

Single Sign On to SAP Net Weaver Enterprise Search 7.2 using Integrated Windows Authentication



Applies to:

SAP Net Weaver Enterprise Search 7.2. For more information, visit the [Search homepage](#).

Summary

For a seamless integration of SAP Enterprise Search in a Microsoft environment Single Sign on is a must. Since the OpenSearch service and the search UI of SAP NetWeaver Enterprise Search 7.2 is based on the ABAP stack, Integrated Windows Authentication is not an option that works out of the box. In this whitepaper we show what configuration steps have to be performed to achieve Single Sign-On for SAP NetWeaver Enterprise Search 7.2 using Integrated Windows Authentication.

Prerequisites

This article assumes that you already have a SAP J2EE instance in your landscape which is configured to issue SAPLOGON based Single-Sign-On-Tickets to your clients.

Authors: André Fischer, Technology Solution Management
Holger Bruchelt, Duet Regional Implementation Group

Company: SAP AG

Created on: 26 February 2010

Updated on: 13 November 2010

Author Bio



André Fischer works in the **Information Worker** Product Technology Group at **SAP AG** on Project Gateway. In addition Andre has lent his talents as an SAP technology consultant for eight years before joining SAP 2004.



Holger Bruchelt works at **SAP AG** in the **Duet Regional Implementation Group** in Germany. Before that he has been working as a technical NetWeaver consultant since 2002.

Table of Contents

Introduction.....	3
SAML protocol based approach	3
SAP Logon Ticket based approach	4
How it works	5
How to section	7
Configuration of the SPNego Login Module	7
The Redirect App	7
Deployment and Configuration of the RedirectApplication	9
Creating Internal Aliases for the OpenSearch Services and the Enterprise Search UI	10
Troubleshooting	15
ESH specific customizing for OpenSearch URL's	15
Outlook 16	
Related Content	17
Copy right	18

Introduction

As the OpenSearch standard (<http://www.opensearch.org/>) has evolved and became popular, SAP NetWeaver Enterprise Search provides an interface for its search functionality in accordance with the OpenSearch standard as of Enterprise Search 7.0 SP3. With the OpenSearch support SAP offers a simple search integration technology that can be used in several integration scenarios.

With Enterprise Search 7.2 the OpenSearch interface has been enhanced based on the extension concept offered by the OpenSearch standard. In addition to the OpenSearch standard the interface now also provides detailed meta data about the search results, connectors being used in a SAP specific namespace.

Since the OpenSearch service and the search UI of ES 7.2 is based on the ABAP stack Integrated Windows Authentication is not an option that works out of the box. Instead the following authentication mechanisms are available when using browser based communication for a SAP NetWeaver Application Server ABAP 7.20:

- HTTP Basic Authentication (HTTP with user ID and password in header data)
- X.509 client certificates (HTTPS/SSL with mutual authentication)
- SAP Logon tickets
- SAML protocol

For a federated search scenario Single-Sign On is a prerequisite. In a scenario where SharePoint 2007 acts as the calling application at a first glance one would expect that no SSO is possible since SharePoint only supports Integrated Windows Authentication to connect to 3rd party OpenSearch repositories

The same problem occurs if one would like to consume the search results of the OpenSearch interface of SAP Enterprise Search as an RSS Feed using Microsoft Outlook 2007.

However it is possible to leverage Integrated Windows Authentication indirectly for the following 2 options:

- SAML protocol
- SAP Logon Tickets

SAML protocol based approach

The solution that leverages the SAML protocol would work as follows. In this scenario the OpenSearch interface of SAP Enterprise Search acts as a service provider (SP). An http based OpenSearch request that is not authenticated would be redirected to an Identity Provider (IdP). If the IdP supports Integrated Windows Authentication a SAML token will be issued that can be used for authentication at the OpenSearch interface of SAP Enterprise Search.

The advantage of using the SAML protocol would be that a SAML infrastructure could be leveraged by several browser based federation scenarios and that only a central configuration is necessary rather than being forced to configure every system individually.

Since the Identity Providers of both vendors are not available yet we will describe this scenario in an upcoming publication. Please stay tuned.

