

SINGLE SIGN-ON Installation and Administration

VERSION 1.2.1

© Copyright 2011 otris software AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means without express written permission of otris software AG. Any information contained in this publication is subject to change without notice.

All product names and logos contained in this publication are the property of their respective manufacturers.

otris software AG reserves the right to make changes to this software. The information contained in this manual in no way obligates the vendor.

Table of Contents

1. General	4
1.1Benefit of single sign-on	4 4 4 4 5 5 6 7 8
 2.1 Installing JCIFS	8 8 9 0
3.1 Installing Waffle	00000
4. SSO Using JESPA (NTLMv1 + NTLMv2)114.1 Installing JESPA114.2 Configuring a JESPA user114.3 Adding a JESPA filter114.3.1 Customizing the parameters12	1 1 1 2
5. SSO Using SPNego (Kerberos)13	3
5.1Setting up the Active Directory135.1.1Creating the required user account135.1.2Configuring the Service Principal Names (SPN)145.2Configuration files for SPNego155.3Installing SPNego165.4Adding the SPNego filter16	3 3 4 5 6
5.4.1Customizing the parameters175.5Setting up Firefox185.6Settings for Internet Explorer185.6.1Enabling auto-login185.6.2Enable integrated Windows Authentication20	7 8 8 8
5.7 Aids	0 2
6.1Installing the SSO filter226.2Adding the SSO filter226.3Setting the url pattern226.4Using the auto-login link23	- 2 2 3

1.1 Benefit of single sign-on

The use of single sign-on (SSO) requires that users authenticate themselves on a workstation only once and can then access all resources and services for which they have permission. Renewed login is not required. With regard to SSO, DOCUMENTS 4 supports several standard procedures on authentication. This document describes setting up the system environment for using these authentication methods in combination with DOCUMENTS 4.

1.2 Requirements

To be able to use SSO, the following requirements must be met for the system environment:

1.2.1 Domain controller

A domain must exist which is managed by a domain controller providing an *Active Directory*. This requires the *Microsoft Windows Server* operating system (tested with version 2008).

1.2.2 Application server

The application server on which the DOCUMENTS 4 installation is running must be accessible by the domain controller and by the workstations from the network. However, it does not necessarily be a member of the domain.

1.2.3 Workstation

Each workstation computer from which SSO should be used must be a member of the domain. Also, each user to log on via SSO should be a member of the domain and be created under the same user name in DOCUMENTS 4 - or, when LDAP coupling is available - be created in LDAP. The user's password must be identical in the domain an in DOCUMENTS 4 or LDAP.

When accessing a workstation that is not a member of the domain, a standard browser dialog (Basic-Auth) will be used to query the user's user name and password (see Fig. 1). The user will then be authenticated against the domain, and gain access to DOCUMENTS 4.

Windows Securit	Y	2	×
Connecting to w	2k8-DEMO.peachit.com.		
	User name		
	Password		
	Domain: PEACHIT Remember my credentials	s	
		OK Cancel	

Fig. 1: Standard logon dialog under Windows 7

1.2.4 Authentication method

SSO setup requires that you are familiar with the authentication method to be used. *NTLMv1*, *NTLMv2* and *Kerberos* are supported. The customer's system administrator must define which authentication method is to be used.

1.3 Setting up the DOCUMENTS 4 server

To allow login via SSO in the DOCUMENTS Manager, you need to add a new property named autoLogin = 1 for the *principal* (Fig. 2).

🔎 peachit (PeachIT DEMOPORTAL) - Portal *				
Settings Administration eMail-Service Properties				
Name Value				
	autoLogin	1		

Fig. 2: Properties of the principal

You need to ensure that the "Auto-login" setting on the "DOCUMENTS -> Settings" menu is turned off. This function cannot be used with SSO at the same time because auto-login and SSO are two competing login procedures.

1.4 Selecting the authentication module

To perform authentication on the Active Directory, multiple authentication modules are available. Module selection depends on which method is to be used for authentication.

Based on the following table, the suitable authentication module can be used using the authentication method.

