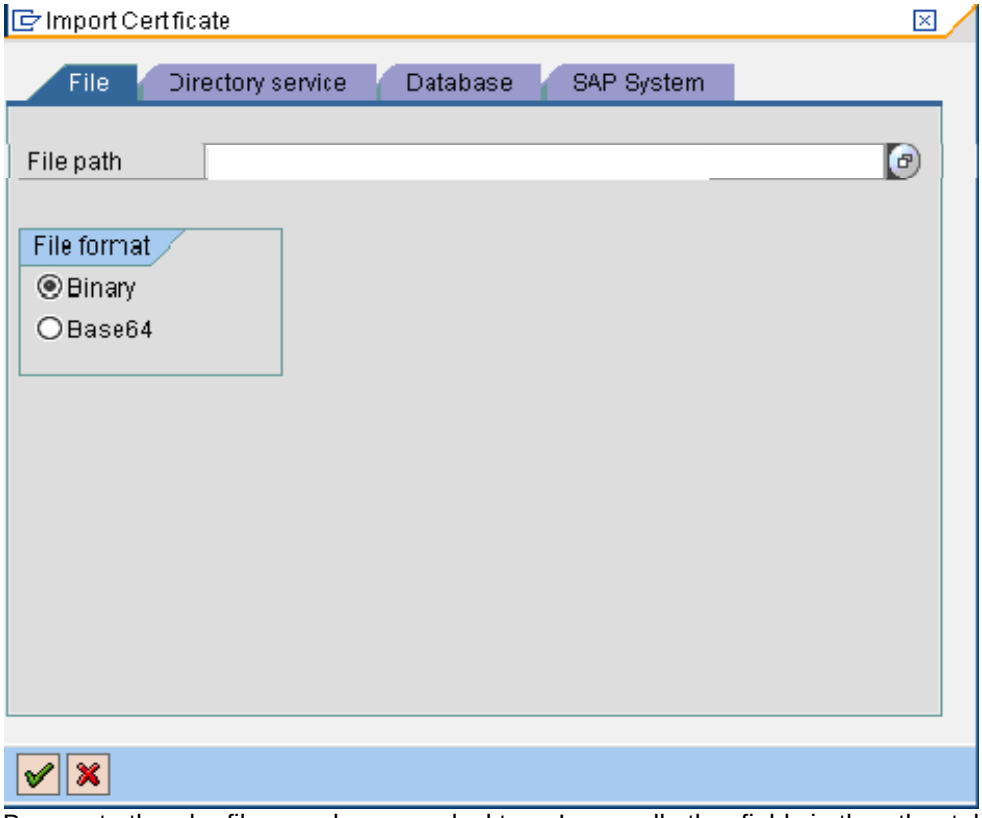
Configuring SAP Web AS ABAP to Accept Logon Tickets from the J2EE Engine

If you want to use Single Sign-On between the J2EE Engine and an SAP Web AS ABAP system, then you must configure the corresponding AS ABAP application server to accept logon tickets accordingly as shown below

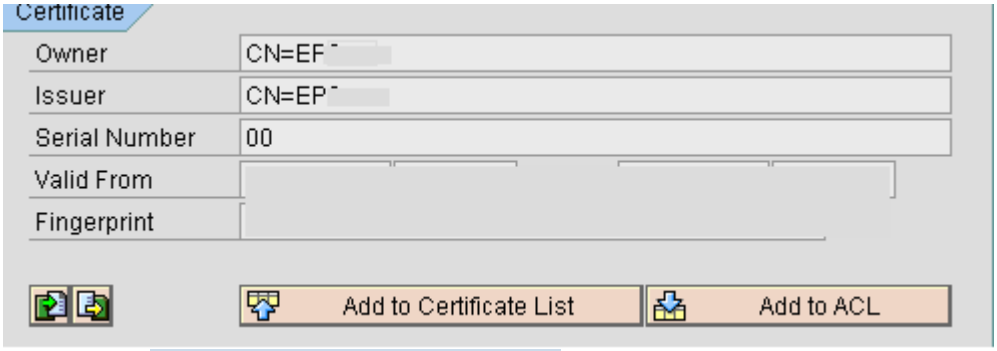
1. Set the profile parameter **login/accept_sso2_ticket** = 1. Set **login/create_sso2_ticket** = 0 unless the server should also be able to issue tickets
2. For Releases >= 6.10, use the trust manager (transaction STRUST or STRUSTSSO2).



3. In the section that says Certificate, select the  (Import Certificate) as shown above to load the certificate (.der file) in the ABAP Stack of your backend System. (i.e. Import the J2EE Engine's public-key certificate into the PSE that is used for logon tickets. Per default this is the System PSE.)

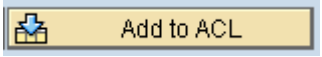


4. Browse to the .der file saved on your desktop. Leave all other fields in the other tabs as is and select the  button to complete the import.

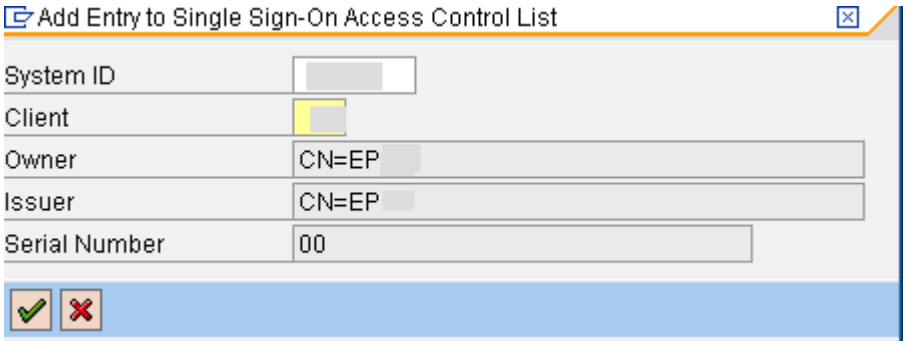


5. Click on the 

button. You will now see CN=EP listed in the Certificate List under System PSE.

6. Click the 

button. Add the J2EE Engine's information to the access control list:



Were SID = Your system SID and Client = 000.

7. Select the  button to complete -> SAVE

Reference links:
http://help.sap.com/saphelp_nw2004s/helpdata/en/61/42897de269cf44b35f9395978cc9cb/content.htm

Result for WAS J2EE

The WAS J2EE Engine accepts logon tickets that have been issued by the server. i.e EP

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.