SAP Logon Ticket based approach

The other option that works already now using components that are already available works as follows:

The authentication options offered by the Java stack can be leveraged by a Web Application Server ABAP as well if users are redirected to a JSP page running on a Web Application Server Java in the event of a logon error. The http request will be authenticated and a SAP Logon Ticket will be issued by the Java stack. The authenticated http request will then be redirected back to the calling URL.

Using transaction SICF it is possible to configure for each service an individual behavior in case of a logon error. Using the option *Redirect to URL* one can specify a URL to which the call is sent if a logon error occurs.

For Enterprise Search we have to use a separate Java stack, for example a SAP NetWeaver Portal, since the Lean Java stack of SAP NetWeaver Enterprise Search must only be used for Lifecycle Management.

Changing the original SAP OpenSearch Services and the UI service of Enterprise Search in SICF would result in a repair that should be avoided. It is rather recommended to create a new service in the customer namespace that acts as a reference to an existing service. The custom service can then be configured to use the *Redirect to URL* feature.

To use this feature it is necessary to deploy a JSP-page on the Java stack that redirects the user back to the OpenSearch service URL after the user has successfully authenticated using Integrated Windows Authentication at the Java stack using the SPNego Login Module.

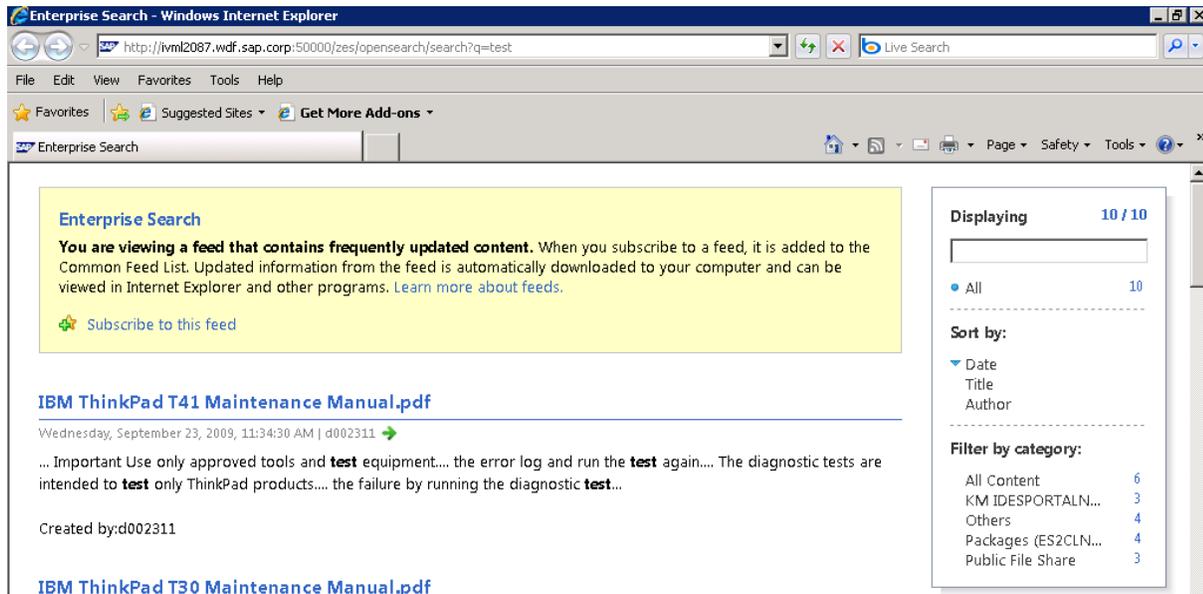
How it works

In our setup we are using a SAP NetWeaver Enterprise Search running on the server *ivml2087* and a SAP NetWeaver Portal 7.01 SP3 running on the server *iwdfvm3137* as the ticket issuing instance.