Auth. Module	NTLMv1	NTLMv2	Kerberos
JCIFS	Yes	No	No
WAFFLE*	Yes	Yes	Yes
JESPA	Yes	Yes	No
SPNEGO	No	No	Yes

* For Waffle the application server must run on a Windows system.

The other configuration steps are explained below to use the respective authentication module.

NOTE! Consider the following when using NTLMv2:

JESPA and WAFFLE allow authentication both via NTLMv1 and NTLMv2. If you want to ensure that NTLMv2 is used, you must set this in the Domain Controller's group policies.

This setting can be found in the Domain Controller under: "Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options"; its name is "Network Security: LAN Manager authentication level". You need to select the appropriate option.

1.5 Overview of the system environment

Fig. 3 shows the structure of the system environment for the use of SSO with DOCUMENTS 4:



Fig. 3: System environment

The sections below describe which steps must be carried out to set up the different authentication modules.

2. SSO Using JCIFS (NTLMv1)

JCIFS is a program library that provides, among others, the functionality for authentication via NTLMv1. Details can be obtained at http://jcifs.samba.org/.

2.1 Installing JCIFS

As a rule, JCIFS version 1.1.9 is already preinstalled. If this is not the case, you can download a current version at <u>http://jcifs.samba.org/</u>. The downloaded archive named jcifs_1.1.9.zip contains the jcifs_1.1.9.jar file. This file must be copied to the www/WEB-INF/lib directory. You will then have to restart Tomcat. JCIFS version 1.1.9 has been successfully tested.

2.2 Adding the JCIFS filter

To enable authentication via NTLMv1, you need to add a filter in the web.xml file of the DOCUMENTS 4 application. To do this, you must insert the following text after the last <filter> element and before the first <filter mapping> element.





2.2.1 Customizing the parameters

- jcifs.http.domainController :Domain Controller's DNS name
- jcifs.smb.client.username: User name of any user with access to the domain (administrator rights not required). That user is used to query information on authenticating the user to be logged in.
- jcifs.smb.client.password: User's password
- jcifs.smb.client.domain: Domain name

Note to specifying the url pattern: The different options for setting the url pattern and its effects are described in section 6.3.

3.1 Installing Waffle

First you need to download the current Waffle package at http://waffle.codeplex.com/. The downloaded archive named waffle.codeplex.com/. The downloaded archive named waffle.l.3.zip contains the waffle.l.3.zip contains the waffle/Bin directory. All files with the ".jar" extension must be copied to the www/WEB-INF/lib directory. You will then have to restart Tomcat. Waffle version 1.3 has been successfully tested.

3.2 Adding the filter

To be able to use WAFFLE, adding the following filter to the web.xml file is enough.

<filter></filter>
<filter-name>WaffleFilter</filter-name>
<filter-class>waffle.servlet.NegotiateSecurityFilter</filter-class>
<init-param></init-param>
<pre><param-name></param-name></pre>
waffle.servlet.spi.NegotiateSecurityFilterProvider/protocols
<pre><param-value>NTLM</param-value></pre>
<filter-mapping></filter-mapping>
<filter-name>WaffleFilter</filter-name>
<url-pattern>/jsp/autologin</url-pattern>

3.2.1 Customizing the parameters

 waffle.servlet.spi.NegotiateSecurityFilterProvider: This parameter is used to set which authentication procedure to use. In our example, NTLMv1 or NTLMv2 is used. Which version is used depends on the Domain Controller settings. See: "NOTE! Consider the following when using NTLMv2." in section 1.4.

To use Kerberos, you need to enter "Negotiate" here.

Note to specifying the url pattern: The different options for setting the url pattern and its effects are described in section 6.3.

4.1 Installing JESPA

JESPA is a program library **subject to a charge** which, among others, provides functions for authentication via NTLMv1 and NTLMv2. JESPA must be purchased from the manufacturer at <u>www.ioplex.com</u>. The downloaded .jar file must be placed in the "www/WEB-INF/lib" directory of the Portal installation. You will then have to restart Tomcat. JESPA version 1.1.6 has been successfully tested.

4.2 Setting up a JESPA user

To be able to use authentication via JESPA, you need to create a COMPUTER account in the Active Directory, and assign it a password. This account can be created directly in the Active Directory. Although an existing computer account can be used, it is recommended that you create a new account so that this can be deleted later, if necessary, without dependencies on the existing system.