When a user opens the URL of the OpenSearch Service

`http://ivml2087.wdf.sap.corp:50100/zes/opensearch/search?q=test`

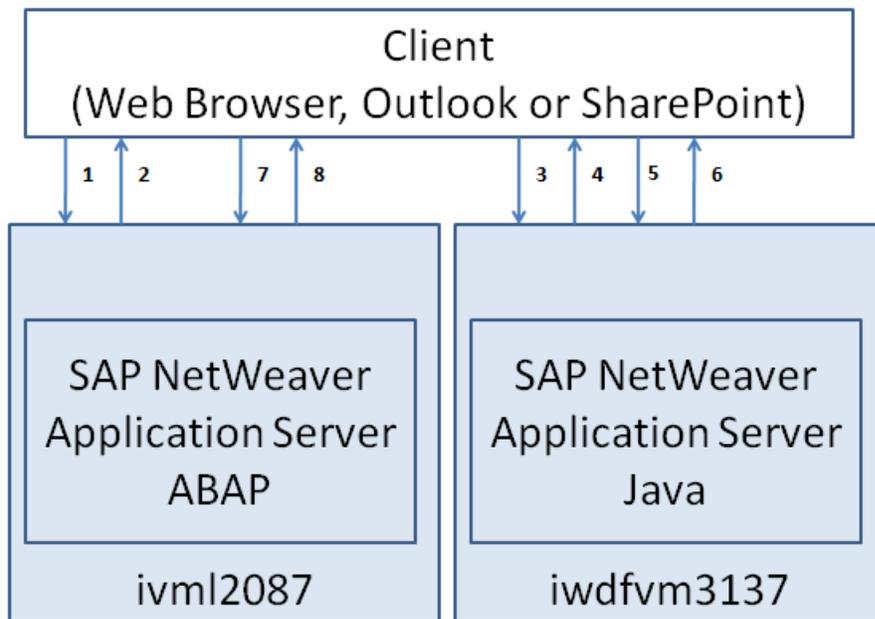
he or she will be authenticated and will get a result that looks similar to the result shown in the following screen shot:



So, what happened? Let's have a look at the http traffic between the browser and the SAP Enterprise Search Server. The HTTP traffic can be recorded with tools like HTTP Watch Professional. The result is shown in the following screen shot.

Method	Result	Type	URL
GET	307	Redirect to http://iwdfv...	http://ivml2087.wdf.sap.corp:50000/zes/opensearch/search?q=test
GET	401	text/html	http://iwdfvm3137.wdf.sap.corp:50000/RedirectApp/test.jsp?to=http://ivml2087.wdf.sap.corp:50000%2fzes%2fopensearch%2fsear...
GET	302	Redirect to http://ivml20...	http://iwdfvm3137.wdf.sap.corp:50000/RedirectApp/test.jsp?to=http://ivml2087.wdf.sap.corp:50000%2fzes%2fopensearch%2fsear...
GET	200	text/xml; charset=utf-8	http://ivml2087.wdf.sap.corp:50000/zes/opensearch/search?q=test

The HTTP responses (307, 401, 302 and 200) are highlighted in the following detailed description



1. The Client sends a request to the Internet Communication Manager (ICM). Based on the URL the ICM decides which service in the ABAP stack to call.
2. Since the initial request cannot be authenticated successfully the ABAP stack sends the preconfigured response (HTTP 307) that redirects the HTTP client to our Java Redirect application:

```
http://iwdfvm3137.wdf.sap.corp:50100/RedirectApp/redirect.jsp?to=
http://ivml2087.wdf.sap.corp:50100<%=PATHTRANS%>
```

3. The client sends a new request using the new URL that points to the jsp-page on the Java server
4. Since the SPNego template is assigned to the RedirectApp the first thing the J2EE does is sent a 401 Authentication Required with www-authenticate header: Negotiate. (HTTP 401)
5. The browser then sends a Kerberos ticket
6. When the request is successfully authenticated on the J2EE Engine the J2EE engine issues a MYSAPSSO2 ticket that is added to the HTTP response. With this ticket we are redirected (HTTP 302) by the JSP page back to the OpenSearch URL on the ABAP server, still passing on the parameters from <PATHTRANS> and any other GET Parameters (Form Fields).
7. The client sends the original request that now contains a SAP Logon Ticket again to ICM
8. The user is now authenticated using the MYSAPSSO2 ticket and the client receives a response (HTTP 200) that contains the OpenSearch result.

How to section

In the following we will describe which configuration steps have to be performed in order to achieve Single Sign-On for the Search UI and the OpenSearch Services of SAP NetWeaver Enterprise Search 7.2. Please note that the URLs and port numbers given here are examples only and can be different from your setup.