To allocate a password to the created account, you need to run the "SetComputerPassword" script that comes with JESPA on the console.

SetComputerPassword jespa\$@peachit.local password

When starting it, you need to append a \$ sign to the name of the account!

4.3 Adding a JESPA filter

To enable authentication via JESPA, you need to add a filter to the web.xml file of the DOCUMENTS 4 application. To do this, you must insert the following text after the last <filter> element and before the first <filter mapping> element.

<	filter>
	<filter-name>HttpSecurityFilter</filter-name>
	<filter-class>jespa.http.HttpSecurityFilter</filter-class>
	<init-param></init-param>
	<param-name>properties.path</param-name>
	<pre><param-value>/WEB-INF/example_ntlm.prp</param-value></pre>
	<filter-mapping></filter-mapping>
	<filter-name>HttpSecurityFilter</filter-name>
	< <mark>url-pattern</mark> >/jsp/autologin

4.3.1 Customizing the parameters

JESPA provides the option to transfer the filter parameters to Properties files. In this example, the settings were transferred to the <code>example_ntlm.rpr</code> file. While downloading, JESPA already has several different configurations.

```
provider.classname = jespa.ntlm.NtlmSecurityProvider
http.parameter.username.name = username
http.parameter.password.name = password
http.parameter.logout.name = logout
http.parameter.anonymous.name = anon
fallback.location = /jespa/Login.jsp
excludes = /Login.jsp
#groups.allowed = W\\Domain Admins
jespa.log.path = /tmp/jespa.log
jespa.log.level = 5
jespa.account.canonicalForm = 3
jespa.bindstr = peachitdc.peachit.local
jespa.dns.servers
  spa.service.acctname
                         jespa$@r
 espa.service.password = password
jespa.domain.netbios.name
jespa.domain.dns.name = peachit.local
 espa.authority.dns.names.resolve = fals
```

- jespa.bindstr: Complete DNS name of Domain Controller
- jespa.dns.servers:DNS server's IP address
- jespa.service.acctname: Name of created JESPA user
- jespa.service.password: Password of created JESPA user:
- jespa.domain.netbios.name: The domain's Netbios name
- jespa.domain.dns.name: Complete DNS name of the domain
- jespa.authority.dns.names.resolve: Must be set to false in this configuration.

Note to specifying the url pattern: The different options for the url pattern setting and its effects are described in section 6.3.

5.1 Setting up the Active Directory

To use Kerberos authentication, you need to make two settings on the Domain Controller.

5.1.1 Creating the required user account

Authentication via Kerberos requires setting up a user account in the Active Directory. It is important here that the following options are selected (see Fig. 4):

- Password does not expire
- no Kerberos preauthentication required

Willi Schreiber Properties
Dial-in Environment Sessions Remote control Remote Desktop Services Profile Personal Virtual Desktop COM+ General Address Account Profile Telephones Organization Member Of
User logon name: Schreiber @peachit.com User logon name (pre- <u>W</u> indows 2000): PEACHIT\ schreiber
Log On <u>T</u> o Unlock account Account options:
Use Kerberos DES encryption types for this account This account supports Kerberos AES 128 bit encryption. This account supports Kerberos AES 256 bit encryption. Do not require Kerberos preauthentication
Account expires Never O End of: Thursday , August 18, 2011
OK Cancel <u>A</u> pply Help

Fig. 4: Example: Windows Server 2008

5.1.2 Configuring the Service Principal Names (SPN)

In addition, you need to create so-called Service Principal Names for the created user. To do this, the "setspn" command is available. This must be used as follows and creates a new SPN for the HTTP service on computername for username:

```
setspn -a HTTP/computername username
```

The following command indicates all SPN assigned to the user wluser:

```
setspn -l wluser
```

Command for searching and displaying SPNs assigned twice:

```
setspn -x
```

For the use with DOCUMENTS 4 you need to set up two SPNs for the DOCUMENTS 4 application server. The service name corresponds to the domain name that is accessed. Assuming DOCUMENTS 4 is installed on the computer named "portalserver" in the "peachit.local" domain, then the commands may look as follows (see Fig. 5):



Fig. 5: The setspn command in the command line

IMPORTANT: A service (HTTP/portalserver) may only be assigned to exactly one user. But a user can be assigned several SPNs. To ensure that these restrictions are kept, you can execute the "setspn -x" command.

5.2 Configuration files for SPNego

For SPNego you need to create two configuration files that can be stored in anywhere within the system. The path to both files is entered later in the filter settings.

```
Content of the krb5.conf file
```

```
spnego-client {
  com.sun.security.auth.module.Krb5LoginModule required;
};
spnego-server {
  com.sun.security.auth.module.Krb5LoginModule required
  storeKey=true
  isInitiator=false
   debug=true;
};
```

Content of the login.conf file

```
[libdefaults]
default_realm = PEACHIT.LOCAL
default_tkt_enctypes = des-cbc-md5 des-cbc-crc rc4-hmac des3-cbc-shal
aes128-cts
default_tgs_enctypes = des-cbc-md5 des-cbc-crc rc4-hmac des3-cbc-shal
aes128-cts
[realms]
PEACHIT.LOCAL = {
    kdc = 192.168.7.75
    default_domain = PEACHIT.LOCAL
}
[domain_realm]
.PEACHIT.LOCAL = PEACHIT.LOCAL
```

The domain name "PEACHIT.LOCAL" must be replaced with the correct domain name here.

5.3 Installing SPNego

Initially, you need to download the current SPNego package at <u>http://spnego.sourceforge.net/</u>. The downloaded .jar file must be copied to the www/WEB-INF/lib directory. You will then have to restart Tomcat. SPNego version r7 has been successfully tested.

5.4 Adding the SPNego filter

To set up Kerberos authentication, you additionally need to add the SPNego filter to the www/WEB-INF/web.xml file. To do this, you must insert the following text after the last <filter> element and before the first <filter mapping> element.

<filter></filter>	
<filter-name>SpnegoHttpFilter</filter-name>	
<filter-class>net.sourceforge.spnego.SpnegoHttpFilter</filter-class>	
<init-param></init-param>	
<param-name>spnego.allow.basic</param-name>	
<pre><param-value>false</param-value></pre>	
<init-param></init-param>	
<pre><param-name>spnego.allow.localhost</param-name></pre>	
<pre><param-value>false</param-value></pre>	
<init-param></init-param>	
<param-name>spnego.allow.unsecure.basic</param-name>	
<pre><param-value>false</param-value></pre>	
<init-param></init-param>	
<param-name><mark>spnego.login.client.module</mark></param-name>	
<param-value>spnego-client</param-value>	
<init-param></init-param>	
<param-name>spnego.krb5.conf</param-name>	
<param-value>C:\tmp\krb5.conf</param-value>	
<init-param></init-param>	
<param-name>spnego.login.conf</param-name>	
<param-value>C:\tmp\login.conf</param-value>	
<init-param></init-param>	
<param-name><mark>spnego.preauth.username</mark></param-name>	
<param-value>spnego</param-value>	
<init-param></init-param>	



5.4.1 Customizing the parameters

- spnego.login.client.module: Name used for the setting in the login.conf file. Default: spondeo-client
- spnego.preauth.username: User name of the created SPNego user
- spnego.preauth.password: Password of the created SPNego user
- spnego.login.server.module: Name used for the setting in the login.conf file. Default: spnego-server

Note to specifying the url pattern: The different options for the url pattern setting and its effects are described in section 6.3.

5.5 Setting up Firefox

To be able to use Kerberos with Firefox, you need to make a setting in the browser. To do this, you start the configuration by specifying "about:config" in the Firefox address line (Fig. 6).

🦥 about:config - Mozilla Firefox				_ D ×
Eile Edit View Higtory Bookmarks Tools Help				
about:config × 🕹 Mozilla Firefox S	tart Page	× +		~
♦ ⇒ about:config			🟫 🗕 🤁 🚼 🗸 Google	۹
Eliter: network.negotiate				×
Preference Name	 Status 	Туре	Value	E
network.negotiate-auth.allow-proxies	default	boolean	true	
network.negotiate-auth.delegation-uris	user set	string	http://portalserver	
network.negotiate-auth.gsslib	default	string		
network.negotiate-auth.trusted-uris	default	string		
network.negotiate-auth.using-native-gsslib	default	boolean	true	
J				

Fig. 6: Firefox settings

You need to enter the URL of the application server key "network.negotiateauth.trusted-uris" here.