To achieve this integration the following steps have to be performed:

- Configuration of the SPNego Login Module in a SAP NetWeaver Application Server Java.
- Deployment of a RedirectionApp on the J2EE engine that is used for the authentication and performs a redirect to the calling service
- Create custom alias services entries for all OpenSearch Services (description, list, search) and the Search UI and configure the redirection to the RedirectionApp in case of Logon Errors

Configuration of the SPNego Login Module

The SPNego (Simple and Protected GSS API Negotiation Mechanism) Module is an authentication method for SAP J2EE Instances which allows authenticating users of a windows domain through a SAP J2EE Server instance. Note that this only works if clients, the Active Directory Server to which the clients authenticate, the J2EE Engine and the Enterprise Search Server sit in the same domain.

In a first step SPNego has to be configured first on the J2EE Engine. To do so open the SPNego Wizard using the SAP NetWeaver Administrator.

<http://iwdfvm3137.wdf.sap.corp:50100/nwa> → Configuration → SPNego Configuration Wizard

For further details about the configuration of the SPNego Login Module see the [blog series](#) of Holger in SDN or consult the Netweaver Help.

We recommend that you perform these steps before continuing with the next steps. Make sure SPNego really works so that you can rule out any other errors in the following steps.

The Redirect App

What does the RedirectApp do? The ear file is very simple and consists mainly of a JSP file. The only reason why this JSP file is not placed alone on the J2EE Engine is because only within an EAR file a login stack (SPNego) can be assigned to it. The JSP looks like this:

```
<%@ page language="java" %>
<%
    String redirectURL = request.getParameter ("to");
    String sapField = request.getParameter("sap-ffield");
    String newURL = redirectURL + "?" + sapField;
    response.sendRedirect (newURL);
%>
```

redirectURL takes the value from the GET parameter "to".
 sapFields takes the value from GET field sap-ffield.
 newURL concatenates these values

Note: The field sap-ffield contains the query string of the URL send to SAP Enterprise Search .

Since the RedirectApp has to be configured in a way that it requires user authentication (in our case SPNego), the web.xml has to contain several configurations. All the required steps are explained in detail in the blog here: <http://www.sdn.sap.com/irj/scn/weblogs?blog=/pub/wlg/11039>

In the end the web.xml should look something like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE web-app PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
"http://java.sun.com/dtd/web-app_2_3.dtd">
  <web-app>
    <display-name>WEB APP</display-name>
    <description>WEB APP description</description>
    <servlet>
      <servlet-name>redirect.jsp</servlet-name>
      <jsp-file>/redirect.jsp</jsp-file>
    </servlet>
    <security-constraint>
      <display-name>SecurityConstraint</display-name>
      <web-resource-collection>
        <web-resource-name>WebResource</web-resource-name>
        <url-pattern>*</url-pattern>
      </web-resource-collection>
      <auth-constraint>
        <role-name>DefaultSecurityRole</role-name>
      </auth-constraint>
      <user-data-constraint>
        <transport-guarantee>NONE</transport-guarantee>
      </user-data-constraint>
    </security-constraint>
    <security-role>
      <role-name>DefaultSecurityRole</role-name>
    </security-role>
  </web-app>
```

Let us now have a look at the following example. The following URL

```
http://ivm12087.wdf.sap.corp:50100/zes/opensearch/search?q=test
```

would result in a redirect to

```
http://iwdfvm3137.wdf.sap.corp:50100/RedirectApp/redirect.jsp?to=http://ivm12087.wdf.
sap.corp:50100%2fzes%2fopensearch%2fsearch&sap-ffield=q%3dtest
```

that would be split up by the JSP into the following components:

- redirectURL = http://ivm12087.wdf.sap.corp:50100%2fzes%2fopensearch%2fsearch
(meaning http://ivm12087.wdf.sap.corp:50100/zes/opensearch/search)
- sapField = q%3dtest
(meaning q=test)

And the final URL the user will be redirected to would then be again:

```
http://ivm12087.wdf.sap.corp:50100/zes/opensearch/search?q=test
```

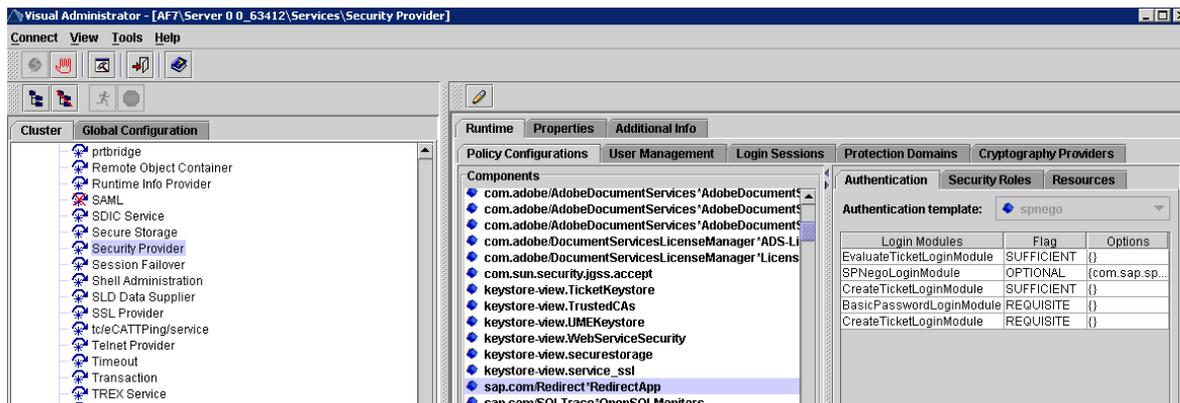
Deployment and Configuration of the RedirectApplication

When SPNego is working, the RedirectApplication (RedirectApp.ear) has to be deployed. This can either be done via the IDE (NetWeaver Developer Studio) or via the following workaround (of course depending on the Java version you can also use SDM to deploy this file).

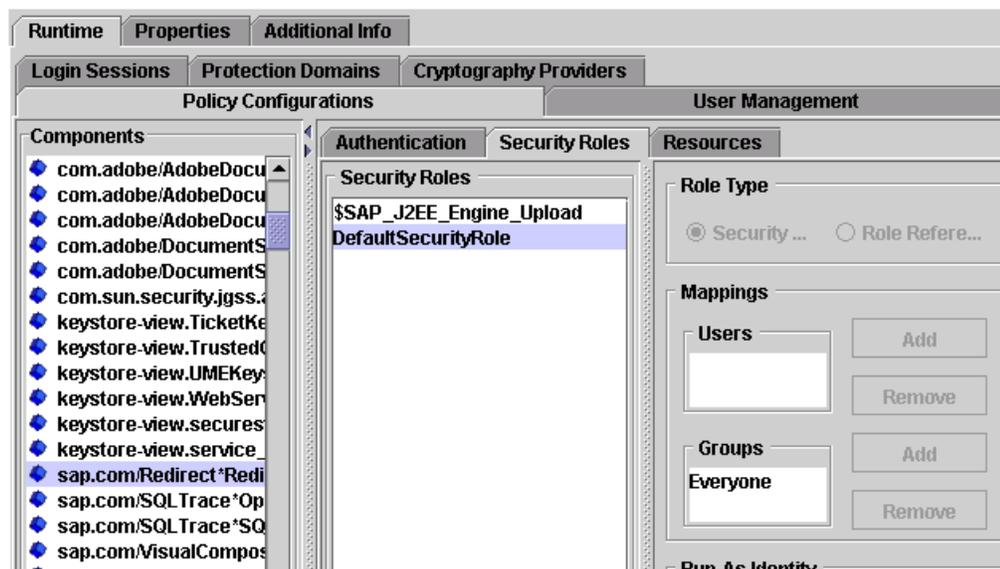
Logon to the server and run

- 1) Execute command: telnet localhost 5<instance number>08
- 2) Log in as SAP system Administrator j2ee_admin.
- 3) Run the following commands at the telnet prompt:
- 4) add deploy
- 5) deploy <full path to SCA> version_rule=all on_prerequisite_error=stop on_deploy_error=stop

Now the Redirect Application should be visible in the components view. Assign the SPNego template via "Used Template":



The Redirect Application currently uses the Action *DefaultSecurityRole* (see web.xml mentioned above). In order to allow every user to call the Redirect application (this does NOT mean that every user will be automatically logged on) we have to assign this role to the *Everyone* Group.



After the deployment and the assignment of the *Everyone* group to the *DefaultSecurityRole* you can already perform a quick test:

Call the URL <http://iwdfvm3137.wdf.sap.corp:50100/RedirectApp/redirect.jsp?http://www.sap.com>. As a result you should be redirected to <http://www.sap.com>.

If that is not working, check the deployment of the *Redirect.ear*.

If it was working, we have to make sure that SPNego was really used for authentication. So disable SPNego (e.g. by deactivating “Enable Integrated Windows Authentication in the Internet Explorer -> Tools -> Internet Options -> Advanced menu or by removing the J2EE Site from the Local Intranet settings).

After doing that – always close the browser before trying again – call again the URL <http://iwdfvm3137.wdf.sap.corp:50100/RedirectApp/redirect.jsp?http://www.sap.com>. This time you should not be redirected to <http://www.sap.com>, but should be prompted for Username & Password, or get a similar error message.

If that is not the case, make sure that you have assigned the *Everyone* Group to the *DefaultSecurityRole* like mentioned above.

Creating Internal Aliases for the OpenSearch Services and the Enterprise Search UI

Now log on to the ABAP stack and go to SICF. Since we want to avoid changing the OpenSearch Services delivered by the SAP standard we want to create new services that use the existing services as a reference.

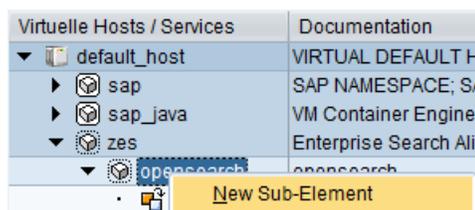
If you have your own namespace, we recommend that you create a node with the same name as the namespace at the top level of the HTTP service hierarchy, and create all your services under this node. As an alternative you can use a namespace whose name starts with Z. A detailed documentation can be found here:

http://help.sap.com/saphelp_nw70/helpdata/en/78/9852bac06b11d4ad310000e83539c3/content.htm

To create an internal service in the SICF service hierarchy, proceed as follows:

1. Call transaction **SICF**.
2. On the initial screen, select an existing virtual host or services/service nodes under which you want to create a service (here `/default_host/zes/opensearch/`).
3. Now select an object in the hierarchy that you want to use as a root node (or parent node) of the service you are creating (this can be an existing service or a [virtual host](#)) and click the button “create host/service” (or right-click and choose *New Subelement*).

In our case it was `/default_host/zes/opensearch/`.



4. In the following *Create a Service* dialog box, do the following
 - a. Enter a name for your alias (for example *search*).
 - b. Choose *Alias to Existing Service*.

Create a Service Element

Name of Service Element to Be Created:

Type of Service Node to Be Created:

Independent Service

Reference to Existing Service

5. In the screen Create/Change a Service Call do the following
 - a. Enter a description (in our example we used *search*)
 - b. Select the Tab *Alias Trgt* and select the required target service in the hierarchy structure

Create/Change a Service Reference

Path

Service Name Service Reference (Active)

Alias Target

Lang. [Other Languages](#)

Description

Description 1

Description 2

Description 3

Service Data | Logon Data | **Alias Trgt** | Error Pages | Administration

Select target handler by double-clicking:

Virtuelle Hosts / Services	Documentation	Referenz Service
bc	BASIS TREE (BASIS FUNCTIONS)	
bw	BW	
es	Enterprise Search	
getdocument	Service for getting documents in enterprise ...	
opensearch	Open Search	
descriptio	Open Search Description	
list	OPML List	
search	Open Search	
meData	meData synchronization Service	
xi	Exchange Infrastructure (XI)	
sap_java	VM Container Engine for Java Applications	
zes	Enterprise Search Alias entries in the custo...	
SAPconnect	SAPCONNECT (E)SMTP	

- c. Select the Tab *Error Pages* select the option *Redirect to URL* and enter a Redirect URL

(here <http://iwdfvm3137.wdf.sap.corp:50100/RedirectApp/redirect.jsp?to=http://ivm12087.wdf.sap.corp:50100<%=PATHTRANS%>>)

be sure also to select the radio button "Form Fields (Text Form)" as shown in the following screen shot.

Service Referen Edit System Help

Create/Change a Service Reference

Path /default_hostzes/opensearch/
 Service Name search Service Reference (Active)
 Alias Target: /default_host/sap/es/opensearch/search
 Lang. English Other Languages

Description
 Description 1 Open Search
 Description 2
 Description 3

Service Data Logon Data Alias Trgt Error Pages Administration

Logon Errors Appl. Errors Logoff Page Not Accessible

Explicit Response Time Documentation
 Explicit Response Page Header
 Alias
 Header Page

Explicit Response Page Body
 Alias
 Body Page

Redirect to URL Status 2
 Redirect
 http://iwdfvm3137.wdf.sap.corp:50000/RedirectApp/test.jsp?to=http://ivml2087.v
 W/o Form Fields Form Fields (Text Form)
 Form Fields (Base64)

System Logon Configuration

6. Save your data.
7. Check that the service is active.

Finally make sure that the following profile parameters