5.6 Settings for Internet Explorer

To be able to use Kerberos with Internet Explorer, two settings must be enabled. In Internet Explorer version 7 or higher these settings are enabled by default.

5.6.1 Enabling auto-login

To allow automatic logon in the Intranet zone, the following option from Fig. 7 and Fig. 8 must be enabled:

Tools -> Internet Options -> Security -> Local intranet -> Custom Level -> User Authentication -> "Automatic logon only in Intranet zone"

Internet Options	? ×
General Security Privacy Content Connections Programs Advance	ed
Select a zone to view or change security settings.	
sites	
Local intranet Sites This zone is for all websites that are found on your intranet. Sites	
Security level for this zone Allowed levels for this zone: All	
Appropriate for websites on your local network Appropriate for websites on your local network (intranet) Most content will be run without prompting you Unsigned ActiveX controls will not be downloaded Same as Medium level without prompts	
Enable Protected Mode (requires restarting Internet Explorer)	
<u>Custom level</u> Default level	
<u>R</u> eset all zones to default level	
OK Cancel Apply	



Security Settings - Local Intranet Zone	x
- Settings	
Seconda	
O Disable	
Enable	
Enable XSS filter	
 Disable 	
O Enable	
Scripting of Java applets	
O Disable	
Enable	
O Prompt	
Magnetication	
Kanal Kana	
Q Anonymous logon	
Automatic logon only in Intranet zone	
Automatic logon with current user name and password	
Prompt for user name and password	
*Takes effect after you restart Internet Evolorer	
rates encer and your estar canternet explorer	
Reset custom settings	7
Reset to: Medium-low (default)	
OK Creat	1
UK Cancel	

Fig. 8: Automatic logon only in Intranet zone enabled

5.6.2 Enable integrated Windows Authentication

This option is enabled on the "Advanced" tab of the Internet Options dialog. The "Enable integrated Windows authentication" option must be selected here (see Fig. 9).

Internet Options
General Security Privacy Content Connections Programs Advanced
Sattian
Seturigs
Security Allow active content from CDs to run on My Computer* Allow active content to run in files on My Computer* Allow software to run or install even if the signature is inva Block unsecured images with other mixed content Check for publisher's certificate revocation Check for server certificate revocation* Check for signatures on downloaded programs Do not save encrypted pages to disk Empty Temporary Internet Files folder when browser is de Enable DOM Storage Finable Integrated Windows Authentication* Enable memory protection to help mitigate online attacks* Enable native XMLHTTP support
*Takes effect after you restart Internet Evplorer
Restore advanced settings
Reset Internet Explorer settings
Resets Internet Explorer's settings to their default Reset
You should only use this if your browser is in an unusable state.
OK Cancel <u>A</u> pply

Fig. 9: Enable integrated Windows Authentication

5.7 Aids

To check correct Kerberos configuration, knowing which tickets are assigned to a client system comes in usefully. This can be checked using the "Kerbtray" program from the Resource toolkit. For the correct function a *Ticket Granting Ticket (TGT)* for the logged-in user as well as a correct *Service Ticket* for the application server must be present (see Fig. 10 and Fig. 11).

Kerberos Tickets	×
Client Principal schreiber@PEACHIT.LOCAL	
 cifs/w2k8peachit.peachit.local HTTP/ckvmsso.peachit.local krbtat/DEACHIT.LOCAL krbtgt/PEACHIT.LOCAL LDAn /w2k8peachit.peachit.local Idap/w2k8peachit.peachit.local/peachit.local 	
Service Principal krbtgt/PEACHIT.LOCAL@PEACHIT.LOCAL Names Times Flags Encryption types Client Name schreiber@PEACHIT.LOCAL	
Service Name krbtgt/PEACHIT.LOCAL@PEACHIT.LO Target Name krbtgt/PEACHIT@PEACHIT.LOCAL	

Fig. 10 :Ticket Granting Ticket (TGT) for user "writer"

Kerberos Tickets	
Client Principal schreiber@PEACHIT.LOCAL	
eifs/w2l-2posching withlocal	<u> </u>
 krbtgt/PEACHIT.LOCAL LDAP/w2k8peachit.peachit.local Idap/w2k8peachit.peachit.local/peachit.local 	
Service Principal HTTP/ckvmsso.peachit.local@PEACHIT.LOCAL	
Names Times Flags Encryption types	
Client Mame schreiber@PEACHIT.LOCAL	
Service Name HTTP/ckvmsso.peachit.local@PEACHI	
Target Name HTTP/ckvmsso.peachit.local@PEACHI	

Fig. 11 :Service Ticket for the ckvmsso.peachit.local

6.1 Installing the SSO filter

The required SSO filter (otrisSSO.jar) has already been installed; it resides in the "www/WEB-INF/lib" directory.

6.2 Adding the SSO filter

To use the SSO functionality for DOCUMENTS 4, you need to add another filter to the web.xml file in addition to the filter of the respective authentication module. To do this, the following code can be copied to the filter section of the web.xml file.

```
<filter>
<filter-name>SSOFilter</filter-name>
<filter-class>de.otris.portal.filter.SSOFilter</filter-class>
</filter>
<filter-mapping>
<filter-name>SSOFilter</filter-name>
<url-pattern>/jsp/autologin</url-pattern>
</filter-mapping>
```

6.3 Setting the url pattern

The url patterns of the different authentication modules and the SSO filter can be set for three different cases:

- /jsp/epctrl.jsp
 SSO is used for the default address of the DOCUMENTS system.
- /jsp/autologin
 SSO is enabled for the autologin link
- 3. /jsp/qv

SSO is enabled for QuickView. (On clicking links referring to DOCUMENTS 4 contents the user will also be authenticated via SSO.)

The different url patterns can be used in any combination. It is important that you use the same setting when setting the respective authentication method filter and for the SSO filter. If multiple url patterns are to be used at the same time, you will have to create the respective new "filter mapping" element.

Example:

<filter-mapping></filter-mapping>
<filter-name>SpnegoHttpFilter</filter-name>
<url-pattern>/jsp/autologin</url-pattern>
<filter-mapping></filter-mapping>
<filter-name>SpnegoHttpFilter</filter-name>
<url-pattern>/jsp/qv</url-pattern>
<filter-mapping></filter-mapping>
<filter-name>SSOFilter</filter-name>
<url-pattern>/jsp/autologin</url-pattern>
<filter-mapping></filter-mapping>
<filter-name>SSOFilter</filter-name>
<url-pattern>/jsp/qv</url-pattern>

In the above example, SSO is enabled for the autologin link and for QuickView. If a user opens the default url of the DOCUMENTS 4 system (/jsp/epctrl.jsp), the login dialog will be displayed.

6.4 Using the auto-login link

To automatically log in to DOCUMENTS 4, you can use an autologin link. To do this, you log in to DOCUMENTS 4 as usual. In the address bar you now replace the "epctrl.jsp" string with "autologin" (Fig. 12 and Fig. 13).



Fig. 12: Original address



Fig. 13: New address

If you open this link now, the user currently logged in to the Windows system will be automatically logged in to DOCUMENTS 4.

7. Table of Figures

Fig. 1: Standard logon dialog under Windows 7	5
Fig. 2: Properties of the principal	5
Fig. 3: System environment	7
Fig. 4: Example: Windows Server 2008	13
Fig. 5: The setspn command in the command line	14
Fig. 6: Firefox settings	18
Fig. 7: The "Internet Options" dialog	19
Fig. 8: Automatic logon only in Intranet zone enabled	19
Fig. 9: Enable integrated Windows Authentication	20
Fig. 10 :Ticket Granting Ticket (TGT) for user "writer"	21
Fig. 11 :Service Ticket for the ckvmsso.peachit.local	21
Fig. 12: Original address	23
Fig. 13: New address	23