```
login/accept_sso2_ticket = 1
login/create_sso2_ticket = 2 (this parameter is optional)
```

are set on the ABAP side using transaction RZ10:

Display Profile 'DEFAULT' Version '000004'		
Parameter ▶▶		
05.03.2010	Active parameters	14:50:06
Parameter Name	Parameter value	
login/create_sso2_ticket	1	
login/accept_sso2_ticket	2	
login/min_password_diff	1	
login/min_password_digits	1	

Now we are almost done. In the final step make sure that the J2EE Engines certificates are trusted by the ABAP system. For this export the J2EE certificate via Visual Administrator:

The screenshot shows the Visual Administrator interface. On the left, the 'Global Configuration' tree is visible, with 'Key Storage' highlighted. The main area is divided into 'Runtime', 'Properties', and 'Additional Info' tabs. Under 'Runtime', the 'Views' tab shows 'DEFAULT' and 'TicketKeystore'. Under 'Entries', 'SAPLogonTicketKeypair' and 'SAPLogonTicketKeypair-cert' are listed. The 'Additional Info' tab displays the certificate details:

```

CERTIFICATE
[creationDate]: Mon Aug 16 15:53:01 CEST 2010
[DN]: OU=J2EE,CN=SPO
[issuerDN]: OU=J2EE,CN=SPO
[validNotBefore]: Mon Aug 16 15:53:01 CEST 2010
[validNotAfter]: Fri Aug 16 15:53:01 CEST 2030
[signAlgorithm]: dsawithSHA(1.2.840.10040.4.3)
[fingerprint]: 89:1C:E1:4D:9E:93:13:CC:75:2C:3E:D4:19:23:3B:82
[subjectKeyIdentifier]: <none>
[publicKey]:
  [algorithm]: DSA
  [format]: X.509
  
```

At the bottom right, the 'Entry' and 'View' sections contain buttons for 'Create', 'Rename', 'Delete', 'Load', 'Export', 'Save to File', 'Load from File', 'Import from Other', 'Generate CSR Request', and 'Import CSR Response'. The 'Export' button is highlighted with a red box.

and import it via transaction STRUSTSSO2 to the ABAP system:

Trust Manager for Single Sign-On with Logon Ticket

- ▶ System PSE
- ▶ SNC SAPCryptolib
- ▶ SSL server Standard
- ▶ SSL client SSL Client (Anony)
- ▶ SSL client SSL Client (Stand
- ✗ SSL client WSSE Web Servi
- ✗ WS Security Standard
- ✗ WS Security Other System
- ✗ WS Security WS Security Ki
- File
- ✗ SSF E-Learning

System PSE

Own Certificate

Owner (Self-Signed)

Certificate List

Owner	
OU=J2EE, CN=EPD	
OU=J2EE, CN=P70	
OU=J2EE, CN=SDN	
OU=J2EE, CN=SP1	

Veri. PSE Password

Certificate

Owner

Issuer

Serial Number

Valid From to

Check Sum

Add to Certificate List Add to ACL

Logon Ticket

Access Control List (ACL)

Sys...	Cl.	Certificate Owner
RDP	005	CN=RDP
SCL	100	CN=SCL, OU=SSL Server, O=SAP-AG, C=DE
SDN	000	OU=J2EE, CN=SDN
SP2	000	OU=J2EE, CN=SP2

That's it. Now you should be able to call the OpenSearch URL
<http://ivml2087.wdf.sap.corp:50100/zes/opensearch/search?q=test>

Like outlined above the Enterprise Search ABAP system will not show you an access denied error, but redirect to
<http://iwdfvm3137.wdf.sap.corp:50100/RedirectApp/redirect.jsp?to=http://ivml2087.wdf.sap.corp:50100%2fzes%2fopensearch%2fsearch&sap-ffield=q%3dtest>

On the J2EE Engine the request would get authenticated via SPNego and a SAP-Logon Ticket would be added to the Cookies. Then the RedirectApp redirects the call back to

<http://ivml2087.wdf.sap.corp:50100%2fzes%2fopensearch%2fsearch&sap-ffield=q%3dtest> (the part after the To=).

When we are back on the Enterprise Search ABAP system we have a SAP-Logon Ticket from a trusted J2EE Engine and we are able to execute the search.

Troubleshooting

For troubleshooting please take a closer look at the deployment steps of the Redirect Application in step "The Redirect App" from the "How To" section above). A Http Watch (or a similar HTTP Trace tool) might also be helpful (in <http://www.sdn.sap.com/irj/scn/weblogs?blog=/pub/wlg/17344> a detailed look on the stream via Http Watch is explained).

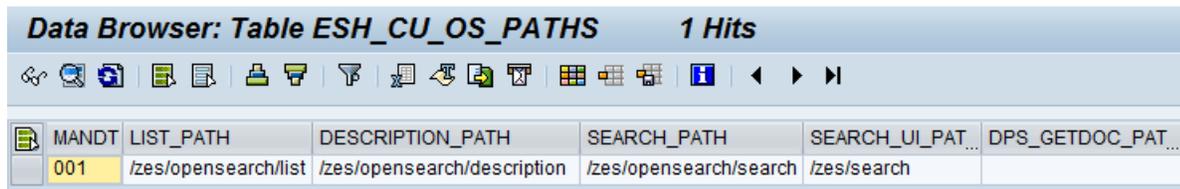
ESH specific customizing for OpenSearch URL's

If the OpenSearch Services and the Search UI in Enterprise Search are accessed via custom created internal alias entries in SICF one has to make sure that the URL's that are returned the OpenSearch Services also point to this custom services that are configured to support Integrated Windows Authentication.

For this one has to maintain appropriate entries in the customizing table ESH_CU_OS_PATHS as described in the SAP Note 1383252.

By entering the value /zes/opensearch/description for description the list service returns the URL /zes/opensearch/description rather than the original URL sap/es/opensearch/description.

Data Browser: Table ESH_CU_OS_PATHS 1 Hits



MANDT	LIST_PATH	DESCRIPTION_PATH	SEARCH_PATH	SEARCH_UI_PAT...	DPS_GETDOC_PAT...
001	/zes/opensearch/list	/zes/opensearch/description	/zes/opensearch/search	/zes/search	

Outlook

Single Sign-On based on Integrated Windows Authentication is a prerequisite if one of the following scenarios should be implemented:

1. Integration of SAP Enterprise Search as a Federated Search location into Microsoft Office SharePoint Server
2. Subscription to search results in SAP Enterprise Search as an RSS feed in Microsoft Outlook 2007

How to setup the scenarios mentioned above we will describe in upcoming whitepapers.

Related Content

[Error message when you subscribe to an RSS feed that requires authentication in Outlook 2007: "Outlook cannot download the RSS content"](#)

[Configuring and troubleshooting SPNego -- Part 1](#)

[Creating the Redirect EAR file](#)

[SAP Developer NetWork – Search Technologies](#)

[Creating and Configuring a SICF Service](#)

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

Copyright

© Copyright 2010 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Excel, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, System i, System i5, System p, System p5, System x, System z, System z10, System z9, z10, z9, iSeries, pSeries, xSeries, zSeries, eServer, z/VM, z/OS, i5/OS, S/390, OS/390, OS/400, AS/400, S/390 Parallel Enterprise Server, PowerVM, Power Architecture, POWER6+, POWER6, POWER5+, POWER5, POWER, OpenPower, PowerPC, BatchPipes, BladeCenter, System Storage, GPFS, HACMP, RETAIN, DB2 Connect, RACF, Redbooks, OS/2, Parallel Sysplex, MVS/ESA, AIX, Intelligent Miner, WebSphere, Netfinity, Tivoli and Informix are trademarks or registered trademarks of IBM Corporation.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc.

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects S.A. in the United States and in other countries. Business Objects is an SAP company.

All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.